Almusawi, E. G. (2021). Using COBIT Framework for Reducing the Audit Risks of Accounting Information systems. *Akkad Journal of Contemporary Accounting Studies*, *1*(1), 52-74.

USING COBIT FRAMEWORK FOR REDUCING THE AUDIT RISKS OF ACCOUNTING INFORMATION SYSTEMS

Inaam Ghadeer Almusawi
University of Kufa,
Najaf, Iraq
E-mail:
inaamm.ghadeer@uokufa.edu.iq
ORCID: 0000-0001-5953-753X

Received: December 2020
1st Revision: February 2021
Accepted: March 2021

ABSTRACT. The fast transition of accounting information systems from manual to electronic media impacts the financial reporting process linked to information technology. First, significant dependence on electronic accounting information systems may expose the company's databases to information security threats, resulting in higher audit risks. As such, this study seeks to demonstrate how information technology governance structures may aid in protecting information in the context of electronic accounting information systems. Second, the study investigates the impact of improving information technology governance in Iraqi private banks in decreasing audit risks using the COBIT framework for internal control. The results indicate that implementing IT governance mechanisms in Iraqi private banks can reduce audit risks identified by external auditors. This framework increases the reliability of accounting information systems and enhances information security in the context of electronic accounting information systems. In addition, the field findings indicated a positive and statistically significant relationship between audit risk reduction and the dimensions of information technology governance (mechanisms and automation, policies, plans, and procedures, responsibility and accountability, skills and experience, knowledge and communication, and goal setting and measurement). Finally, the study proposes that Iraqi private banks implement the COBIT framework for internal control to govern information technology and risk management in electronic accounting information systems.

JEL Classification: D81, D82, M83

Keywords: COBIT, information risks, information security, AIS, Audit risks

Introduction

The use of information technology in the accounting and financial fields has seen a steady increase in the financial institutions operating in Iraq in the last10 years, particularly in the banking sector, which has led to increased interest in academic professionals and researchers

in studying the risks, means of control and auditing of electronic accounting systems applied in these institutions. Oversight of electronic accounting information systems is at the heart of audits conducted in the areas of IT auditing, financial auditing as well as IT Governance. Recent studies in the field of auditing the IT environment have confirmed the likes of Von Solms (2005), Iliescu (2010), Alfarajet et al. (2011), Haseley and Brucker (2012), Walker et al. (2012), Rubino and Vitolla (2014a) and others on the role that IT governance mechanisms play in achieving the organization's objectives, The effective application of IT Governance helps to emphasize that it supports the realization of The organization's objectives are to improve the effectiveness of investing and providing a mechanism for controlling IT risks. COBIT's internal control framework is a general model for internal control and information security protection, as well as a platform for better IT management and capabilities to provide added value to the organization and establish a risk management program to solve new problems resulting from the use of information technology in the organization's operations. From this point of view, the current study focuses on assessing the potential role of strengthening IT governance mechanisms in accordance with the COBIT internal control framework in reducing the risk of auditing electronic accounting systems Using the accounting system as a whole.

1. Literature Review

Studies on the subject of information technology governance varied, including those that focused on the security of financial information announced in financial statements, while other aspects of the research were of interest to researchers, including the relationship to the internal control system, money laundering, as well as the effectiveness of the application of governance mechanisms under electronic accounting information systems. The use of IT governance mechanisms to reduce the risks to information security in government units by reducing electronic financial manipulation under the e-government system. IT Governance of principles, objectives, and standards contributes to reducing electronic financial manipulation and achieving information security requirements in government units under the application of the e-government system.

As for study Vandervelde (2007) & Tuttle lose Aimed into test Frame Theoretical IT governance under framework COBIT For internal control in various areas of audit including operational audit, compliance Systems, and instructions as well as a financial audit. The results of this study have shown moan. It is important and useful for the audit profession to look for tests Academy For its applications, which provide a field guide for policymakers in promoting existing audit applications or not. As she showed, Results have a correlation between an application framework COBIT Internal Control Wall calendar Total operational risk COBIT Under electronic accounting systems. The results showed also moan Framework COBIT Could bemoan the cusses Dom Lilten Auditors' conduct in providing assistance in IT audits.

The Abu-Musa study (2009) also aimed to test the importance and application of related information and technological control objectives in accordance with the COBIT framework in Saudi companies. A few have confirmed that IT governance mechanisms have been properly implemented in their organizations. The results also showed that banks, financial institutions, and service institutions are more interested in implementing the COBIT framework than other organizations and that IT specialists, internal auditors, and executives are more aware of the importance of implementing the COBIT framework than others. Pramod, Li, and Gao (2011) proposed a framework to combat money laundering in banks by combining COBIT framework processes for information control and related technology with COSO framework components for internal oversight. Based on control processes and methods in electronic accounting systems.

On the other hand, she sought study (2014b) Ruby & Vitolla to Explain how IT Governance supports the system management dangers of Project ERM, In particular, the study focused on clarification How to help Goals Information and technology control Connected by companies in access into Its objectives Through the integration of the system management Project risks And a framework. COBIT for internal control. And I've shown Results Study moan Integration between framework COBIT. The framework of COSO ERM Could bemoan. Represents To any organization road؛ Good to achieve Goals Censorship Interior Ministry And management. Risks as well as company governance. Finally, the Fazlida & Said study (2015) sought to develop a theoretical framework for information security risks, Governance, and obstacles to its application. Based on the above, it can be said that the current Drahis distinguished from previous studies in that it highlights the importance of applying IT governance mechanisms in the Iraqi banking sector because of its usefulness in supporting information security and increasing the confidence of customers in this sector in the banking industry in general, as well as the current study focuses on evaluating the role of IT governance in reducing the risk of auditing electronic accounting information systems applied in banks Iraqi lye, which has not been tested in most previous studies.

3.1. IT Governance

Information technology governance is one of the concepts that has received great attention in recent times and has become an important topic in information technology. The It Institute has pointed out that Governance is the responsibility of the Board of Directors and Executive Management and is an integral part of the company's Governance and consists of leadership, organizational structure, and processes that emphasize the support of the organization's technology and ensure the achievement of the organization's strategy and objectives (Mirela,2010:33). Van Grembergen (2002) stressed that information governance is the regulatory capacity exercised by the Board of Directors, Executive Management, and IT Department to control the design and implementation of the IT strategy and to emphasize integration between the organization and information technology. Businesses include all levels of the organization. IT Governance includes managing IT processes and projects and emphasizing compatibility between those activities and the organization's specific needs in its strategies.

1. The organization's management understands the potential determinants of information technology.
2. The information technology function understands the objectives and needs of the organization associated with those goals.
3. This mutual understanding is carried out and monitored by the organization through accountability and the governance structure often.

Understanding the value and cost of information technology is important for both the manager, the board, and the IT department. Achieving successful compatibility between the organization and information technology requires that the organization's objectives and purposes comply with the organization's information systems needs and when information technology is able to meet those needs in cooperation with management. On this basis, the Department has a responsibility to take into account key areas of IT governance.

1. **Strategic Alignment**. Management has a responsibility to manage compatibility and harmony within the organization by emphasizing that IT strategies are compatible with the organization's strategies and that the provision of information technology is done in a timely and budgetary manner and carries an appropriate job description and balance in IT investments that support the

organization as a whole and those that help it grow and compete. It is achieved by information technology leading to increased administrative effectiveness.

2. **Value Delivery**. It is to improve the return on investment in INFORMATION technology by implementing a project to provide value to the customer, meet business requirements and verify the integrity and accuracy of information. The effectiveness of providing value is achieved only when costs have balanced against the return on investment in information technology. Management should ensure information technology that is compatible with the provision of value by building the technological infrastructure that enables the organization to grow and influence in new markets, increase total return, improve customer satisfaction, ensure customer retention and manage competitive strategies.
3. **Risk Management**. Addressing legal and regulatory compliance needs is concerned with understanding and managing the risks of key processes. Risk management is motivated by the need for management to demonstrate Governance in the company for various users, such as shareholders, regulators, users, customers, and processors. This includes determining risk tolerance, estimating knowledge of IT risks, and identifying risk exposures. Risk management in the Organization should also be an integral part of its operations to ensure a rapid response to ever-changing risk challenges.
4. **Resource Management**. It means properly reconciling IT potential with business needs, including improving IT resources, improving knowledge, and aligning with available potential. To achieve this, management should seek to emphasize the provision of appropriate methods and skills required in the organization to manage IT projects and that the objectives are realistic and achievable. Effective Governance of IT spending can lead to substantial cost savings.
5. **Performance Measurement**. Measuring IT performance through the use of a balanced scorecard is a very effective tool for the Board of Directors to achieve compatibility between information systems and the organization's strategy.

3.2. COBIT Internal Control Framework

COBIT's internal oversight framework is one of the most important developments in IT governance, with a range of best governance practices and audits of electronic information systems and related technology while emphasizing the reconciliation of its objectives applied in companies to those of those companies. COBIT's framework is concerned with internal oversight of electronic information systems, technology related to these systems, and protection of information security. The emergence of this framework dates back to the mid-1990s. Regulatory its operations. The first version of this framework appeared in 1996, while the second version was released in 1998, and the COBIT framework witnessed many subsequent developments based entirely on its audit, where this framework underwent a further development process under which it became a comprehensive framework for its management. IT management guidelines in the third version of the COBIT3 framework, which included metrics, key success factors, and Maturity Models for IT processes. Developments in IT Governance have not only continued to produce COBIT4 in 2005, which contains many concepts that illustrate governance and management mechanisms, for example:

- Compatibility between the organization's objectives and those of information technology and its relationship to supporting IT processes.
- Tasks and responsibilities within IT processes.
- Overlapping relationships between IT processes.

COBIT's latest release was COBIT5, released in 2012, and emphasized the concept of hand its quantity within the organization, and according to ISACA (2012), this version provides a more comprehensive framework that helps organizations achieve their goals in the areas of Governance and IT management. In it. It provides the necessary support to an organization in managing information technology in a comprehensive manner for the entire project, taking into account the identification of functional areas and the identification of responsibilities as well as the interests of internal and external beneficiaries. In this context, the fifth version of the COBIT framework identified the principles of internal control (DeHaes and Van Grembergen,2015) of five basic principles outlined in figure (1) as follows:

1. **Meeting Stakeholder Needs**-This principle means thatCOBIT must provide all processes and other factors that support the organization's value creation process through the use of information technology in a way that meets the needs of beneficiaries (stakeholders). This principle is critical for organizations because of the different objectives set for each organization, which requires them to adopt the objectives used to meet their objectives. However, the challenge for organizations is how to achieve this compatibility between the organizations and IT goals, which has led many researchers to seek a working guide to understand how the organization's objectives can affect relevant IT goals and vice versa.
2. **Covering the end-of-end coverage of the Enterprise** – Through this principle, the COBIT framework integrates IT Governance into the Governance of the company as a whole:
   - 2.1. Covering all functions and processes within the organization, the COBIT framework focuses not only on its function but also treats information and related techniques as assets that should be treated like any other asset in the organization.
   - 2.2. It takes into account all its Governance and management factors extensively and within the end-to-end method. For example, it must include everything internal or external that may be considered appropriate for the Governance and management of the organization's information.

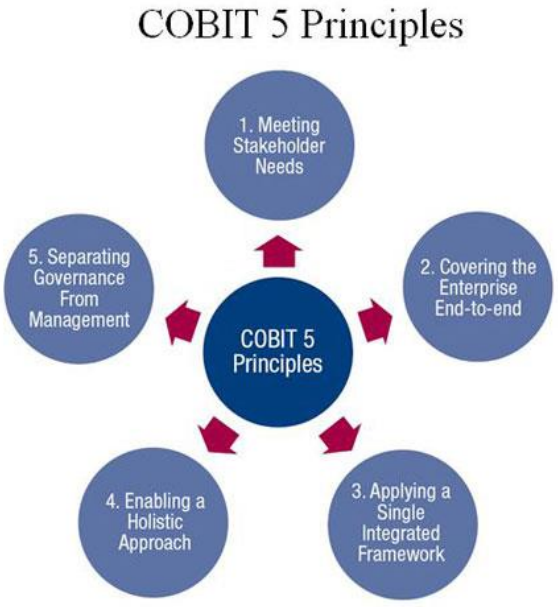

Figure 1: Principles of IT Governance

3. **Applying an Integrated Framework** - There are many good IT standards and applications, each providing a working guide for a subset of IT activities, and COBIT's framework is based on coordination and compatibility with other appropriate standards and frameworks to create a unified approach, so the COBIT framework serves as a comprehensive framework for Governance and IT management in the organization.

4. **Enabling a Holistic Approach**- Efficient and effective IT governance and management in the organization requires a comprehensive approach that takes into account a number of elements interacting with each other.

1. Principles, policies, and frameworks
2. Operations
3. Organizational structures
4. Culture, ethics, and behavior
5. Information
6. Services, infrastructure, and applications
7. People, skills, and specialties

5. Separating Governance from management the COBIT framework distinguishes a clear distinction between Governance and management, encompassing different types of activities, requiring different regulatory structures, and serving different purposes.

Based on the foregoing, COBIT internal control framework is an integrated IT governance framework that deals primarily with electronic accounting systems and specializes in providing IT control mechanisms used in the preparation of financial disclosures. Three points are:

1. Allow the organization's management to make a benchmark comparison with regard to information technology protection and control.
2. Its users are assured of the adequacy of protection and the availability of appropriate control mechanisms.
3. The auditor can express his opinion on internal oversight and advise on the availability of security for information technology.

3.3. Risks of Auditing Electronic Accounting Systems

Audit risks are defined as risks related to the auditor's failure by inadvertently modifying a banner appropriately on financial statements that are essentially fundamentally flawed. The second fieldwork criteria require the auditor to understand the nature and environment of the unit, including the internal control system, to identify the risk of fundamental errors in the client's financial statements. The audit risk model is the basis on which auditors take into account risks in planning procedures for obtaining proof of proof. This model helps auditors determine how much evidence to compile at each stage of the audit (Arens et al., 2012).

This model is usually formulated as follows:

$$PDR = \frac{\text{AAR}}{\text{IR} \times \text{CR}}$$

Where:
PDR= Planned Discovery Risks
AAR= Acceptable Audit Risks
AND= inherent risks

CR= Control Risks

Planned Detection Risk risks are the risks that proof of a particular part of the single part fails to detect errors that exceed the level of errors allowed. There are points to know when talking about the dangers of planned discovery. The first is that the risks of planned discovery depend on the other three factors in the audit risk model (acceptable audit risks, inherent audit risks, and control risks). They change only when the auditor changes one of the other risk factors. The second point is that the risks of planned discovery determine the amount of evidence that the auditor must compile and are inversely proportional to the scale of the risk of planned discovery. If the level of risk of planned discovery decreases, the auditor needs to compile more evidence to achieve a lower level of risk of detecting a scheme. On the contrary, the level of risk of planned salary discovery is high, so that the amount of evidence to be collected around the salary component must be reduced.

- Inherent risk measures the auditor's assessment of the possibility that there may be substantial errors as a result of error or fraud in a particular part or item before taking into account the effectiveness of the internal control system. If the auditor concludes that there are errors, there is a high level of inherent risk. The terms of the financial statements vary in the level of risk they carry, with acquisitions of fixed assets, inventory, and cash payments enjoying a high level of inherent risk, while the risk is lower in other items such as salaries, human resources, etc. Based on audit results in previous years.
- Control Risk. Risks resulting from a fundamental error in an item that cannot be prevented or detected in a timely manner through internal control procedures. The customer's inner house. There is a strong relationship between inherent risks and control risks, as both types affect the level of risk of planned discovery.
- Acceptable Audit Risk risks and measures how the auditor is prepared to be here as material errors in financial statements after the audit is completed and an unreserved opinion is reached. The risk situation is zero, which means full certainty, and 100%risk means complete uncertainty.

Auditors usually accept a certain level of risk or non-verification when performing the audit function. An efficient auditor understands that risks exist and deals with those risks in an appropriate manner. Most of the risks faced by auditors are difficult to measure and require careful attention before the auditor can respond appropriately. Responding appropriately to those risks is key to achieving a high-quality audit. An effective internal control system contributes to reducing audit risks, particularly in electronic accounting systems that adopt advanced information technology (2008:14). Those auditors should understand the mucus associated with accelerated technological changes and how to evaluate those risks to a particular customer. The risk impact is not only on electronic accounting information systems but also on the manual system, but to varying degrees depending on the level of complexity of the company's system, where the risk increases as the use of more sophisticated information technology increases.

3.3. COBIT's Role In Reducing Audit Risk

IT has become a strategic element for creating opportunities, innovation, and achieving the competitive advantage of organizations, but at the same time, it requires increasing inherent risks related to trust, integrity, as well as the security of the information generated. Effective IT governance mechanisms can therefore add value to the organization from the point of view of its users. COBIT's framework provides a comprehensive framework that helps organizations

achieve their goals and create added value by creating effective IT governance mechanisms within the organization.

In this research, elements or components of the COBIT internal control framework have been adopted as a basis for evaluating the role of strengthening IT governance mechanisms in reducing audit risk.

1. **Responsibility and Accountability** - Refers to IT governance procedures related to the identification of powers and responsibilities within the organization, which may include clear identification of responsibilities and powers in IT management, the preparation of a professional conduct guide for IT customers, as well as reports on evaluating user behavior within the organization.
2. **Awareness and Communication**. A range of government measures aimed at ensuring communication channels between different management levels related to IT management may include periodic reports to management on the compatibility of IT with the organization's strategy, reports on technical problems, and appropriate solutions.
3. **Policies, plans, and procedures**- refer to governance procedures related to evaluating the effectiveness of means of controlling data transmission within the system; such procedures may include strict controls on data transmission during data entry, processing, as well as outputs, as well as periodic reports from the IT department to detect unauthorized network access.
4. **Tools and Automation**- This element focuses on software governance procedures and database activity control systems.
5. **Skills and Expertiseskills and expertise**- governance procedures for the level of competence and competence required for IT customers.
6. **Goals and Measurement**- The last element is concerned with governance procedures related to setting and measuring IT objectives as well as evaluating the performance of the STRUCTURED IT department.

Such actions are expected to have a positive impact on the level of risk associated with auditing electronic accounting information systems. The third research is therefore devoted to testing the role of strengthening IT governance mechanisms in reducing the risk of auditing the electronic audit environment.

2. Research Methodology

The research Problem

Despite the role played by electronic information systems in facilitating the financial reporting process of companies, their emergence has been accompanied by increased risks of information security through hacking of information systems or attempts to manipulate accounting information, especially in the financial sector, which negatively affects the external auditor's assessment of the inherent degree of risk associated with each item of financial statements. On this basis, the problem with research lies in need to demonstrate the importance of implementing IT governance mechanisms in enhancing the security of electronic accounting systems and to assess the role of strengthening IT governance mechanisms in reducing audit risk under electronic accounting information systems.

The importance of research

The increasing use of information technology in accounting and financial areas has led to increased interest in oversight of electronic information systems, as the risks to such systems may lead to a loss of confidence in accounting information and fundamental errors in the financial reporting measurement process. The risks of corporate information systems adversely affect the integrity and accuracy of the information announced in financial statements. Moreover, assessing the risks of auditing accounting information systems is a key element in its financial audits.

Research goals

To clarify the importance of implementing IT governance mechanisms in enhancing information security under electronic accounting systems. A theoretical statement of the COBIT framework for internal control of electronic information systems. Assessing the role of strengthening IT Governance in reducing the risk of auditing electronic accounting systems.

Research hypotheses

In light of the research problem and the purpose of achieving its objectives in testing the impact of enhancing the company's IT governance on the external audit auditor's assessment of audit risks, the research is based on a single key hypothesis that:
"There is a statistically significant relationship between strengthening the company's IT governance and reducing the risk of electronic accounting information systems auditing."
The following sub-hypotheses are derived from this hypothesis:

Sub-hypothesis 1
Ho1:There is a statistically significant relationship between the liability variable and the risks of auditing electronic accounting information systems.

Sub-hypothesis 2
Ho2: There is a statistically significant relationship between the knowledge and communication variable and the risks of auditing electronic accounting information systems.

Sub-Hypothesis 3
Ho3:There is a statistically significant relationship between the policy variable and plans and the risks of auditing electronic accounting information systems.

Sub-Hypothesis 4
Ho4:There is a statistically significant relationship between the variable mechanisms and their relevance and the risks of auditing electronic accounting information systems.

Sub-Hypothesis 5
Ho5: There is a statistically significant relationship between the skills and experience variable and the risks of auditing electronic accounting information systems.

Sub-Hypothesis 6
Ho6: There is a statistically significant relationship between the variable objectives, measurement, and the risks of auditing electronic accounting information systems.

.

3. The Results

Research Measurements

This research is concerned with analyzing and testing the main and sub-research hypotheses, and for this purpose, the five-weight(Likert)scale, which is distributed from its highest weight and which gave (5) degrees to represent the answer field (fully agreed) to its lowest weight, which was given (1) degree to represent the answer field (not fully agreed) and among them three other weights are (2,3.4) to represent the answer fields (agreed, neutral, not agreed) respectively. Table 1 shows the distribution of resolution paragraphs to the main axes of the research.

Table1Distribution of resolution paragraphs

to	Dimensions of the measuring tool	Shortcut	Paragraphs	Number of paragraphs
1	**Strengthening IT governance**	**X**	**1-18**	**18**
1	Responsibility and accountability	*x1*	1-3	3
2	Knowledge and communication	*x2*	4-6	3
3	Policies and plans	*x3*	7-9	3
4	Mechanisms and mechanisms	*x4*	10-12	3
5	Skills and experience	*x5*	13-15	3
6	Goals and measurement	*X6*	16-18	3

The Sincerity and Stability of The Scale

In order to verify the sincerity of the measurement tool represented by the questionnaire was presented to a group of professors of the Faculty of Management and Economics at Kufa University, and their observations and suggestions on the correction of the resolution were taken, and the CronbachAlphalaboratories were adopted as a tool to ensure the stability and internal consistency of the paragraphs of this measure. The results shown in table 2 showed that the value of the Cronbach Alpha stability factor exceeded the acceptable 60% approval rate for the study results and for all study variables.

Table 2. Stability of the Study Scale

Variable	Shortcut	Value of Alpha
Strengthening IT Governance	X	.849
Responsibility and accountability	*x1*	.861
Knowledge and communication	*x2*	.883
Policies and plans	*x3*	.887

Mechanisms and mechanisms	*x4*	.865
Skills and experience	*x5*	.888
Goals and measurement	*X6*	.901
All variables		.892

Research sample

The research sample was represented by Iraqi commercial banks operating in Najaf province, as the commercial transactions of the banking sector are carried out through electronic accounting systems and can therefore meet the main purpose of the research, which is to test the role of IT governance mechanisms in reducing the risk of the audit process. Accordingly, 60 questionnaires were distributed to sample members of all administrative levels, accountants, auditors, and branch managers, of which 48 forms were recovered with a recovery rate of 80%.

Description and analysis of sample characteristics

Analysis of the demographic data of the search sample appears in table3.

Table 2 Demographics of the Search Sample

Variable	Categories	Number	%
Nature of work	manager	24	50
	accountant	18	38
	Checker	6	12
	Total	48	100
Scientific qualification	Doctor	0	0
	Master	6	19
	Bachelor	33	56
	diploma	9	25
	Total	48	100
Experience	1-5 years	12	25
	5-10 years	15	31
	10-20 years old	18	38
	20 years and over	3	6
	Total	48	100

Hypotheses Test Results

This section specializes in measuring the correlations between the research variables contained in the first main hypothesis, which states:

- H0 Null Hypothesis: "There is no statistically significant relationship between strengthening the company's IT governance and reducing the risk of electronic accounting information systems auditing."
- H1 AlternativeHypothesis: "There is a statistically significant relationship between strengthening the company's IT governance and reducing the risk of electronic accounting information systems auditing."

One-Sample T-Test was used at a morale level (5%) with a level of confidence (95%) for the two-party curve in order to test the main study hypothesis and sub-hypotheses, as Table 4 shows the results of the T-test of the main hypothesis and its hypotheses. Sub.

Table 4: Results of the main hypothesis test for research

One-Sample Test						
	Test Value = 3					
	t	of the	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference Lower	Upper
X1	28.341	47	.000	1.31896	1.2253	1.4126
X2	25.255	47	.000	1.14563	1.0544	1.2369
X3	24.082	47	.000	1.64583	1.5083	1.7833
X4	44.610	47	.000	1.68792	1.6118	1.7640
X5	26.299	47	.000	1.27104	1.1738	1.3683
X6	16.619	47	.000	.85396	.7506	.9573

Table 4 shows that the moral level of all variables was zero and that the averages for the six variables tested were greater than the default value of (3). Furthermore, the above results indicate that there are positive effects of the study variables related to strengthening its Governance in the company and reducing the risk of auditing electronic accounting information systems. Risks of auditing electronic accounting systems. To determine the level of relationship between the study variables and the audit risk checker's assessment level, a person's simple link coefficient was used to test each sub-hypothesis individually. The following are the results of the testing of the sub-hypotheses of the study:

The results of the first sub-hypothesis test:

- The first sub-hypothesis is to test the relationship between the liability and accountability variable and reduce the risk of auditing and states:
- **H0 Null Hypothesis**: There is no statistically significant relationship between the liability variable and the liability and risks of auditing electronic accounting information systems.
- **H1 Alternative Hypothesis**: There is a statistically significant relationship between the liability variable and accountability and the risks of auditing electronic accounting information systems.

Table 5 shows the results of the correlation (using the Pearson simple link coefficient) between the liability and accountability variable and reduce the risk of auditing electronic accounting information systems.

Table 5: Results of the First Sub-Hypothesis Test

Correlations			
		X	X1
And	Pearson Correlation	1	.876**
	Sig. (2-tailed)		.000
	N	48	48
X1	Pearson Correlation	.876**	1
	Sig. (2-tailed)	.000	
	N	48	48
**. Correlation is significant at the 0.01 level (2-tailed).			

The results in the table above indicate a strong and statistically significant correlation between the liability variable and the liability variable as an independent variable and reduce the risk of auditing electronic accounting information systems as a dependent variable, as the value of Pearson's factor of simple ranks between them (0,876)indicates this result. To the strength of the relationship between them, which means accepting the first sub-hypothesis.

Results of the second sub-hypothesis test:

The second sub-hypothesis specializes in testing the relationship between the knowledge variable and communications and reducing the risk of auditing and states:

- H0 Null Hypothesis: There is no statistically significant relationship between the knowledge and communication variable and the risks of auditing electronic accounting information systems.
- H1 Alternative Hypothesis: There is a statistically significant relationship between the knowledge and communication variable and the risks of auditing electronic accounting information systems.

Table 6 shows the results of the correlation between the knowledge and communication variable and reduce the risk of auditing electronic accounting information systems.

Table 6: Results of the Second Sub-Hypothesis Test

Correlations			
		X	X2
And	Pearson Correlation	1	.731**
	Sig. (2-tailed)		.000
	N	48	48
X2	Pearson Correlation	.731**	1
	Sig. (2-tailed)	.000	
	N	48	48
**. Correlation is significant at the 0.01 level (2-tailed).			

The results in Table 6 show a relatively strong and statistically significant correlation between the knowledge and communication variable as an independent variable and reduce the risk of auditing electronic accounting information systems as a dependent variable, and the value of Pearson coefficient for simple arrangements between them (0), 731), this result indicates the strength of the relationship between the two variables, which means accepting the second sub-hypothesis.

Results of the third sub-hypothesis test:

The third sub-hypothesis is to test the relationship between the policy variable and plans and reduce the risk of auditing and states:

- H0 Null Hypothesis: There is no statistically significant relationship between the policy variable and plans and the risks of auditing electronic accounting information systems.
- H1 Alternative Hypothesis: There is a statistically significant relationship between the policy variable and plans and the risks of auditing electronic accounting information systems.

The results shown in Table 7 include Pearson's correlation coefficient for the relationship between policy variables and plans and reducing the risk of auditing electronic accounting information systems.

Table 7: Results of the Third Sub-Hypothesis Test

Correlations			
		And	X3
And	Pearson Correlation	1	.811**
	Sig. (2-tailed)		.000
	N	48	48
X3	Pearson Correlation	.811**	1
	Sig. (2-tailed)	.000	
	N	48	48

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

Referring to These results, we can find a strong and significant ejection link. Statistics At the moral level (1%Ben. Variable Policies and plans Independent Change Committee Reducing the risk of auditing electronic accounting information systems As a continuing variable., because The value of the coefficient Pearson’s no. Simple arrangements between them (0,811) This result indicates The power of the relationship Between the two variables، Which indicates the Acceptance of the sub-hypothesis Third.

Results Of The Fourth Sub-Hypothesis Test

The fourth sub-hypothesis specializes in testing the relationship between variable mechanisms and automation and reducing the risk of auditing and states:

- H0 Null Hypothesis: There is no statistically significant relationship between variable mechanisms, automation, and the risks of auditing electronic accounting information systems.
- H1 Alternative Hypothesis: There is a statistically significant relationship between variable mechanisms, automation, and the risks of auditing electronic accounting information systems.

Table 8 shows the results of Pearson’s test of the relationship between variable mechanisms and their mechanisms and reduces the risk of auditing electronic accounting information systems.

Table 8: Results of the Fourth Sub-Hypothesis Test

Correlations

		And	X4
And	Pearson Correlation	1	.882**
	Sig. (2-tailed)		.000
	N	48	48
X4	Pearson Correlation	.882**	1
	Sig. (2-tailed)	.000	
	N	48	48

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

The results in the table above indicate a strong and statistically significant correlation between the variable mechanisms and its binding as an independent variable and reduce the risk of auditing electronic accounting information systems as a dependent variable, as the value of the pearson coefficient for simple arrangements between them (0), 882). This result refers to the strength of the two-variable relationships, indicating the acceptance of the fourth sub-hypothesis.

Results of the Fifth Sub-Hypothesis Test:

The fifth sub-hypothesis specializes in testing the relationship between the skills variable and experience and reducing the risk of auditing and states:

- H0 Null Hypothesis: There is no statistically significant relationship between the skills variable and experience and the risks of auditing electronic accounting information systems.
- H1 Alternative Hypothesis: There is a statistically significant relationship between the skills variable and experience and the risks of auditing electronic accounting information systems.

Table 9 shows the results of the link relationship using the Pearson coefficient for the simple correlation between the skills and experience variable and the reduction of the risk of auditing electronic accounting information systems.

Table 9: Results of the Fifth Sub-Hypothesis Test

Correlations

		And	X5
And	Pearson Correlation	1	.704**
	Sig. (2-tailed)		.000
	N	48	48
X5	Pearson Correlation	.704**	1
	Sig. (2-tailed)	.000	
	N	48	48

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

The results in the table above indicate a relatively strong and statistically significant correlation between the skills variable and experience as an independent variable and reduce the risk of auditing electronic accounting information systems as a dependent variable, as the value of Pearson's laboratory for simple ranks between them (0), 704). This result indicates the strength of the relationship between the two variables, which means accepting the fifth sub-hypothesis.

Results of the Sixth Sub-Hypothesis Test:

The sixth sub-hypothesis is to test the relationship between the variable objectives and measurement and reduce the risk of auditing and states:

- H0 Null Hypothesis: There is no statistically significant relationship between the variable objectives, measurement, and the risks of auditing electronic accounting information systems.
- H1 Alternative Hypothesis: There is a statistically significant relationship between the variable objectives, measurement, and the risks of auditing electronic accounting information systems.

Table (10) shows the results of the link relationship using the Pearson coefficient for the simple correlation between the objective variable and measurement and reducing the risk of auditing electronic accounting information systems.

Table 10: Results of the Sixth Sub-Hypothesis Test

Correlations

		And	X6
And	Pearson Correlation	1	.624**
	Sig. (2-tailed)		.000
	N	48	48
X6	Pearson Correlation	.624**	1
	Sig. (2-tailed)	.000	
	N	48	48

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

The results in Table 10 indicate a relatively strong and statistically significant ejective correlation at the moral level (1%) between the goal variable and measurement as an independent variable and reduce the risk of auditing electronic accounting information systems as a dependent variable, as the value of the Pearson factor for simple arrangements between them (0), 624). This result indicates the strength of the relationship between the two variables, indicating the acceptance of the sixth sub-hypothesis.

Discussion and interpretation of results

Figure 2 shows the varying impact of IT governance dimensions or elements in the level of risk of auditing electronic accounting information systems. It is clear from this form that the tool variable and its mechanism are the most influential in reducing the risk of auditing

electronic accounting information systems, with the average response of sample members to paragraphs related to this variable 4.69, which is high compared to other variables. Governance on tools and their mechanism. This finding can be explained by the fact that procedures such as software that enable the company to detect attempts to hack the system or automated database audit mechanisms to detect gaps in internal control methods greatly help reduce the risks inherent in terms of the financial disclosures, as well as the existence of an integrated software system to manage the base Data will undoubtedly facilitate and secure the transmission of information within the system, reducing the risk of hacking or manipulating information.

The second variable in terms of impact on audit risk was the policy and plan variable, with the average response of sample members to paragraphs relating to this variable at 4.65, indicating the importance of it-related policy and planning procedures within the organization in reducing audit risks. The means of controlling the transmission of data in its various stages inputs, processing, and outputs electronically or manually, as well as audits related to the detection of unauthorized access to the system, contribute to reducing cases of data manipulation or the introduction of false data, thereby reducing the risk of auditing such data. The third variable in importance was the responsibility and accountability variable, with the average response of sample members to the relevant paragraphs of 4.32, indicating the interest of sample members in liability and accountability procedures and their impact on reducing audit risks. The organization's preparation for an explicit description of responsibilities and powers related to IT activities, the existence of a guide to fair, professional conduct, as well as reports of breaches and questionable behaviors contribute to creating an environment that supports fair behavior within the organization, which reflects positively on the level of confidence in the system applied as a whole.

The skills and experience variable came in fourth place in terms of importance, with the average response of sample members to the relevant paragraphs 4.27, indicating that there is a relative impact of this variable in reducing the risk of auditing. The continuous evaluation of employee compliance with the company's information security standards, in addition to continuous training, leads to a reduction in cases of intentional or unintentional error and thus reduces the risk of system audit. The knowledge and communication variable came in fifth place with an average response of 4.15 for the resolution paragraphs related to this variable. The organization's successful efforts to invest its technologies in achieving its objectives and providing added value for its investment have positively affected the level of audit risk inherent in some of the organization's financial statements.

Finally, the objectives and measurement variables are sixth in importance in influencing the level of audit risk in electronic accounting systems. The average response of sample members to paragraphs related to this variable was 3.85, a small percentage compared to other variables. Information, the development of the organization's operational plans, as well as the existence of an effective mechanism to link its performance to the organization's objectives may contribute to increasing the effectiveness of internal control methods in electronic accounting systems from the continuous evaluation of technology within the organization.

Based on the foregoing, it can be said that an effective internal control system in organizations that adopt high-tech electronic accounting information systems such as banks or other organizations with IT governance mechanisms based on the COBIT internal control framework leads to the following benefits:

1. Improving the efficiency of the performance of the information technology applied in the organization by improving the security of information generated by the accounting system at every stage of it.
2. Improve the efficiency of its investment in the organization and avoid unnecessary spending in this area.

3. Increase the confidence of information users and other customers in the organization's information through an effective oversight mechanism for the work of the accounting system applied both technically and the availability of qualified personnel to deal with the system.
4. Reduce the effort and time spent by the external auditor as a result of an effective internal control system and a low level of audit risk to ensure that the associated audit costs are reduced.
5. Improving the quality of external auditing, which is a direct result of reduced audit risk and improving the security of information announced in financial statements.

Conclusions

Providing an appropriate environment for internal control under electronic accounting information systems through the application of IT governance mechanisms contributes to improving the quality of external auditing and affects reduced audit costs. The results of the statistical analysis of the responses of the sample members indicated a positive and statistically significant relationship between strengthening IT Governance and reducing the risk of electronic accounting information systems auditing. Field results showed a positive and statistically significant relationship between components of IT Governance that are compliant with variables (responsibility and accountability, knowledge and communication, policies and plans, mechanisms and mechanisms, skills and experience, objectives and measurement) and reduce the risk of electronic information systems auditing. The results of the research hypotheses test showed a disparity in the impact of IT governance procedures on the risks of auditing at the level of sub-variables, where the greatest impact of the variable mechanisms and its mechanisms, and then policy and plan variables, responsibility, and accountability, skills, and experience, knowledge, and communications respectively, while the impact of the variable objectives and measurement was the least among the Other changes. Iraqi companies operating the electronic accounting information systems environment, particularly Iraqi national banks, should adopt the COBIT internal control framework to ensure that companies have sufficient confidence in the applicable accounting system and improve information security within the system. The researcher recommends the need to establish an independent Iraqi internal control body that will issue binding instructions to companies to adopt governance standards commensurate with the needs of companies depending on the nature of their activity and the level of complexity in their it. Iraqi companies should adopt strict rules in selecting employees working in the IT department in a way that ensures that the company provides scientifically and behaviorally qualified cadres to work in this field. The need to work on the existence of effective means of continuously evaluating the mechanisms of control of information technology applied in companies as a result of the continuous development of the means of hacking electronic systems or attempting to manipulate their information. The researcher recommends the need to conduct future studies in the field of evaluating the effectiveness of the internal control system by adopting the COBIT and COSO frameworks for internal control.

References

Abu Hajar, Sameh, and Abedin, Amina, 2014," the role of IT governance mechanisms in reducing information security risks to reduce electronic financial manipulation in government units under the e-government system," the 5th Annual Conference of the Accounting Department School of Commerce - Cairo University.

Abu-Musa, A., (2009)," Exploring the importance and implementation of COBIT processes in Saudi organizations," Information Management & Computer Security, Vol. 17 Iss 2 pp. 73 – 95

Al-Alarkapi, Naji Shayeb Kayem, the role of internal oversight in reducing the threats of the automated accounting information system to achieve value for the organization and customer, doctoral thesis, Faculty of Management and Economics - University of Baghdad, 2008.

Alfaraj M. Hussain, and Qin S, (2011), "Operationalising CMMI: integrating CMMI and COBIT perspective," Journal of Engineering, Design and Technology, Vol. 9 Iss 3 pp. 323 – 335.

Arens A, Elder RJ, Beasley (2012) ''Auditing and Assurance Services: An Integrated Approach'' 14th edition. Pearson Prentice Hall.

De Haes, S., & Van Grembergen, W. (2015) ''Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5'' Second Edition, Springer International Publishing Switzerland.

Fazlida, M.R., and Said, J., (2015) "Information Security: Risk, Governance and Implementation Setback," Procedia Economics and Finance, Vol. 28, pp. 243–248.

Hamdan Allam Mohammed, Anousah Mohammed Salameh, and Al-Utaibi Mahmoud Hosni. (2012). The impact of the royal structure on the level of investment in information technology and its impact on the performance of Jordanian banks: an analytical study for the period 2008-2003. Journal of the Islamic University: Economic and Administrative Studies, Volume (20), Issue (2), p. 381-416.

Hardy, G. 2006, "Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges," Information Security Technical Report, vol. 11, no. 1, pp. 55-61.

Haseley, S. & Brucker, J. 2012. Assessing IT Governance: Considerations for Internal Audit. Journal of the Association of Healthcare Internal Auditors, 31(2): 54-58

Iliescu F M. (2010), Auditing IT Governance. Economic Informatics. 14(1): 93-102.

ISACA. (2007). COBIT 4.1. Retrieved from www.isaca.org

ISACA. (2012). COBIT 5 . Retrieved from www.isaca.org

Khalil, Mohammed (2005) "The role of corporate governance in achieving the quality of accounting information and its implications for the stock market - Applied Theory Study," Journal of Business Research Studies, Year 25, First Issue of Zagazig University.

Messier, W.F.; Glover, S.M.; Prawitt, D.F. (2008) Auditing and Assurance Services A Systematic Approach, 6th Ed., McGraw Hill Irwin, New York

Mirela, G. (2010). Audit Methodology for IT Governance. Informatica Economic, 14(1), pp 32-42.

Moeller, R. R. (2013). *Executive's guide to IT governance: improving systems processes with service management, COBIT, and ITIL* (Vol. 637). John Wiley & Sons.

Pramod, V., Li, J., & Gao, P. (2012). A framework for preventing money laundering in banks. *Information Management & Computer Security*.

Rubino, M., & Vitolla, F. (2014). Corporate governance and the information system: how a framework for IT governance supports ERM. *Corporate Governance*.

Rubino, M., & Vitolla, F. (2014). Internal control over financial reporting: opportunities using the COBIT framework. *Managerial Auditing Journal*.

Sigler, K. E., & Rainey III, J. L. (2019). *Securing an IT Organization Through Governance, Risk Management, and Audit*. Auerbach Publications.

Tuttle, B., & Vandervelde, S. D. (2007). An empirical examination of CobiT as an internal control framework for information technology. *International Journal of Accounting information systems*, *8*(4), 240-263.

Van Grembergen, W., & De Haes, S. (2010). A research journey into enterprise governance of IT, business/IT alignment and value creation. *International Journal of IT/Business Alignment and Governance (IJITBAG)*, *1*(1), 1-13.

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both?. *Computers & Security*, *24*(2), 99-104.

Grembergen, W. (2002, January). Introduction to the Minitrack" IT Governance and Its Mechanisms". In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*.

Walker, A., McBride, T., Basson, G., & Oakley, R. (2012). ISO/IEC 15504 measurement applied to COBIT process maturity. *Benchmarking: An International Journal*. 19,2, 159-176.

Annex No. (1)

Research instrument

Dear professors:

Good greeting

The form in your hands is part of the tagged search requirements (the role of IT Governance in reducing the risk of auditing electronic accounting information systems under the COBIT internal control framework) and this questionnaire, through its questions, aims to identify your opinions on the impact of strengthening IT governance mechanisms and procedures on the external auditor's assessment of the level of audit risk in the ELECTRONIC ACCOUNTING INFORMATION SYSTEMS ENVIRONMENT.

Part 1: Personal information.

Section 1: General information. Please choose the appropriate answer by placing the X signal in the right place:

Branch Manager	accountant	Checker	
			Answer
Scientific qualification	1.Ph.D.		
	2- Master		
	3- Bachelor		
	4- Diploma		
	Another, please mention it.		
Years of practical experience	1- Less than 5 years		
	2- From 5 years to less than 10 years		
	3. From 10 years to less than 20 years		
	4- 20 years and older.		

Section 2: Resolution.

This questionnaire consists of six axes in accordance with the theories and objectives of the study, and you are asked to express your opinions objectively and honestly until the study achieves its objectives.

#	**Paragraphs** **Do you think that having the requirements below helps reduce the risk of auditing electronic accounting information systems:**	**I don't quite agree. 1**	**I don't agree. 2**	**neutral 3**	**agree 4**	**I totally agree. 5**
1	Axis**1: Responsibility and accountability procedures**					
.1	Clear identification and characterization of people who are compromised about various IT activities					
.2	The existence of a written guide to the policies pursued within the bank that clearly describes					

	fair behavior patterns and suspicious behaviors, distributed to customers of electronic information.					
.3	Reports of relatively important unfair behaviors must be prepared and recorded in a special register with the statement of corrective actions in question					
2	**Axis II: Knowledge and communication procedures**					
.4	Established channels of communication with senior management with executives to ensure that management implements the Bank's strategies and objectives					
.5	Information expert reports provided to management outlining current and future business needs as well as appropriate solutions to IT problems					
.6	Periodic reports on its compatibility with the organization's strategy and expected risks and determine the added value of IT investment					
3	**Axis 3: Policy and Plan Actions**					
.7	Periodic evaluation reports are in the IT department for the effectiveness of data source control procedures, data entry, data processing, data transmission, and output control.					
.8	Strict controls on manual data transmission related to confidential and sensitive information for Link.					
.9	Reports from the IT department are submitted to the Department periodically, identifying a record of audit cases that reveal unauthorized network access activities.					
4	**Axis 4: Mechanism and Automation Procedures**					
.10	The Bank has mechanisms that provide electronic solutions consisting of software that enables the Bank to detect and evaluate any unauthorized changes or entry of the system within the entire IT infrastructure and provide immediate and effective corrections					
.11	The existence of database activity audit mechanisms in the bank that can automatically follow up activities and detect gaps in control methods					
.12	Having an integrated software system within the bank that manages a unified database that					

	allows departments and tasks within the bank to share information and communicate it easily and securely					
5	**5th Axis: Skills and Experience Procedures**					
.13	Strict IT recruitment standards including academic background, integrity, and confidentiality					
.14	There is an ongoing review by the Department of Information Technology staff to ensure that they understand and comply with the bank's information system security policies.					
.15	Implementing ongoing training programs for users to improve their skills and knowledge of its developments and provide opportunities for individuals to upgrade their careers					
6	**Axis 6: A procedure related to setting goals and measuring**					
.16	The bank's strategy includes a clear definition of the IT department's objectives for each calendar year, and the IT department's strategy includes adopting the Bank's business plan as a priority for its projects and activities.					
.17	There are annual workshops for branch managers in which Astra will be selected for the next year, and managers will be urged to develop operational plans for the coming year					
.18	A mechanism to determine the effectiveness and efficiency of performance using a measurement system that links IT performance to the organization's objectives, such as a balanced performance card					