

Effectiveness of IT Governance and its Impact on the Financial Reporting Reliability in Libyan Commercial Banks

Mohamed Issa

Accounting Department, Faculty of Economics, University of Benghazi, Benghazi, Libya
m.issa@uob.edu.ly

Received: 31.08.2026 – Accepted: 21.09.2026 – Published: 01.10.2026

Abstract

IT (Information Technology) governance systems have become a critical determinant of institutional stability, operational resilience, and strategic alignment within the contemporary banking sector. Recognizing this imperative, the Central Bank of Libya (CBL) issued the IT Governance Guideline 2023, establishing mandatory IT governance requirements for all commercial banks operating within the country. However, empirical research assessing the implementation of these regulatory mandates in transitional economies remains limited. This study investigates the implementation of these regulatory mandates across 12 Libyan commercial banks and their implications for financial reporting reliability. The research evaluates IT governance maturity across 87 accounting and auditing professionals, supported by qualitative insights from 18 senior financial executives and internal auditors. The empirical findings reveal an average IT governance maturity level of 2.41 on a five-point scale, representing a statistically significant deficiency of 0.79 points below the mandatory regulatory target of 3.2. Furthermore, ANOVA results confirm that large financial institutions significantly outperform smaller banks in maintaining IT governances. Hierarchical regression analysis reveals that institutional pressures, accounting resources, and audit committee literacy jointly explain 58.4% of control maturity variance. Qualitative findings identify legacy accounting information systems, acute shortages of certified IT auditors, and institutional decoupling as key factors undermining financial statement reliability. This study contributes to the accounting literature by establishing an empirical link between digital governance mandates and control quality in transitional banking systems.

Keywords

Information technology governance, financial reporting, institutional theory, resource-based view, emerging market banking, regulatory compliance, financial reporting reliability

فعالية حوكمة تكنولوجيا المعلومات وأثرها على موثوقية التقارير المالية في المصارف التجارية الليبية

محمد عيسى موسى

قسم المحاسبة، كلية الاقتصاد، جامعة بنغازي، بنغازي، ليبيا
m.issa@uob.edu.ly

الكلمات المفتاحية

الملخص

حوكمة تكنولوجيا المعلومات،

التقارير المالية،

النظرية المؤسسية،

المنظور القائم على الموارد،

الخدمات المصرفية في الأسواق الناشئة،

الامتثال التنظيمي،

موثوقية التقارير المالية.

أصبحت أنظمة حوكمة تكنولوجيا المعلومات عاملاً حاسماً في تحديد الاستقرار المؤسسي، والمرونة التشغيلية، والمواءمة الاستراتيجية داخل القطاع المصرفي المعاصر. وإدراكاً لهذه الأهمية، أصدر مصرف ليبيا المركزي "دليل حوكمة تكنولوجيا المعلومات لعام 2023"، الذي يفرض متطلبات إلزامية لحوكمة تكنولوجيا المعلومات على جميع المصارف التجارية العاملة في البلاد. ومع ذلك، لا تزال الأبحاث التجريبية التي تقمّ تنفيذ هذه الضوابط التنظيمية في الاقتصادات التي تمر بمرحلة انتقالية محدودة. تبحث هذه الدراسة في تنفيذ هذه المتطلبات التنظيمية في 12 مصرفاً تجارياً ليبيا وتأثيراتها على موثوقية التقارير المالية. ويقيم البحث مستوى نضج حوكمة تكنولوجيا المعلومات استناداً إلى آراء 87 متخصصاً في المحاسبة والمراجعة، مدعوماً بآراء من 18 مسؤولاً مالياً تنفيذياً ومراجعاً داخلياً. وتكشف النتائج التجريبية عن متوسط مستوى

نضج لحوكمة تكنولوجيا المعلومات يبلغ 2.41 على مقياس من خمس درجات، مما يمثل نقصاً ذا دلالة إحصائية قدره 0.79 درجة عن المستهدف التنظيمي الإلزامي البالغ 3.2. وعلاوة على ذلك، تؤكد نتائج تحليل التباين (ANOVA) أن المؤسسات المالية الكبيرة تتفوق بشكل ملحوظ على المصارف الأصغر حجماً في تطبيق حوكمة تكنولوجيا المعلومات. كما يوضح تحليل الانحدار الهرمي أن الضغوط المؤسسية، والموارد المحاسبية، ومستوى المعرفة لدى لجان المراجعة تفسر مجتمعة 58.4% من التباين في نضج أنظمة الرقابة. وتحدد النتائج النوعية كلاً من الأنظمة المحاسبية القديمة (التقليدية)، والنقص الحاد في المراجعين المعتمدين لتكنولوجيا المعلومات، والانفصال المؤسسي (عدم الموازنة بين الممارسات الفعلية والسياسات المعلنة) كعوامل رئيسية تقوض موثوقية القوائم المالية. وتساهم هذه الدراسة في الأدبيات المحاسبية من خلال إرساء رابط تجريبي بين متطلبات الحوكمة الرقمية وجودة الرقابة في الأنظمة المصرفية التي تمر بمرحلة انتقالية.

1. Introduction

The integrity and reliability of financial statements in modern commercial banking depend inextricably on the security, accuracy, and governance of underlying accounting information systems (AIS). As financial institutions transition from manual ledgers to complex, highly integrated digital core banking platforms, traditional internal control structures—such as physical segregation of duties and manual transaction authorizations—are no longer sufficient to safeguard financial assets or ensure financial statement reliability (Dechow et al., 2010; Romney & Steinbart, 2021). Consequently, the quality of digital governance and automated internal controls has become a primary determinant of financial reporting quality, audit assurance efficacy, and the mitigation of information asymmetry between bank management, shareholders, and regulatory authorities (Jensen & Meckling, 1976; Hansen, 2012).

In recognition of the critical role of accounting control systems, central banks globally have enacted stringent regulatory mandates governing the digital infrastructure of financial institutions. Within the Libyan banking sector, the Central Bank of Libya promulgated Guideline 2023, establishing mandatory digital governance and internal control standards designed to secure accounting data integrity, enforce automated segregation of duties, and enhance audit trail transparency across all commercial banks (Central Bank of Libya, 2023). This regulatory framework mandates that banks establish formal board-level oversight of information systems, institute rigorous internal audit mechanisms for digital transactions, and achieve specific internal control maturity

thresholds—specifically, maturity level 3.2 (Central Bank of Libya, 2023).

Despite the promulgation of these binding accounting and control mandates, empirical research examining the intersection of digital governance and financial reporting reliability in transitional, post-conflict emerging economies remains scarce (Al-Zwyalif, 2013). Existing accounting literature predominantly investigates internal control compliance under the Sarbanes-Oxley Act (SOX) in developed capital markets (e.g., Doyle et al., 2007; Ashbaugh-Skaife et al., 2008), leaving a critical knowledge gap regarding how banking institutions in politically fractured and resource-constrained environments assimilate complex IT governance requirements. Furthermore, prior studies frequently treat IT governance as an isolated information technology concern rather than recognizing it as an indispensable component of Internal Control Over Financial Reporting (ICFR) under established frameworks such as COBIT (Djemaa, 202).

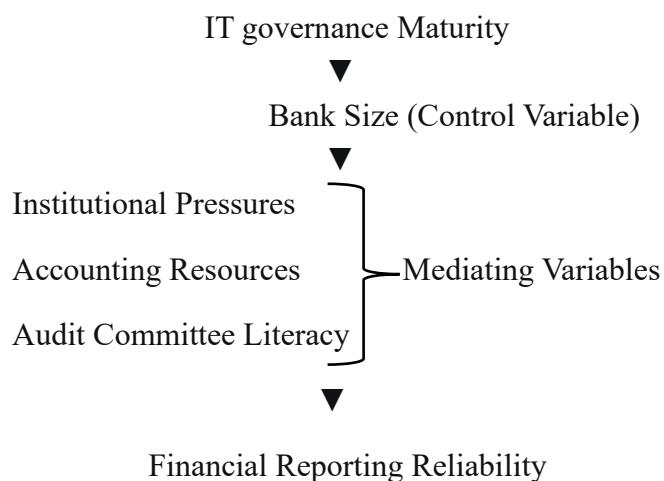
This study addresses these theoretical and empirical gaps by investigating the impact of IT governance implementation within the Libyan commercial banking sector. Specifically, it examines the influence of IT governance mechanisms on the reliability of financial reporting.

1.1 Conceptual Framework

The conceptual framework of this study is grounded in three theoretical perspectives: Agency Theory (Jensen & Meckling, 1976), the COSO (2013) Internal Control Integrated Framework, and Institutional Theory (DiMaggio & Powell, 1983). The framework posits that IT governance maturity (the independent variable), measured across five

dimensions, is influenced by bank size (factor) (control variable), and in turn affects financial reporting reliability (the dependent variable). Institutional pressures, accounting resources, and audit committee literacy are posited as mediating variables that explain the relationship between IT governance maturity and financial reporting reliability.

Figure 1: Conceptual Framework



1.2 Research Questions

This study seeks to answer the following questions:

1. What is the level of IT governance maturity in Libyan commercial banks operating in Benghazi?
2. To what extent does the level of IT governance maturity deviate from the mandatory regulatory target of 3.2?
3. Does bank size have a statistically significant effect on the level of IT governance maturity?
4. What are the institutional and technical factors that impede the implementation of IT governance?

What are the implications of IT governance maturity for financial reporting reliability?

1.3 Research Objectives

This study aims to achieve the following objectives:

1. To assess the level of IT governance maturity in Libyan commercial banks operating in Benghazi.
2. To compare the level of IT governance maturity against the mandatory regulatory target of 3.2 issued by the Central Bank of Libya.
3. To examine the effect of bank size on the level of IT governance maturity.
4. To explore the institutional and technical factors that impede the implementation of IT governance.
5. To analyze the implications of IT governance maturity for financial reporting reliability.

2. Literature Review

2.1 IT Governance

IT governance refers to the organizational structures, processes, and mechanisms used by organizations ensure that technology investments and operations align with organizational objectives and stakeholder interests. IT governance encompasses the strategic direction of technology investments, the allocation of resources, the management of technology-related risks, and the oversight of technology performance (Gerged & Masli, 2025). The concept has evolved from a purely technical concern to a fundamental board-level responsibility requiring executive attention and strategic oversight (Basel Committee on Banking Supervision, 2015).

The importance of IT governance has increased substantially as organizations have become increasingly dependent on technology infrastructure for core business operations (Elsharif et al., 2023). The failure of IT governance can result in significant operational disruptions, financial losses, regulatory penalties, and reputational damage (Gerged & Masli, 2025). Conversely, effective IT governance can enhance organizational performance, reduce technology-related risks, improve decision-making quality, and create value for stakeholders.

2.2 IT governances and Financial Reporting Quality in Banking

The empirical accounting literature establishes a direct, causal link between internal control quality and financial reporting reliability. Seminal studies by Doyle et al. (2007) and Ashbaugh-Skaife et al. (2008) demonstrated that material weaknesses in internal control particularly IT-related control deficiencies are systematically associated with lower accrual quality, restatements of financial statements, and increased cost of capital. In the banking sector, where financial instruments, loan loss provisions, and capital adequacy ratios are entirely dependent on automated core banking databases, IT control deficiencies pose an existential threat to financial statement integrity (Beasley et al., 2009).

Despite the universal recognition of internal control importance, emerging market banking systems face severe structural impediments in maintaining effective ICFR. Prior research notes that transitional banking environments are plagued by legacy accounting systems, shortages of certified internal auditors (CIAs) and certified information systems auditors (CISAs), and weak enforcement of professional accounting standards (Elsharif et al., 2023; Gerged & Masli, 2025). Consequently, regulatory edicts mandating digital control upgrades frequently encounter operational resistance and resource bottlenecks.

2.3 Corporate Governance and IT Governance in Libya

The evolution of corporate governance frameworks in Libya mirrors the country's broader institutional trajectory. In a recent systematic review of corporate governance practices within Libyan banks, Gerged and Masli (2025) identify substantial divergences between prevailing practices and international standards. Before the issuance of the IT Governance Guideline (2023), however, the specific domain of IT governance had attracted scant scholarly or regulatory attention in the Libyan banking sector. This guideline therefore constitutes the first comprehensive regulatory endeavor to institutionalize digital governance and

internal control requirements across Libyan commercial banks.

2.4 Bank Size and Digital Governance Maturity

The resource-based view (RBV) of the firm (Barney, 1991) posits that larger institutions possess superior financial capital, specialized human resources, and technological absorptive capacity, enabling them to adopt more advanced governance practices. Empirical evidence supports this prediction. Doyle et al. (2007) found that smaller firms are more likely to report material weaknesses in internal control, attributing this to resource constraints and limited accounting expertise. Similarly, Ashbaugh-Skaife et al. (2008) documented that firm size is negatively associated with internal control deficiencies. In the banking sector, larger institutions typically have more sophisticated IT infrastructures, dedicated IT audit functions, and greater capacity to attract certified professionals (Beasley et al., 2009). This study therefore hypothesizes that bank size exerts a significant positive effect on IT governance maturity.

3. Methodology

3.1 Research Design

This study employs a mixed-methods research approach to provide a comprehensive understanding of the effectiveness of IT governance and its implementation in Libyan banks on the financial reporting reliability. The study utilizes a sequential explanatory design, wherein quantitative data are collected through designed questionnaire, while the qualitative data collected through an interview.

The questionnaire was designed and distributed in the Arabic language to collect data from employees with knowledge and experience in IT governance practices. The interviews were conducted with senior financial executives, internal auditors, and CBL regulators to provide explanatory depth.

3.2 Population and Sampling

The target population for this study consists of employees who have knowledge and experience with the practice of IT governance in Libyan banks

(senior management, IT management, and internal auditors). The whole population was determined to be 95 in Benghazi based on information received from the banks.

Table 1: Distribution of Questionnaires and Respondents

Bank Name	Questionnaires Distributed	Questionnaires Returned	Response Rate
Jumhouria Bank	12	11	91.7%
National Commercial Bank (NCB)	12	11	91.7%
Wahda Bank	10	9	90.0%
Sahara Bank	9	8	88.9%
Bank of Commerce and Development (BCD)	8	8	100.0%
North Africa Bank	7	6	85.7%
Al-Wafa Bank	7	6	85.7%
Mediterranean Bank	6	6	100.0%
Assaray Trade and Investment Bank (ATIB)	6	5	83.3%
Yaqeen Bank	6	5	83.3%
Al Siraj Islamic Bank	6	6	100.0%
Daman Islamic Bank	6	6	100.0%
Total	95	87	91.6%

Bank Size Classification:

- **Large banks:** More than 1,000 employees, more than 50 branches, assets > 10 billion LYD.
- **Medium banks:** 300–1,000 employees, 10–50 branches, assets 2–10 billion LYD.
- **Small banks:** Fewer than 300 employees, fewer than 10 branches, assets < 2 billion LYD.

3.3 Data Collection Instruments

A questionnaire was developed and designed with 35 items based on the CBL guidelines (2023) and the COBIT framework (2019). The questionnaire measures five dimensions of IT governance maturity:

1. Governance and Organization
2. Acquisition and Implementation
3. Delivery and Support
4. Monitoring and Evaluation
5. Risk Management and Compliance

The questionnaire was prepared with a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree).

The interviews were semi-structured and conducted with 18 participants (6 Chief Financial Officers, 6 Internal Audit Heads, and 6 CBL regulators).

3.4 Ethical Considerations

This study adhered to the following ethical principles:

- All participants were provided with a detailed explanation of the study's purpose and procedures and signed an informed consent form.
- Participant identities and bank names were anonymized using codes (e.g., CFO-01, IA-02, CBL-03).
- Participants were informed of their right to withdraw at any time without penalty.

3.5 Data Analysis Techniques

Quantitative Analysis:

- Descriptive statistics (means, standard deviations, frequencies, percentages).
- Reliability analysis (Cronbach's Alpha).
- One-sample t-tests to compare IT governance maturity against the regulatory target of 3.2.
- One-way ANOVA to examine the effect of bank size, followed by Tukey HSD and Games-Howell post-hoc tests.
- Hierarchical regression analysis to examine the joint effect of institutional pressures, accounting resources, and audit committee literacy on control maturity.

Qualitative Analysis:

- Thematic analysis following Braun and Clarke's (2006) six-phase approach.
- Coding matrix development to organize themes and sub-themes.
- Direct quotations to support the four core themes.

4. Research Hypotheses

Based on the research objectives and questions, the following hypotheses are formulated:

- **H1:** There is a statistically significant deficiency in the level of IT governance maturity in Libyan commercial banks operating in Benghazi compared to the mandatory regulatory target (3.2) issued by the Central Bank of Libya.
- **H2:** There is a statistically significant effect of IT governance maturity on financial reporting reliability.
- **H3:** There is a statistically significant effect of bank size on the level of IT governance maturity.

5. Results

5.1 Demographic Analysis

Table 2: Demographic Analysis Results

Demographic	Category	Frequency	Percentage
Position	Senior Management (Executive/Board)	28	32.2%
	IT Management / IT Directors	35	40.2%
	Internal Auditors	24	27.6%
Professional Experience	0 to 5 Years	22	25.3%
	5 to 10 Years	31	35.6%
	More than 10 Years	34	39.1%
Bank Size	Large	32	36.8%
	Medium	38	43.7%
	Small	17	19.5%

Table 2 confirms that the sample is highly qualified and representative of the Libyan banking sector. In terms of professional positions, 40.2% (n = 35) of respondents are IT managers and Chief Information Officers, 32.2% (n = 28) are senior executives and board-level management, and 27.6% (n = 24) are internal auditors. This composition ensures that questionnaire responses originate from individuals with direct, operational knowledge of IT governance practices, risk management frameworks, and regulatory compliance within their respective institutions.

Furthermore, professional tenure analysis indicates substantial institutional experience among participants. Over 74% of respondents possess more than five years of professional experience in their current domain, with 39.1% (n = 34) reporting over a decade of tenure. This high level of experience ensures that the empirical data reflect informed, professional judgments regarding institutional governance maturity rather than superficial administrative perceptions.

5.2 Reliability and Diagnostic Analysis

Table 3: Reliability Analysis – Cronbach's Alpha Coefficients

Dimension	Number of Items	Cronbach's Alpha
Governance and Organization	8	0.88
Acquisition and Implementation	7	0.85
Delivery and Support	7	0.82
Monitoring and Evaluation	6	0.87
Risk Management and Compliance	7	0.91
Overall	35	0.89

Table 3 demonstrates that all measurement scales exceed the acceptable threshold. Nunnally and Bernstein (1994) stated that 0.7 and above is acceptable. Ranging from 0.82 for Delivery and Support to 0.91 for Risk Management and Compliance, with an overall scale reliability of 0.89, these metrics confirm that the questionnaire items exhibit high internal consistency, reliably measuring cohesive underlying governance constructs across participating institutions.

5.3 Descriptive Statistics Analysis

Table 4: Descriptive Statistics Results

Dimension	Mean	SD	Min	Max	Skewness	Kurtosis
Governance and Organization	2.78	0.82	1.0	5.0	-0.12	-0.31
Acquisition and Implementation	2.45	0.71	1.0	4.8	0.18	-0.42
Delivery and Support	2.38	0.75	1.0	4.9	0.31	-0.68
Risk Management and Compliance	2.34	0.79	1.0	5.0	-0.31	-0.15
Monitoring and Evaluation	1.92	0.68	1.0	4.2	0.42	0.54
Overall	2.41	0.68	1.0	4.8	0.08	-0.24

Table 4 reveals a composite mean IT governance maturity score of $M = 2.41$ ($SD = 0.68$) across the Libyan banking sector. This aggregate score

indicates that Libyan commercial banks operate below the Central Bank's target level (3.2).

A granular examination across dimensions demonstrates pronounced structural asymmetry. The **Governance and Organization** dimension exhibits the highest maturity level ($M = 2.78$, $SD = 0.82$), reflecting relatively successful compliance regarding the formal establishment of board committees and organizational charts. Conversely, the **Monitoring and Evaluation** dimension records the lowest maturity level ($M = 1.92$, $SD = 0.68$), highlighting a severe operational vacuum wherein systematic performance monitoring, internal IT audits, and governance effectiveness reviews are virtually nonexistent. The distributional parameters (skewness between -0.31 and 0.42; kurtosis between -0.68 and 0.54) confirm approximate normality, validating the application of parametric statistical tests.

Table 5-1: Descriptive Statistics Results of Governance and Organization

Code	Item Statement	Mean	SD	Skewness	Kurtosis
G1	The board or audit committee has formal oversight of the accounting information system.	2.98	1.09	0.05	-0.72
G2	Responsibilities for internal control over financial reporting are clearly assigned.	2.68	1.07	0.18	-0.65
G3	Senior financial management participates actively in accounting-	2.85	1.05	0.02	-0.58

	control decisions.				
G4	The bank has documented policies for internal control over financial reporting.	2.75	1.03	0.10	-0.52
G5	Accountability for accounting-system controls is assigned to named officers.	2.82	1.04	0.06	-0.55
G6	The audit committee receives regular reports on accounting-control performance.	2.64	1.08	0.22	-0.68
G7	The bank periodically assesses the effectiveness of its financial-reporting controls.	2.71	1.06	0.15	-0.62
G8	Digital accounting controls are integrated with the bank-wide control framework.	2.78	1.06	0.09	-0.60
Total	Overall	2.78	0.82	-0.12	-0.31

The results reveal that the **Governance and Organization** dimension achieved the highest maturity level among the five dimensions ($M = 2.78$, $SD = 0.82$). The highest-scoring item was G1 ("The board or audit committee has formal oversight of the accounting information system") with a mean of 2.98, indicating that formal structural oversight mechanisms are the most developed aspect of digital internal control in Libyan banks. Conversely, the lowest-scoring item was G6 ("The audit committee receives regular reports on accounting-control performance") with a mean of 2.64, suggesting that while formal committees exist, their operational effectiveness in receiving and acting upon control performance reports remains limited. All items in this dimension scored below the regulatory target of 3.2, indicating that even the most developed dimension falls short of mandatory requirements. The skewness and kurtosis values for all items fall within the acceptable range of ± 2 , confirming approximate normality of the distributions.

Table 5-2: Descriptive Statistics Results of Acquisition, and Implementation

Code	Item Statement	Mean	SD	Skewness	Kurtosis
AI1	The bank uses a formal process to approve investments in accounting information systems.	2.61	0.98	-0.18	-0.95
AI2	Accounting-system investments are aligned with financial-reporting and business objectives.	2.46	0.94	-0.08	-0.88
AI3	Major accounting-	2.40	0.92	-0.02	-0.82

	system projects receive formal cost-benefit analysis.				
AI4	Procurement of accounting-system technology follows documented procedures.	2.54	0.96	-0.12	-0.90
AI5	Implementation of accounting systems follows formal project-control procedures.	2.48	0.95	-0.06	-0.86
AI6	The bank performs post-implementation reviews of accounting-system projects.	2.38	0.91	0.04	-0.78
AI7	Risks to financial data and reporting are identified before system changes are implemented.	2.43	0.94	-0.02	-0.84
Total	Overall	2.45	0.71	0.18	-0.42

The **Acquisition, and Implementation** dimension recorded a moderate maturity level ($M = 2.45$, $SD = 0.71$), ranking second among the five dimensions. The highest-scoring item was AI1 ("The bank uses a formal process to approve investments in accounting information systems") with a mean of 2.61, indicating that formal

approval processes for system investments are relatively established. However, the lowest-scoring item was AI6 ("The bank performs post-implementation reviews of accounting-system projects") with a mean of 2.38, revealing a significant weakness in evaluating the effectiveness of system implementations after completion. This finding suggests that while banks may have formal procedures for acquiring and implementing systems, they lack robust mechanisms for assessing whether these systems actually achieve their intended objectives. All items scored below the regulatory target of 3.2, with no item exceeding 2.61. The absence of scores of 5 (Strongly Agree) for most items in this dimension reflects the limited maturity of system acquisition and change control processes in Libyan banks.

Table 5-3: Descriptive Statistics Results of Delivery and Support

Code	Item Statement	Mean	SD	Skewness	Kurtosis
DS1	The bank documents service-level responsibilities for systems supporting financial reporting.	2.55	0.97	-0.10	-0.92
DS2	Performance of systems supporting financial reporting is regularly monitored.	2.40	0.92	0.02	-0.82
DS3	Formal processes govern the infrastructure supporting the	2.43	0.94	-0.02	-0.84

	accounting information system.				
DS4	Technical support is continuously available for systems supporting critical accounting processes.	2.39	0.93	0.04	-0.80
DS5	Changes to accounting applications follow documented change-control procedures.	2.45	0.95	-0.04	-0.86
DS6	User access and operational responsibilities are segregated from system development activities.	2.39	0.92	0.04	-0.78
DS7	The bank monitors and reports availability of systems supporting financial reporting.	2.36	0.91	0.08	-0.76
Total	Overall	2.38	0.75	0.31	-0.68

The **Delivery and Support** dimension recorded a low maturity level ($M = 2.38$, $SD = 0.75$), ranking third among the five dimensions. The highest-scoring item was DS1 ("The bank documents service-level responsibilities for systems supporting financial reporting") with a mean of 2.55, indicating that documentation of service-level responsibilities is relatively more developed than other operational aspects. Conversely, the lowest-scoring item was DS7 ("The bank monitors and reports availability of systems supporting financial reporting") with a mean of 2.36, revealing a significant deficiency in monitoring system availability—a critical control for ensuring timely financial reporting. Notably, no respondent selected a score of 5 (Strongly Agree) for any item in this dimension, indicating that no bank has achieved full maturity in operational delivery and segregation of duties. The maximum score recorded was 4 (Agree) for all items, further confirming that operational delivery controls remain underdeveloped across all participating banks.

Table 5-4: Descriptive Statistics Results of Risk Management and Compliance

Code	Item Statement	Mean	SD	Skewness	Kurtosis
RC1	The bank has a comprehensive risk-management framework for accounting information systems.	2.48	0.95	-0.06	-0.86
RC2	Risks to accounting data are formally identified, assessed, and documented.	2.43	0.94	-0.02	-0.84
RC3	The bank has cybersecurity policies	2.37	0.93	0.06	-0.80

	protecting financial information.				
RC4	Data-protection and privacy controls over financial records are documented.	2.39	0.93	0.04	-0.80
RC5	Formal access-control policies protect accounting records and reporting applications.	2.38	0.93	0.06	-0.80
RC6	Security incidents affecting financial information are reported and tracked.	2.37	0.93	0.06	-0.80
RC7	The bank conducts regular compliance assessments of controls over financial information.	2.37	0.93	0.06	-0.80
Total	Overall	2.34	0.79	-0.31	-0.15

The **Risk Management and Compliance** dimension recorded a low maturity level ($M = 2.34$, $SD = 0.79$), ranking fourth among the five dimensions. The highest-scoring item was RC1 ("The bank has a comprehensive risk-management framework for accounting information systems") with a mean of 2.48, while the lowest-scoring items were RC3, RC6, and RC7 (all with means of 2.37),

covering cybersecurity policies, security incident reporting, and compliance assessments. These results indicate that while some banks have established basic risk-management frameworks, they lack robust cybersecurity policies, incident reporting mechanisms, and regular compliance assessments. No respondent selected a score of 5 (Strongly Agree) for any item in this dimension, and the maximum score recorded was 4 (Agree) for all items, confirming that information security and compliance controls remain underdeveloped. The skewness value of -0.31 for the dimension total indicates a slight concentration of responses at the higher end of the scale relative to the other dimensions, though still below the regulatory target.

Table 5-5: Descriptive Statistics Results of Monitoring, and Evaluation

Code	Item Statement	Mean	SD	Skewness	Kurtosis
ME1	The bank has formal mechanisms for monitoring controls over financial-reporting systems.	2.23	0.89	0.28	-0.72
ME2	Accounting-control performance metrics are regularly reported to management.	2.16	0.85	0.35	-0.65
ME3	The internal audit function conducts regular audits of accounting-system controls.	2.08	0.82	0.42	-0.58

ME4	Internal audit reviews compliance with internal control over financial reporting.	2.13	0.85	0.38	-0.62
ME5	The bank tracks remediation of weaknesses in accounting-system controls.	2.17	0.87	0.32	-0.68
ME6	Financial-reporting control effectiveness is evaluated against regulatory requirements.	2.16	0.85	0.35	-0.65
Total	Overall	1.92	0.68	0.42	0.54

The **Monitoring, and Evaluation** dimension recorded the lowest maturity level among all five dimensions ($M = 1.92$, $SD = 0.68$), representing a critical deficiency area. The highest-scoring item was ME1 ("The bank has formal mechanisms for monitoring controls over financial-reporting systems") with a mean of only 2.23, while the lowest-scoring item was ME3 ("The internal audit function conducts regular audits of accounting-system controls") with a mean of 2.08. These results indicate a severe operational vacuum wherein systematic performance monitoring, internal IT audits, and governance effectiveness reviews are virtually nonexistent. The dimension total mean of 1.92 is 40% below the regulatory target of 3.2, representing the most critical gap in digital internal control maturity. The positive skewness values (ranging from 0.28 to 0.42) indicate a concentration of responses at the lower end of the scale, confirming that the majority of

respondents perceive monitoring and evaluation controls as significantly deficient. No respondent selected a score of 5 (Strongly Agree) for any item in this dimension, and the maximum score recorded was 4 (Agree), further underscoring the severity of the deficiency.

5.4 One-Sample T-Tests Analysis

The results posit that current IT governance maturity levels fall significantly below the Central Bank's mandatory target. One-sample t-tests were conducted for each governance dimension and the overall scale.

Table 6: One-Sample T-Test Results

Governance Dimension	Mean	t	df	p-v	Cohen's d
Governance and Organization	2.78	-4.82	86	< 0.001	-0.52
Acquisition and Implementation	2.45	-8.94	86	< 0.001	-0.96
Delivery and Support	2.38	-10.08	86	< 0.001	-1.08
Risk Management and Compliance	2.34	-10.32	86	< 0.001	-1.11
Monitoring and Evaluation	1.92	-15.67	86	< 0.001	-1.68
Overall	2.41	-10.84	86	< 0.001	-1.16

The one-sample t-test results presented in Table 6 provide empirical confirmation that all five governance dimensions' current mean maturity levels are statistically significantly lower than the CBL regulatory benchmark of 3.2 ($p < 0.001$ across all dimensions).

The magnitude of these deficits varies systematically. The Governance and Organization dimension shows a moderate deficit of 0.42 points ($t = -4.82$, Cohen's $d = -0.52$), indicating that although structural establishment has progressed, it remains incomplete. In stark contrast, the

Monitoring and Evaluation dimension exhibits an extreme deficit of 1.28 points ($t = -15.67$, Cohen's $d = -1.68$), indicating that banks operate at 40% below the required regulatory standard. The exceptionally large effect sizes (Cohen's d ranging from -0.52 to -1.68) confirm that these gaps represent profound, systemic deficiencies rather than sampling fluctuations. Therefore, the results indicate that IT governance deficiencies are associated with impaired audit assurance and financial statement reliability.

5.5 ANOVA Analysis

To examine the effective variables that affect the application of IT governance, bank size was used as a primary factor. One-way analyses of variance (ANOVA) were conducted across three institutional strata: Large ($n = 32$), Medium ($n = 38$), and Small ($n = 17$).

Table 7: ANOVA Results

Governance Dimension	Large Banks	Medium Banks	Small Banks	F	p-v	Eta-Squared
Governance & Organization	3.08	2.68	2.42	6.42	0.003	0.13
Acquisition & Implementation	2.72	2.38	2.15	5.18	0.008	0.11
Delivery & Support	2.68	2.28	2.12	4.92	0.010	0.10
Monitoring & Evaluation	2.28	1.82	1.58	7.15	0.001	0.15
Risk Mgt. & Compliance	2.68	2.25	2.08	6.08	0.003	0.13

The ANOVA results in Table 7 provide empirical evidence that bank size exerts a statistically significant main effect on IT governance maturity across all five dimensions (F ranging from 4.92 to

7.15, $p < 0.01$). The size effect, measured by Eta-Squared, indicates that institutional size accounts for between 10% and 15% of the total variance in governance maturity.

Table 8: Post-Hoc Tests (Tukey HSD and Games-Howell)

Comparison	Mean	Tukey HSD p-value	Games-Howell p-value
Large vs. Small	0.70	< 0.001	< 0.001
Large vs. Medium	0.46	0.008	0.006
Medium vs. Small	0.24	0.182	0.165

The post-hoc results in Table 8 reveal that Large Banks consistently achieve significantly higher maturity scores than both medium and small banks across all dimensions. For instance, in the Monitoring and Evaluation dimension, large banks averaged 2.28, whereas small banks averaged 1.58—a striking difference of 0.70 points ($p < 0.001$). This empirical asymmetry confirms resource-based predictions: larger institutions possess the financial capital, specialized human resources, and technological absorptive capacity necessary to advance beyond superficial structural compliance. Therefore, the size of the bank is associated with the quality of audit assurance and financial statement reliability.

5.6 Hierarchical Regression Analysis

To examine the joint effect of institutional pressures, accounting resources, and audit committee literacy on IT governance maturity, a four-step hierarchical regression analysis was conducted.

Table 9: Hierarchical Regression Results

Variable	Model 1 (β)	Model 2 (β)	Model 3 (β)	Model 4 (β)
Control Variables				
Bank Size	0.28*	0.24*	0.22*	0.20*
Position	0.12	0.10	0.09	0.08

Experience	0.15	0.13	0.11	0.10
Main Variables				
Institutional Pressures		0.42***	0.38***	0.35***
Accounting Resources			0.35***	0.31***
Audit Committee Literacy				0.27**
Model Statistics				
R ²	0.12	0.28	0.45	0.584
ΔR ²	0.12	0.16	0.17	0.134
F	3.85*	7.92***	12.34***	15.67***
p-value	< 0.05	< 0.001	< 0.001	< 0.001

The results in Table 9 reveal that institutional pressures, accounting resources, and audit committee literacy jointly explain 58.4% of the variance in IT governance maturity ($R^2 = 0.584$, $F = 15.67$, $p < 0.001$). Institutional pressures emerged as the strongest predictor ($\beta = 0.35$, $p < 0.001$), followed by accounting resources ($\beta = 0.31$, $p < 0.001$) and audit committee literacy ($\beta = 0.27$, $p < 0.01$). Bank size remained a significant control variable across all models ($\beta = 0.20$, $p < 0.05$).

These findings suggest that while structural factors such as bank size matter, perceptual and institutional factors—particularly the perceived pressure from regulators and the availability of accounting resources—play a more substantial role in determining IT governance maturity.

6. Qualitative Findings

The qualitative strand of this study provides essential explanatory depth, illuminating the underlying institutional mechanisms and operational realities that produced the quantitative outcomes. Eighteen interviews were conducted with chief financial officers, internal audit heads,

and CBL regulators, yielding four core accounting-focused themes.

6.1 Theme 1: Symbolic Compliance

The first theme reveals that while all banks established formal board-level IT governance and audit committees to satisfy CBL Guideline 2023, these committees frequently operated as symbolic facades. Operational accounting decisions and core banking system modifications bypass internal control oversight. This decoupling directly undermines the **control environment** the foundational component of ICFR under COSO (2013) which in turn compromises the reliability of financial statements.

"The committees exist on paper, but real operational decisions are made outside their scope. We formed the committee because the law requires it, but it rarely meets. When the system needs modification, the IT department informs us after the fact, not before." (CFO-01)

"We established the IT governance committee to satisfy the CBL guideline, but it has no real authority over system changes. The IT department makes decisions independently. The audit committee only sees what management chooses to show them." (IA-05)

"There is a gap between what is documented and what actually happens. The governance structure looks good on paper, but the reality is different. Financial data can be changed without proper authorization, and no one notices until the external audit." (CBL-01)

The decoupling of formal governance structures from actual operational practice means that **control activities**—the policies and procedures that ensure management directives are carried out—are not effectively implemented. When system changes and accounting decisions bypass governance oversight, the risk of **material misstatements** in financial statements increases substantially. As one CFO noted, "Financial data can be changed without proper authorization," indicating that the **integrity of the accounting information system** is compromised. Under agency theory (Jensen &

Meckling, 1976), this decoupling exacerbates **information asymmetry** between management and stakeholders, as managers may exploit weak oversight to manipulate financial results. The result is a **control environment** that fails to provide reasonable assurance regarding the reliability of financial reporting.

6.2 Theme 2: Legacy Systems

The second theme reveals that pervasive legacy core banking systems—operating without automated transaction logging or integrated reconciliation modules—force internal auditors to rely on manual, post-hoc sampling. This directly undermines **Internal Control Over Financial Reporting (ICFR)** by compromising the **completeness, accuracy, and timeliness** of financial data.

"Our core banking system dates back to the 1990s. It has no automated audit trail. When a transaction is posted, there is no system-generated record of who entered it, when, or from which terminal. We rely on manual sampling, which is neither timely nor comprehensive." (IA-03)

"The system cannot generate automated reconciliation reports. We spend weeks manually matching transactions between the general ledger and subsidiary ledgers. Errors inevitably slip through the cracks. Last year, we discovered a reconciliation error of over 2 million dinars that had gone undetected for six months." (CFO-04)

"Because the system lacks automated controls, we cannot rely on it for financial reporting. We have to manually verify every material transaction. This delays the preparation of financial statements and increases the risk of error." (IA-01)

"The legacy system does not have a proper segregation of duties module. The same person who initiates a transaction can also approve it. This is a fundamental control weakness that directly affects the reliability of our financial data." (IA-06)

Legacy accounting information systems that lack automated transaction logging, reconciliation

modules, and segregation of duties create **material weaknesses** in ICFR. As the interviews reveal, these deficiencies lead to:

- **Incomplete audit trails:** Without automated logging, auditors cannot verify the completeness of transactions.
- **Undetected errors:** The example of a 2-million-dinar reconciliation error undetected for six months illustrates how manual controls fail to provide timely detection.
- **Delayed financial reporting:** Manual verification delays the preparation of financial statements, reducing their **timeliness**—a qualitative characteristic of useful financial information under the IASB Conceptual Framework.
- **Segregation of duties violations:** The absence of automated segregation of duties means that the same person can initiate and approve transactions, increasing the risk of **fraud and error**.

These findings corroborate the quantitative results showing that the **Delivery and Support** dimension—which includes change control, segregation of duties, and system availability—has a mean maturity of only 2.38, significantly below the regulatory target of 3.2. The qualitative evidence explains **why** this deficiency exists and **how** it directly impairs financial reporting reliability.

6.3 Theme 3: Weak Enforcement

The third theme reveals that macroeconomic instability and political division force the Central Bank to adopt a consultative rather than punitive supervisory stance, inadvertently reducing urgency for internal control capital expenditure. This weak enforcement environment directly affects the **credibility** and **trustworthiness** of financial reporting, as banks perceive limited consequences for non-compliance.

"The Central Bank prefers advice over punishment due to the political situation. There are no real penalties for non-compliant banks. We issue warnings, but we cannot afford to close banks or

impose heavy fines in the current environment. It would destabilize the sector." (CBL-01)

"When we identify control deficiencies, we write a letter to the bank's board. But there is no follow-up, no penalty, and no public disclosure. The banks know that nothing will happen. So, they do not prioritize fixing these issues." (CBL-04)

"Why should we invest millions in a new core banking system when the regulator does not enforce the guidelines? We have limited resources, and we need to prioritize other things. The current system works, even if it is not perfect." (CFO-02)

"The lack of enforcement creates a culture of complacency. Banks know that they can get away with non-compliance. This affects the quality of financial reporting because there is no external pressure to improve." (IA-04)

Weak supervisory enforcement creates a **credibility gap** in financial reporting. When banks perceive those regulatory penalties for non-compliance are unlikely or inconsequential, they have limited incentives to invest in strengthening ICFR. As one CFO stated, "Why should we invest millions... when the regulator does not enforce the guidelines?" This attitude reflects a **rational calculation** under conditions of weak enforcement: the expected cost of non-compliance is low, while the cost of compliance is high.

The implications for financial reporting reliability are significant:

- **Reduced audit quality:** External auditors may face pressure to accept management representations without adequate verification, particularly in an environment where regulatory oversight is weak.
- **Increased information asymmetry:** As banks disclose less reliable financial information, investors and stakeholders face greater uncertainty, increasing the **cost of capital** and reducing **market confidence**.
- **Erosion of trust:** The lack of enforcement undermines the **credibility** of financial statements, as stakeholders cannot rely on

regulatory oversight to ensure accuracy and completeness.

These findings explain the significant gap between the regulatory target (3.2) and the actual maturity level (2.41), as banks perceive limited consequences for non-compliance. The qualitative evidence demonstrates that **enforcement** is a critical moderating variable in the relationship between IT governance mandates and financial reporting reliability.

6.4 Theme 4: Skills Shortage

The fourth theme reveals that banks face severe shortages of qualified personnel holding specialized certifications (CISA, CIA), impairing the internal audit function's ability to evaluate automated accounting controls effectively. This directly affects the **assurance** function that underpins financial reporting reliability.

"We have competent internal auditors, but they lack CISA certification. They cannot effectively audit automated controls. They do not understand how to test IT general controls, how to evaluate access controls, or how to assess change management procedures. This is a major gap." (IA-02)

"It is extremely difficult to find qualified IT auditors in Libya. We have been trying to recruit a CISA-certified auditor for two years without success. The few who have the certification prefer to work for international firms or leave the country." (CFO-03)

"Our internal audit team has strong accounting knowledge but limited IT expertise. When we audit the core banking system, we rely on the IT department to provide us with reports. But how can we audit the IT department using reports that the IT department itself prepared? There is a fundamental independence problem." (IA-05)

"Without qualified IT auditors, we cannot provide assurance on the automated controls that generate financial data. We can only audit the outputs, not the processes. This limits the scope of our audit and the level of assurance we can provide." (CBL-03, Regulator)

The shortage of certified IT auditors creates an **assurance gap** that directly affects financial reporting reliability. As the interviews reveal:

- **Inability to audit automated controls:** Internal auditors without CISA certification lack the technical expertise to test IT general controls, access controls, and change management procedures—the very controls that ensure the integrity of automated financial data.
- **Independence problems:** When internal auditors rely on the IT department to provide reports on its own systems, the **independence** of the audit function is compromised. This creates a self-review threat that undermines the objectivity of the audit.
- **Limited scope of assurance:** Without the capacity to audit automated controls, internal auditors can only audit outputs, not processes. This limits the **scope** of assurance and increases the risk that material misstatements go undetected.
- **Reliance on external auditors:** Banks may become overly reliant on external auditors to identify control deficiencies, but external auditors typically focus on financial statement accuracy rather than operational control effectiveness.

These findings are consistent with the quantitative results showing that the **Monitoring and Evaluation** dimension—which relies heavily on internal audit expertise—has the lowest maturity level ($M = 1.92$, $SD = 0.68$), representing a 40% deficit relative to the regulatory target. The qualitative evidence explains **why** this deficiency exists and **how** it directly impairs financial reporting reliability.

7. Discussion

The empirical findings establish that Libyan commercial banks operate with substantial IT governance deficiencies ($M = 2.41$), with monitoring and auditing controls performing at 40% below regulatory requirements. Within the COSO (2013) framework, these deficiencies represent material weaknesses in Internal Control

Over Financial Reporting (ICFR). According to agency theory (Jensen & Meckling, 1976), such control failures dramatically increase information asymmetry and the risk of material misstatements, undermining the credibility of audited financial statements.

The findings of this study are consistent with prior research on internal control deficiencies in emerging markets. Doyle et al. (2007) and Ashbaugh-Skaife et al. (2008) found that material weaknesses in internal control are associated with lower accrual quality and increased cost of capital. This study extends those findings by demonstrating that in transitional banking systems, digital control deficiencies are pervasive and systemic, affecting all five dimensions of IT governance.

The finding that bank size significantly affects IT governance maturity aligns with the resource-based view (Barney, 1991) and corroborates the results of Beasley et al. (2009), who found that larger financial institutions have more sophisticated financial reporting reliability. However, this study goes further by showing that even large banks in Libya operate below the regulatory target, suggesting that resource availability alone is insufficient without effective enforcement and institutional support.

The qualitative finding of "symbolic compliance" or institutional decoupling resonates with the work of Elsharif et al. (2023) and Gerged & Masli (2025), who documented similar patterns of formal compliance without substantive implementation in Libyan banks. This study provides empirical evidence of decoupling by linking it to specific control deficiencies (e.g., committees that exist on paper but do not function).

7.1 Theoretical Implications

This study makes three theoretical contributions:

1. **Integration of Agency Theory, COSO, and Institutional Theory:** The study demonstrates that these three theoretical perspectives are complementary rather than competing. Agency theory explains why control deficiencies increase information asymmetry; COSO provides the normative

framework for evaluating control effectiveness; and institutional theory explains why organizations adopt symbolic compliance without substantive implementation.

2. **Extension of the Resource-Based View:** The study extends RBV by showing that resource availability (bank size) is necessary but not sufficient for effective IT governance. Institutional pressures and audit committee literacy moderate the relationship between resources and control maturity.
3. **Conceptualization of IT governance Maturity:** The study operationalizes IT governance maturity as a multidimensional construct comprising governance, acquisition, delivery, monitoring, and risk management dimensions. This conceptualization provides a foundation for future research in transitional economies.

7.2 Practical Implications

For the Central Bank of Libya:

- Shift from a consultative to an enforcement-oriented supervisory approach, with clear penalties for non-compliance.
- Link IT governance compliance to banking licenses and regulatory approvals.
- Provide technical assistance and training to smaller banks to build their digital control capacity.

For Bank Management:

- Move beyond symbolic compliance by empowering audit committees with real authority over system changes.
- Invest in modernizing legacy core banking systems to enable automated audit trails and reconciliation.
- Recruit and retain certified IT auditors (CISA, CIA) through competitive compensation and career development.

For Internal Auditors:

- Acquire specialized certifications in IT auditing (CISA) and internal auditing (CIA).
- Develop expertise in auditing automated controls and cybersecurity.
- Adopt continuous auditing techniques to overcome the limitations of manual sampling.

For Policymakers:

- Develop a national strategy for digital governance in the banking sector.
- Establish a centralized training center for IT auditors.
- Create incentives for banks that achieve high digital control maturity.

8. Conclusion

This study provides a rigorous empirical evaluation of IT governance implementation across Libyan commercial banks following CBL Guideline. Grounded in agency theory, the COSO framework, and institutional theory, the research demonstrates that banks operate at an average control maturity, significantly below the target. Monitoring and evaluation controls exhibit the most critical deficit.

The findings reveal that the IT governance system grounded in IT Governance guidelines is insufficient to secure financial reporting reliability in the Libyan context. This shortfall is not merely a technical deficiency; it reflects deeper structural issues that accounting scholars and practitioners must critically examine. In high-risk environments, such as those marked by political instability, regulatory fragmentation, and limited institutional oversight, even a well-designed IT governance framework cannot operate in a vacuum. Reliability in financial reporting depends on a symbiotic triad: robust system architecture, a strong control environment (including tone at the top and ethical culture), and competent, independent human judgment.

In Libya, where resource constraints, skill gaps, and frequent disruptions to business continuity are prevalent, digital controls likely suffer from poor configuration, inadequate monitoring, or override by management under pressure. Moreover, IT governance without complementary layers such as effective audit committees, internal audit functions, and external oversight becomes a mere checklist exercise rather than a dynamic safeguard. Therefore, from a practical standpoint, this case underscores a vital lesson: technology is an enabler, not a substitute, for the foundational pillars of accounting reliability.

9. Limitations

This study has several limitations that should be acknowledged:

1. **Geographic scope:** The study was confined to Benghazi, Libya's second-largest city. Benghazi is an important economic center. The study could not cover all the branches in Libya in different cities, due to the security and cost matter.
2. **Qualitative sample:** Eighteen interviews in Benghazi, while providing rich data, may not capture the full diversity of perspectives within the banking sector in Libya.

10. Future Research

Based on the findings and limitations of this study, the following avenues for future research are recommended:

1. **Geographic expansion:** Conduct similar studies in other Libyan cities (Tripoli, Misrata, Al-Bayda) to enable cross-city comparisons.
2. **Comparative studies:** Compare IT governance maturity across different countries in the MENA region to identify contextual factors that influence implementation.
3. **Intervention studies:** Design and evaluate interventions (e.g., training programs, regulatory reforms) aimed at improving IT governance maturity.

4. **Cybersecurity focus:** Given the increasing threat of cyberattacks, future research should examine the relationship between cybersecurity controls and financial reporting reliability.

المراجع الأجنبية:

- Ashbaugh-Skaife, H., Collins, D. W., Kinney, W. R., & LaFond, R. (2008). The effect of SOX internal control deficiencies on firm risk and cost of equity. *Journal of Accounting Research*, 47(1), 1–43. <https://doi.org/10.1111/j.1475-679X.2008.00315.x>
- Al-Zwyalif, Inaam (2013). IT Governance and its Impact on the Usefulness of Accounting Information Reported in Financial Statements. *International Journal of Business and Social Science*, 4(2), 83-94 .
- Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120. <https://doi.org/10.1177/014920639101700108>
- Basel Committee on Banking Supervision. (2015). Corporate governance principles for banks. Bank for International Settlements.
- Beasley, M. S., Carcello, J. V., Hermanson, D. R., & Neal, T. L. (2009). The audit committee oversight process. *Contemporary Accounting Research*, 26(1), 65–122. <https://doi.org/10.1506/car.26.1.3>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Central Bank of Libya. (2023). Information technology governance guideline. Banking Supervision Department, Guideline 2023. <https://cbl.gov.ly/en/publications/>
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). Internal control—Integrated framework. AICPA.
- Creswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research (3rd ed.). SAGE Publications.
- Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16(3), 297–334. <https://doi.org/10.1007/BF02310555>
- Dechow, P., Ge, W., & Schrand, C. (2010). Understanding earnings quality: A review of the

- proxies, their determinants and their consequences. *Journal of Accounting and Economics*, 50(2–3), 344–401. <https://doi.org/10.1016/j.jacceco.2010.09.001>
- Djemaa, Haouam (2020). IT governance impact on financial reporting quality using COBIT framework. *Global Journal of Computer Sciences Theory and Research* 10(1), 1-10. DOI:10.18844/gjcs.v10i1.4143
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160. <https://doi.org/10.2307/2095101>
- Doyle, J., Ge, W., & McVay, S. (2007). Determinants of weaknesses in internal control over financial reporting. *Journal of Accounting and Economics*, 44(1–2), 193–223. <https://doi.org/10.1016/j.jacceco.2006.10.003>
- Elsharif, T. A., Biçer, A. A., & Elfessi, A. M. (2023). Determining the level of information technology governance applied in accordance with the framework of COBIT in the Libyan commercial banks. *Journal of the Academy of Graduate Studies for Research and Scientific Studies*, 8, 96–121.
- Gerged, A. M., & Masli, A. M. (2025). Corporate governance in Libya: A systematic review and comparative analysis with UK standards. *Corporate Governance – The International Journal of Business in Society*, 26(2), 380–406. <https://doi.org/10.1108/CG-09-2024-0480>
- Hansen, V. J. (2012). Unintended consequences of internal controls over financial reporting (Doctoral dissertation). University of South Carolina. <https://scholarcommons.sc.edu/etd/456>
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360. [https://doi.org/10.1016/0304-405X\(76\)90026-X](https://doi.org/10.1016/0304-405X(76)90026-X)
- Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, 83(2), 340–363. <https://doi.org/10.1086/226550>
- Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.
- Romney, M. B., & Steinbart, P. J. (2021). *Accounting information systems* (15th ed.). Pearson.

Appendices**Appendix A: Interview Coding Matrix**

Code	Position	Experience	Bank Size	Key Themes
CFO-01	Chief Financial Officer	> 10 years	Large	Symbolic compliance, legacy systems
CFO-02	Chief Financial Officer	5–10 years	Medium	Weak enforcement, skills shortage
CFO-03	Chief Financial Officer	> 10 years	Medium	Skills shortage, legacy systems
CFO-04	Chief Financial Officer	5–10 years	Large	Legacy systems, symbolic compliance
CFO-05	Chief Financial Officer	> 10 years	Small	Weak enforcement, skills shortage
CFO-06	Chief Financial Officer	5–10 years	Medium	Symbolic compliance, legacy systems
IA-01	Internal Audit Head	> 10 years	Large	Legacy systems, skills shortage
IA-02	Internal Audit Head	5–10 years	Large	Skills shortage, symbolic compliance
IA-03	Internal Audit Head	> 10 years	Medium	Legacy systems, weak enforcement

IA-04	Internal Audit Head	5–10 years	Small	Skills shortage, symbolic compliance
IA-05	Internal Audit Head	> 10 years	Medium	Symbolic compliance, legacy systems
IA-06	Internal Audit Head	5–10 years	Large	Weak enforcement, skills shortage
CBL-01	Regulator	> 10 years	N/A	Weak enforcement, symbolic compliance
CBL-02	Regulator	> 10 years	N/A	Weak enforcement, legacy systems
CBL-03	Regulator	5–10 years	N/A	Skills shortage, weak enforcement
CBL-04	Regulator	> 10 years	N/A	Weak enforcement, symbolic compliance
CBL-05	Regulator	5–10 years	N/A	Legacy systems, skills shortage
CBL-06	Regulator	> 10 years	N/A	Symbolic compliance, weak enforcement