

---

Mahdi, Z. R. (2021). IT Governance and Information Security of Accounting Information Systems: A Case Study. *Akkad Journal of Contemporary Accounting Studies*, 1(2), 75-93.

## IT GOVERNANCE AND INFORMATION SECURITY OF ACCOUNTING INFORMATION SYSTEMS: A CASE STUDY

**Zahraa Rahim Mahdi**

*University of Kerbala,*

*Kerbala, Iraq*

*E-mail: [mail@mail.me](mailto:mail@mail.me)*

*ORCID*

*Received: January 2021*

*1st Revision: March 2021*

*Accepted: June 2021*

**ABSTRACT.** This paper aims to determine the level of information technology governance available in the commercial bank (Bank Audi - Najaf branch) using the seven components of COBIT represented. These elements constitute principles, policies, frameworks, processes, organizational structure, culture, ethics, behaviors, information, skills, experience, services, and infrastructure. The research uses the statistical method through a survey of administrators and managers in the Audi Bank - Najaf branch to determine the level of information technology governance available and compare it with the COBIT model, a tool for controlling information technology. The results show that applying information technology governance mechanisms in Iraqi commercial banks can reduce audit risks assessed by external auditors, increase the reliability of accounting information systems, and support information security in light of electronic accounting systems. Finally, applying a model to measure information technology governance in Iraqi commercial banks under the framework COBIT will be a standard measure of the level of governance of information technology and help these banks reduce risk.

**JEL Classification:** M40,  
M42, M83

**Keywords:** IT governance, internal auditing, AIS, information security, audi bank

### Introduction

The use of information technology in the accounting and financial fields has led to a steady increase in financial institutions operating in Iraq. Especially in banking sector institutions in the last 10 years, which has increased the interest of academic and professional researchers in studying the means of control and risk, and scrutinizing the electronic accounting systems applied in these organizations. In this echo, risk and control of electronic accounting information systems are at the heart of the audit process in organizations that rely on high-tech information systems in the areas of IT audit and financial auditing. In addition to IT governance, some recent studies in the field of it environment auditing have emphasized the role of IT governance mechanisms in achieving the organization's objectives. The effective application of IT governance helps to ensure that information technology helps achieve the objectives of organizations and improves the effectiveness of investing in them. Maximizing returns from

the use of information technology leads to improved productivity and increased competencies and largely depends on how it risks are managed, how it is measured and its performance evaluated. COBIT's internal control framework improves the quality of auditing electronic accounting systems.

## 1. Literature review

In addition to the security of financial information disclosed in financial statements, researchers also looked into the relationship between the internal control system, money laundering, and the effectiveness of governance mechanisms applied to electronic accounting information systems, among other aspects of the research. Reducing electronic financial manipulation through IT governance systems reduces the danger of information security in government entities. As a result of IT governance concepts, objectives, and standards, e-government systems are less susceptible to electronic financial manipulation and information security needs are met. As for Vandervelde & Tuttle's research (2007) Test Frames were fired at. Its theoretical framework is applied to IT governance. COBIT Including operational audits, compliance audits, and other aspects of internal control. Systems and procedures, as well as an audit of the company's finances. The findings of this study demonstrate that moaning is common. There are several advantages to searching for examinations in the Academy for the audit profession. As a guide for policymakers that want to promote or not promote current audit applications. she demonstrated An application framework is linked to the results. COBIT The calendar and internal control of the company. Operational risk as a whole COBIT In the digital age, accounting is done electronically. Moaning was also seen in the results. COBIT framework Perhaps he complains about the actions of Dom Liltenb Auditors in giving IT audit support. Related information and technology control objectives were tested in the Abu-Musa study (2009), which was based on the COBIT framework. Only a few firms have confirmed that IT governance systems have been adequately implemented. COBIT implementation is more popular in banking and service firms than other industries, as well as among IT professionals, auditors and executives who are more aware of the need of applying the framework than those who are less familiar with it, according to the findings. Using the COBIT framework procedures for information control and related technologies, Pramod, Li, and Gao (2011) established a framework to prevent money laundering in banks. Based on electronic accounting system control procedures and methodologies. While she was interested in studying Ruby & Vitolla (2014b) The perils of system administration can be mitigated through IT governance. Clarification of Project ERMI was the topic of this investigation. How to aid your goals. Information and technology are in charge. Its goals can be seen by firms that are linked to it. Integrating system management into the process A framework for assessing project risks. COBIT is a framework for internal auditing. And I have demonstrated this, as well. Results Moans of exhaustion are heard throughout the classroom. Incorporation of the COBIT framework into a frame work COSO ERM Represents a sigh of relief The route to any organization Good to attain your goals Censorship of the Ministry of Interior and the management of the government. In addition to a company's policies and procedures, there are risks. A theoretical framework for information security threats, governance, and challenges to its application was developed in the Fazlida & Said research (2015). Following this, it can be concluded that the current study is distinct from previous studies in that it emphasizes IT governance mechanisms in Iraq's banking sector because of its usefulness in supporting information security and increasing customer confidence, as well as the current study focuses on the role of IT governance in reducing the risk of auditing electronic accounts.

There has been an increase in interest in the concept of IT governance in recent years, making it an important area of discussion in the field of information technology. For example,

according to an IT Institute report, the Board of Directors and Executive Management are responsible for overseeing the company's governance, which includes the board's oversight of governance as well as its governance structure, procedures, and leadership (Mirela,2010:33). Information governance, according to Van Grembergen (2002), 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 are made up of people from many walks of life. As part of an organization's overall strategy, IT governance focuses on ensuring that IT procedures and projects are aligned with those requirements.

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 of the NSB.

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 Strategic Compatibility. 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 value saving. 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 are 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 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 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 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.

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 IT 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 it audit, where this framework underwent a further development process under which it became a comprehensive framework for IT 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 it 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 IT beneficiaries.

In this context, the fifth version of the COBIT framework identified the principles of internal control (De Haes and Van Grembergen, 2015:104) of five basic principles outlined in figure (1) as follows:

1. Meeting Stakeholder Needs users needs -This principle means that COBIT 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 adapt the IT objectives used to meet their objectives. However, the challenge for organizations is how to achieve this compatibility between the organization's and IT goals, which has led many researchers to seek a work guide to understand how the organization's objectives can affect relevant IT goals and vice versa.

2. Covering the end-to-end coverage of the Enterprise End-to-end project – 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 the IT function but also treats information and related techniques as assets that should be treated as any other asset in the organization.

2.2. It takes into account all IT 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.

3. application frame Integrated work Applying an Integrated Framework – There are many good IT standards and applications, each of which provides a work guide for a subset of IT activities, and a framework COBIT. On coordination and conform to other appropriate standards and frameworks to create a unified approach, and therefore the framework COBIT. It serves as a comprehensive framework for governance and IT management in the organization.

4. Enabling the comprehensive portal 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. It 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.

Audit risks are defined as risks related to the auditor's failure by inadvertently modifying a number appropriately on financial statements that are essentially fundamentally flawed. The second field work criteria requires 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., 2012:259).

This model is usually formulated as follows:

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

Where:

PDR= Planned Discovery Risks

AAR= Acceptable Audit Risks

AND= inherent risks

CR= Control Risks

1. Planned Detection Risk risks are the risks that proof of a particular part or 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 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.

2. Inherent 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 the results of the audit in previous years. Inherent risks are inversely associated with the risks of planned discovery and directly with the amount of audit evidence.

3. 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.

4. Acceptable Audit Risk. risk 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. Fundamental errors.

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 high-quality audit. An effective internal control system contributes to reducing audit risks, particularly in electronic accounting systems that adopt advanced information technology. The 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.

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 a 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 behaviour within the organization.

2. Awareness and Communication. A range of governance 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 Expertise skills 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 section 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**

### ***Research problem***

Despite the role played by electronic accounting systems and their computerized application programs in facilitating the financial reporting process of companies, their emergence has been accompanied by increased risks of information security, through the penetration of information systems or attempts to manipulate accounting information, especially in the financial sector. On this basis, the problem of research lies in the need to demonstrate the importance of applying IT governance mechanisms in enhancing the security of electronic accounting systems. Assess the role of strengthening IT governance mechanisms in enhancing the quality of auditing under electronic accounting information systems.

### ***The importance of research***

The optimal use of information technology in the accounting and financial fields has led to increased interest in the control of electronic information systems. The risks to these systems may lead to a loss of confidence in accounting information and substantial errors in the measurement process. In addition to damaging the reputation of financial institutions and their

relationship with their customers. Control of INFORMATION technology governance and the provision of security and protection are critical to reaching the objectives of the banks they apply. Accordingly, the importance of research stems from the importance of the risk assessment process associated with electronic accounting information systems. The auditor's assessment of audit risks affects the way audit tasks are performed, and the quality of auditing in general. In addition, assessing the risks of auditing accounting information systems is an essential element of IT audits.

### ***Research goals***

The research aims to achieve the following:

1. Clarify the importance of implementing IT governance mechanisms in enhancing information security under electronic accounting systems
  - 2Theoretical statement of the COBIT framework for internal control of electronic information systems.
- Assess the role of IT governance and its impact on the quality of auditing electronic accounting systems.

### ***The research hypothesis***

The study is based on one key hypothesis that:

"There is a statistically significant correlation between the strengthening of the bank's IT governance and the quality of auditing electronic accountingsystems", and this hypothesis is derived from the sub hypotheses:

The firstsub-hypothesis/ Ho1 there is a statistically significant relationship between the variable principles, policies and frameworks for information technology and the quality of auditing of electronic accounting systems.

The second sub-hypothesis / Ho2 there is a statistically significant relationship between the process variable of information technology and the quality of auditing of electronic accounting systems.

Sub-hypothesis III /Ho3 there is a statistically significant relationship between the variable organizational structure of information technology and the quality of auditing of electronic accounting systems.

Sub-hypothesis IV / Ho4 there is a statistically significant relationship between the variable culture, ethics and behaviors of information technology and the quality of auditing electronic accounting systems.

Sub-hypothesis V/Ho5 has a statistically significant relationship between the information variable for information technology and the quality of auditing electronic accounting systems.

Sub-hypothesis VI / Ho6 there is a statistically significant relationship between the service variable, infrastructure,and applications for information technology and the quality of auditing of electronic accounting systems

Sub-hypothesis VII /Ho7 there is a statistically significant relationship between the individual variable, the skills and competencies of information technology and the quality of auditing electronic accounting systems. .

### 3. Results

In this study, the main and sub-research hypotheses are analyzed and tested using a five-weight(Likert)scale, which is distributed from its highest weight, which was given (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 agree) and among them three other weights are The distribution of resolution paragraphs to the major research axes is depicted in Table 1.

**Table1Distribution of resolution paragraphs**

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

#### *The sincerity and stability of the scale*

It was decided to use the Cronbach Alpha laboratories to ensure the stability and internal consistency of the paragraphs of this measure in order to verify the sincerity of the measurement tool represented by the questionnaire, which was presented to a group of professors from the Faculty of Management and Economics at Kufa University and their observations and suggestions on how to improve the resolution were taken into consideration. Table 2 shows that the value of the Kronbach Alpha stability factor exceeded the acceptable 60 percent acceptance rate for the research outcomes as well as for all study variables, as demonstrated by the value of the stability factor.

**Table2 Stability of the Study Scale**

Variable	Shortcut	Value of Alpha
Strengthening IT governance	<b>X</b>	<b>.849</b>

Responsibility and accountability	$x1$	<b>.861</b>
Knowledge and communication	$x2$	<b>.883</b>
Policies and plans	$x3$	<b>.887</b>
Mechanisms and mechanisms	$x4$	<b>.865</b>
Skills and experience	$x5$	<b>.888</b>
Goals and measurement	$X6$	<b>.901</b>
<b>All variables</b>		<b>.892</b>

### *The sample selection*

The research sample consisted of Iraqi commercial banks operating in Najaf province, because the commercial transactions of the banking sector are carried out through electronic accounting systems, and thus can be used to test the role of information technology governance mechanisms in reducing the risk of the audit process, which was the primary goal of the research. So, 60 questionnaires were issued to sample members at all administrative levels, as well as to accountants, auditors, and branch managers. Of the 60 questionnaires disseminated, 48 forms were recovered, representing an 80 percent recovery rate.

### *Description and analysis of sample characteristics*

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

**Table3 Demographics of the Search Sample**

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

### Hypotheses test results

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

H0 Hypothesis of Nothingness: "There *is no statistically significant relationship between strengthening the company's IT governance and reducing the risk of electronic accounting information systems auditing*"

H1 Alternative Hypothesis: "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

For the six variables studied, Table 4 reveals that all variables had moral levels of nil, and that averages exceeded the default value of three. According to these findings, the research variables have favorable effects on increasing corporate governance and lowering audit risks associated with electronic accounting information systems. The dangers of auditing computerized financial systems.

Pearson's simple link coefficient was used to examine each sub-hypothesis independently to establish the amount of correlation between the study variables and the audit risk checker's assessment level. The outcomes of the study's sub-hypotheses testing are as follows:

#### 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 Hypothesis of Nothingness: 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 Hypothesis of Nothingness: 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 Hypothesis of Nothingness: 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 variable 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).

And Refer These results. into 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 into The power of the relationship Between the two variables, Which indicates that 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 Hypothesis of Nothingness: 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 its 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 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 Hypothesis of Nothingness: 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	.704**	1
	Correlation		
	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 skill 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 correlation coefficient 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 Hypothesis of Nothingness: 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	1	.624**
	Correlation		
	Sig. (2-tailed)		.000
	N	48	48
X6	Pearson	.624**	1
	Correlation		
	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 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 its 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 means, greatly help reduce the risks inherent in the terms of the financial disclosures, and the existence of an integrated database management software system will contribute to. There is no doubt that it facilitates and secures the transmission of information within the system, thereby reducing the risk of penetration or manipulation of 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 behaviours contribute to creating an environment that supports fair behaviour within the organization, which reflects positively on the level of confidence in the system applied as a whole.

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 variable is 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

The implementation of information technology governance procedures leads to the reduction of financial manipulation in the context of electronic accounting systems. It is more effective to use IT governance mechanisms in electronic accounting systems when they are implemented as part of the COBIT internal control framework. The implementation of the COBIT internal control framework results in a reduction of information security risks in the context of electronic accounting information system. As a consequence of the increased intensity of controls implemented in the organization as a result of the implementation of the COBIT framework, accounting information consumers have more trust in their financial statements. In addition to enhancing the quality of external auditing and lowering audit costs, establishing an adequate environment for internal control in electronic accounting information systems through the use of IT governance mechanisms may help minimize audit expenses. The results of the statistical analysis of the responses of the sample members revealed a positive and statistically significant relationship between strengthening information technology governance and lowering the risk of electronic accounting information systems auditing, according to the findings. The findings from the field revealed a positive and statistically significant relationship between components of information technology 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, according to the researchers. When the research hypotheses were tested, the results revealed a disparity in the impact of IT governance procedures on the risks of auditing at the level of sub-variables, with the greatest impact being had by the variable mechanisms and its mechanisms, followed by policy and plan variables, responsibility and accountability, skills and experience, knowledge and communications, and finally the variable objectives and measurement, while the least significant difference was found to be between the variable objectives and measurement and the variable objectives and measurement. Company owners and operators of electronic accounting information systems environments, particularly national banks in Iraq, should adopt the COBIT internal control

framework to ensure that companies have sufficient confidence in the applicable accounting system and to improve information security within the system. As recommended by the researcher, an independent Iraqi internal control body should be established that will issue binding instructions to companies in order for them to adopt governance standards that are commensurate with their needs, taking into consideration both the nature of their activity and the level of complexity in their operations. Iraqi enterprises should establish tight guidelines for choosing workers who work in the information technology department, in order to ensure that the company produces cadres who are scientifically and behaviorally equipped to operate in the field of IT. As a consequence of the continual development of means of hacking electronic systems or attempting to manipulate their information, there is a pressing need to work on the creation of effective means of continuously reviewing the mechanisms of control of information technology implemented in businesses. The researcher advises that future studies in the field of assessing the efficacy of internal control systems be conducted using the COBIT and COSO frameworks for internal control, which are currently being developed.

## 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.
- Al-Alarkapi, Naji Shayeb Kayem, 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.
- 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.
- 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.
- 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
- 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.

- 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](http://www.isaca.org)
- ISACA. (2012). COBIT 5 . Retrieved from [www.isaca.org](http://www.isaca.org)
- 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., (2013) ‘ ‘ Executive’s Guide to IT Governance Improving Systems Processes with Service Management, COBIT, and ITIL’ ’ John Wiley & Sons, Inc.
- Pramod, V., Li, J., and Gao, P., (2012),"A framework for preventing money laundering in banks", Information Management & Computer Security, Vol. 20 Iss 3 pp. 170 – 183.
- Rubino, M. ,and Vitolla, F. , (2014a) "Corporate governance and the information system: how a framework for IT governance supports ERM", Corporate Governance, Vol. 14 Iss 3 pp. 320 - 338
- Rubino, M. ,and Vitolla, F. , (2014b) "Internal control over financial reporting: opportunities using the COBIT framework", Managerial Auditing Journal, Vol. 29 Iss: 8, pp.736 – 771
- Sigler, K. E., and Rainey, J.L., (2016) ‘ ‘ Securing an IT Organization through Governance, Risk Management, and Audit (Internal Audit and IT Audit)’ ’ Taylor & Francis Group, LLC
- 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. (2009). Enterprise governance of IT: Achieving strategic alignment and value . New York: Springer.
- Van Grembergen, W., 2002, Introduction to the minitrack IT Governance and its Mechanisms, Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS).
- Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both?. Computers & Security, 24(2), 99-104.
- Walker, A; McBride, TM; Basson, G; Oakley, R, (2012),"ISO/IEC 15504 measurement applied to COBIT process maturity", Benchmarking: An International Journal, Vol. 19 Iss 2 pp. 159 – 176.