# Impact of COSO and COBIT5 Regulatory Integration in the Correct Application of Cyber Governance in Jordanian Commercial Banks

**Professor Dr. Osama Abdel Munem Ali**

**Abstract**

*This study aimed to demonstrate the effect of the regulatory complementarity of COSO and COBIT5 decisions on the correct application of cyber governance in Jordanian commercial banks. The study population included Jordanian commercial banks, whose number until the end of 2019 was (13) banks. Due to the limitations of the study population, a comprehensive survey method was adopted in determining the study sample, as the study sample included the entire population of the study. The researcher also used the proportional stratified sampling method for the purposes of representing the study population, so that it included selecting a sample of individuals working at the upper and middle administrative levels in Jordanian commercial banks. And To answer the questions and hypotheses of the study, the Statistical Package for Social Sciences - SPSS was used, and linear correlation and hierarchical regression analysis were used to choose the study hypotheses. Many results were reached, the most important of which was that the supervisory complementarity of the decisions of the COSO and COBIT5 Committee exists in the correct application of cyber governance in Jordanian commercial banks. Management in a timely manner, and taking into account the needs and requirements of users of information and communication systems when updating the internal control system according to the directions of the COSO and Cobit 5 decisions, in order to achieve the correct application of cyber governance in it.*

**Key words:** COSO Committee: COBIT5 Committee: Cyber Governance: Jordanian Commercial Banks

**Introduction:**

The existence of an effective and integrated system for risk management and internal control is considered a major factor in establishing a good and correct system for implementing cyber governance within commercial banks, and a basic indicator to support and strengthen the comprehensive control exercised by the board of directors, the board of managers or the supervisory board according to the style or type of management that the banks choose to conduct their affairs. Given the importance of having control tools that control and monitor the work of information systems and technology in banks, it was imperative to adopt supervisory frameworks that govern information technology in banks, and from these frameworks, which are called the term COBIT: Control Objectives for Information and Related, where the COBIT framework is considered. IT risk management is important for both managers, And auditors, and users to understand the information technology systems that belong to their banks, as well as help in developing the correct application of cyber governance in them. Also, there must have been another supporter for these supervisory systems and their activities within banks, which enables the existence of a supervisory system that integrates with the **COBIT** system and this system is (COSO)and It is considered an integrated internal control framework, which aims to provide guidance for assessing and strengthening control systems and promoting the correct application of cyber governance as well. Based on the foregoing, the current study has worked on demonstrating the regulatory complementarity effect of the decisions of the COSO Committee and COBIT 5 on the correct application of cyber governance in Jordanian commercial banks.

**The study's Problem:**

Clear controls and frameworks must be in place to measure the extent to which Jordanian commercial banks accomplish their business using advanced information technology, which will help their internal control bodies to perform their work better than before by using the (COBIT 5) framework for information technology systems and developing cyber governance work. Especially if there is a regulatory integration with the COSO system, which undoubtedly will lead to highlighting the correct application of cyber governance in it, so the study problem crystallizes with the following questions: The first main study question: Is there a statistically significant effect at a significant level ($\alpha \leq 0.05$) for the supervisory integration of the decisions of the COSO Committee (control environment, risk assessment, control activities, information and communication, and control) and COBIT5 (planning and organizing, acquisition and implementation, support and delivery, Monitoring, evaluation, mentoring and monitoring) in the correct application of cyber governance in Jordanian commercial banks.

The second main study problem The question of the second main study: Is there a statistically significant effect at a significant level ($\alpha \leq 0.05$) for the supervisory integration of the decisions of COBIT5 (planning and organizing, owning and implementing, support and delivery, monitoring and evaluation, direction and control) and COSO (control environment, risk assessment, activities Supervision,

Information and Communications, and Monitoring) in the correct application of cyber governance in Jordanian commercial banks.

**Study hypotheses:**

The study is based on the following assumptions:

The hypothesis of the first main study The first main hypothesis, H01, states that: There is no statistically significant effect at a significant level ($\alpha \leq 0.05$) for the supervisory integration of decisions of COSO (control environment, risk assessment, control activities, information and communication, and control) and COBIT5 (planning and organizing, owning and implementing, Support, delivery, monitoring and evaluation, guidance and monitoring) in the correct implementation of cyber governance in Jordanian commercial banks.

The hypothesis of the second main study The second main hypothesis H02 states that: There is no statistically significant effect at a significant level ($\alpha \leq 0.05$) for the supervisory integration of the decisions of COBIT5 (planning and organizing, owning and implementing, support and delivery, follow-up and evaluation, direction and control) and COSO (control environment, evaluation Risks, supervisory activities, information and communication, and monitoring) in the correct application of cyber governance in Jordanian commercial banks.

**The Study Approach**

The researcher relied on the descriptive and analytical approach to describe and analyze the phenomenon under study represented by the supervisory integration of COSO and COBIT5 in the correct application of cyber governance in Jordanian commercial banks. which was reached from analyzing the data received from the given questionnaire and finding the correlation between the variables and the ideas that are being discussed around it and the procedures That they contain and the effects they induce

**The type and nature of the study :**

The field survey was relied upon in the process of collecting the primary data for this study, so this study is, in terms of purpose, a field and illustrative study, as it works to discover the effect between the variables, and it is also considered deductive in nature as it is based on previous studies

**Survey's strategy:**

Sampling was used in order to know the variables that cause the existence of the phenomenon to reach the effect and the result, and to study the current facts related to the nature of the phenomenon.

**Population and study sample**

The population of the study included Jordanian commercial banks, whose number until the end of 2019 was (13) banks. Due to the limitations of the study population, a comprehensive survey method was adopted in determining the study sample, as the study sample included the entire population of the study. The researcher also used the proportional stratified sampling method for the purposes of representing the study population, so that it included selecting a sample of individuals working at the upper and middle administrative levels in Jordanian commercial banks.

**Unit of analysis**

The inspection and analysis unit consisted of individuals working at the higher administrative levels (general and executive directors), and middle administrative levels (directors, heads, units and departments of financial management, internal control and audit department, information technology management, and risk management) in Jordanian commercial banks, who numbered (383) Employees. Which were determined by relying on the uma sekaran sample size table, the researcher distributed (383) questionnaires to the members of the study sample, and retrieved (341) questionnaires, of which (21) were unfit for analysis, so that the researcher had (320) questionnaires valid for analysis, and a retrieval rate that reached (83.6%) of the total collected questionnaires, which is a statistically acceptable percentage.

**Data collection methods**

The study relied on collecting data on two sources: First: Secondary sources: represented, articles, scientific periodicals, research papers, reports, publications and previous studies, whether Arab or foreign, which dealt with the topics and dimensions of the current study variables, with the aim of taking a general perception about the subject of study, and being familiar with the latest developments that received the topics of the study.

Second: The primary sources: represented by the main study tool (the questionnaire), which was designed to achieve the purpose of the study, so as to cover all aspects addressed by the theoretical framework, questions and hypotheses on which the study was based.

The questionnaire included a number of paragraphs that reflect the study variables and their dimensions, and the questionnaire included three parts, as follows: The first part: the components of internal control according to the COSO model, which included (control environment, risk assessment, control activities, information and communication, and monitoring). The second part: the COBIT5 system, which included (planning and organizing, owning and implementing, support and delivery, monitoring and evaluation, direction and control). Part Three: Cyber Governance, which included (cybersecurity governance requirements, cybersecurity program, cybersecurity policy, cyber information security management, and assessment and management of cyber risks).

**The theoretical side**:

The concept of internal control according to COSO The word COSO is the abbreviation for The Committee of Sponsoring Organization of Treadway Commission, which means the Committee of Sponsoring Organizations emanating from Treadway. Founded in 1985, COSO is a joint initiative of five private sector organizations dedicated to providing leadership thinking through the development of frameworks and guidelines on Enterprise Risk Management (ERM).) And internal control, and to deter fraud. Among the organizations supporting COSO: (COSO, 2020)

1. Institute of Internal Auditors, IIA.
2. The American Institute of Certified Public Accountants (AICPA).
3. American Accounting Association AAA.
4. The Institute of Management Accountants IMA.
5. FEI Financial Analysts Institute.

Whereas, the COSO Committee issued in 1992 a report containing comprehensive perceptions of the concept of internal control and its evaluation, as the COSO Organizational Committee defined internal control as a process affected by the Board of Directors of the company, the executive management and all concerned personnel in the company, the main objective of which is to provide reasonable assurance and guarantee. That the control objectives relating to operational processes, financial reportingand compliance have been achieved.

**COSO, 2012)**

**The audit objectives are as follows**: (Hamdan, 2018) (AL Shammari & Khalawi, 2018)

1- Objectives related to the effectiveness and efficiency of operational processes
2- Objectives related to reliability and accuracy of financial reports
3- Objectives related to applicable laws, regulations and instructions that the company must abide by. Components of an internal control system according to COSO

The internal control components include five main elements according to the COSO report: (Majeed, 2019) (Ahmad, 2017) (Al-Husseini and Al-Sabry, 2017) (COSO, 2014)

**First: Control Environment**: The control environment is the basis upon which internal control is practiced in the company, and the control environment is represented by a set of standards, policies and procedures that define the direction of the company and the views of the Board of Directors and management regarding the importance of internal control.

**Second: Risk Assessment**: All companies are exposed to many risks, whether these risks are from inside or outside the company, regardless of the nature of their work or their size, and since all components of internal control, from the control environment to the follow-up, must be subjected to the risk assessment that Included in it, and with an understanding of the nature of the work, the company will be able to gain insight into the internal and external factors and their impact on risks, identifying and assessing these risks that may affect the company's achievement of its objectives, and then the company will then choose the appropriate responses to these risks and monitor performance for change. COSO, 2020)

**Third: Control Activities**: The control activities are represented in the control procedures over the activities of the procedures and policies that help in ensuring the management and implementation of the directives issued by the higher management through monitoring the operations that occur throughout the company. It also helps to ensure that the necessary measures are taken to confront the risks that are exposed to achieve the goals of the company.(Saleh, 2014)

**Fourth: Information and Communication**: These are continuous, iterative systems or processes to obtain and share information throughout the company. The company makes use of information systems to capture, process and manage data and information in a form and time frame that enables people to carry out their responsibilities.(COSO, 2020)

**Fifth: Monitoring:** The internal control system in the company often changes, and the company's objectives and the components of the internal control system may also change over time, and the procedures may also become less effective and outdated, and they may not be published or distributed in the way that was chosen or developed, or they may be considered unjust. Sufficient to support the achievement of new or updated goals. Whereas, monitoring activities are selected, developed and implemented to ascertain whether each component of internal control is still in place and functioning or if there is a need for change, and monitoring activities provide valuable inputs for management to use when determining whether the internal control system is appropriate and capable of addressing new risks. (COSO, 2014)

**Benefits of the internal control system:** (COSO, 2012)
The internal control system provides many benefits to the company, as it provides management and the board of directors with more confidence regarding achieving goals, provides feedback on how the company operates, and helps to address and manage emergency events. One of the most important benefits that an effective internal control system provides to many companies is its ability to meet specific requirements for access to capital markets, and to provide innovation that is driven by capital and economic growth. Such access comes with responsibilities for providing reliable and timely reports to shareholders, creditors, capital providers, and entities. For example, effective internal control supports reliable external financial reporting, which in turn contributes to enhancing investor confidence in providing the required capital.

**The concept of information technology governance**

Hussein and Khalaf (2019) defined IT governance as: Instructions, laws and rules whose implementation is the responsibility of both the board of directors and the executive management in order to achieve control over information technology risks and work to increase the return on spending on them, in addition to achieving correlation and harmony between the company's strategy And information technology strategy, which works to achieve a competitive advantage for the company, add value to it, and effectively achieve its goals.

While Al-Hammoudi defined the essence (2019) of IT governance as: the process of arranging and strategically aligning information technology in a way that is consistent and in line with business activity, and as a result of this arrangement the highest value of business activity is achieved by developing effective and permanent control of information technology to ensure accountability and management Risk and performance.

As for (Haes & Grembergen, 2015: 123), he defined information technology governance as: the processes, organizational structures, and organizational leaderships that work to ensure the sustainability of information technology in a way that works to achieve the goals and strategy of the company.

**The importance of IT governance according to COBIT 5**

The importance of COBIT 5 is illustrated by the following: (Zambrano, 2017)

1- Maximizing the value of the company through achieving and maintaining balance, whereby levels of risks are reduced and benefits are achieved in addition to the use of resources.

2- The rules and principles of information technology governance can be adhered to in all establishments of various sizes, types and objectives.

3- Supporting the activities related to information technology and achieving maximum efficiency, which would achieve high levels of consistency in the system within the company.

4- Facilitating the work of the supervisory authorities within the company, including internal auditors and audit committees, and supports the work of the Board of Directors, and facilitates the work of the external auditor.

5- Develop general and detailed instructions for all information technology operations and activities.

6- Finding a common language for all concerned parties, and drawing and specifying directives related to achieving a common goal.

7- Linking the needs of stakeholders with the needs of the company, by arranging goals and priorities, in order to focus on important issues regardless of the limited resources or their abundance.

**IT fields and controls according to COBIT 5**

The framework of COBIT 5 provides a sound approach to the completion and implementation of IT governance processes, and it has identified 34 control processes on information technology that contain more than 300 control objectives that are evaluated in four areas: (Megasyah & Arifnur, 2020) (Hussein and Khalaf, 2019) (Al-Basri)And Muhammad, 2019)

**First: planning and organizing**

This field covers strategies related to knowing the way in which information technology can make the best contribution to achieving the objectives of the company's activities, in addition to knowing the strategic vision that must be communicated, achieved and managed in relation to various aspects of information technology in addition to preparing the correct organization and laying the infrastructure for information technology. In its right place, and since this field includes ten goals, its main goal is the strategic alignment between the company's business and technology, by having a minimum level of planning (short, medium term), providing the company with the organizational structures of the technology apparatus, and carrying out communication regarding Technology strategies with business partners and departments, in addition to the company providing human resources policies that relate to the IT team, information security policy, and quality policies that relate to technology.

**Second: possession and implementation**

In order to form a strategic vision on information technology, this requires knowledge of the solutions that are provided from information technology, and work to own and develop them, and to be implemented in a way that ensures integration within the processing operations of the company's activities, in addition to that this vision must include the perpetuation of systems and changes that areRelated to it in order to verify its continuity in meeting the solutions set for the objectives of the company's activities.(Megasyah & Arifnur, 2020)

**Third: Delivery and Support**

This field is concerned with the actual provision of required services, working to manage the security of services and the continuity of their provision to users, and the management of operational facilities and data. This area includes achieving governance during the provision of information services, whether these are logistical services or services of a purely technical character, and working to support users. It also includes managing processes related to the continuity of information services, service agreements and contractors, in addition to managing arrangements or settings related to system and device variables To be tuned in order to work with each other in harmony, it also includes employee training and skills development, emergency events and risk management, performance improvement, and quality management: (Hussain & Khalaf, 2019)

**Fourth: Monitoring and evaluation**

All processing according to information technology requires that these technologies be accessed according to regular contexts regarding their compliance with control requirements and regarding their quality. This field is concerned with addressing aspects related to internal control follow-up, compliance with legislation, performance management, and provision of governance, as these objectives include improving the level of technical procedures and evaluating them, and implementing internal and external audits periodically in order to work to ensure compatibility with the policies and requirements chosen for application Al-Basri & Mohammed, 2019)

Fifth: Direction and control. Monitoring is the collection and analysis of information related to a project or program and takes place during the implementation of the project or program. As for the calendar, it is the periodic evaluation of an organization, project, or program that may be conducted internally or by external independent evaluators. This determinant includes the following targets (Abdelbasset, 2014):

**Cyber governance: its concept, importance and goal**

The concept of cyber security governance.

Some researchers believe that the concept of cyber governance revolves around the data of electronic governance in companies and banks, so we find that (Saleh and Al-Saleh, 2018) defined it as a set of mechanisms that include drawing the strategic direction of the organization, to control the variables of its internal environment, meet its requirements and prepare to face the variables of its external environment and adapt to it

As for (Al-Saeed, 2019), he considers that what is meant by governance in the context of cybersecurity is that it is the principles, administrative rules and methods used in an entity to control decision-making powers and identify those with responsibility and accountability in carrying out the tasks and duties related to protecting the entity from cyber attacks or misuse of information assets, while ensuring Continuity of operations in the event of accidents or disasters. Accordingly, the cybersecurity governance aims to direct, monitor, guide and improve the decisions and actions of individuals to raise efficiency and facilitate coordination of efforts between the relevant authorities, in line with the direction and aspirations of the stakeholders in the entity (internal factors), and in a manner that does not contradict the agreements and laws to which the entity is a partof (external factors) .

**Factors affecting the design of cybersecurity governance programs in banks**: The prevailing culture of cybersecurity in the corridors of the entity is affected by the style of governance followed by its higher management, whether this is documented in its systems, policies and regulations, or practiced without documentation.

When designing a cybersecurity governance program, three main levels must be taken into account: First, the responsibility for defining the security vision and priorities, and this task is often assigned to the Cybersecurity Supervisory Committee. Second, the responsibility for defining the programs and implementation mechanisms is assigned to the director of cybersecurity in the entity and their work team. Third, the responsibility for implementing and following up the initiatives and programs is assigned to the various departments and divisions in the entity each according to their job duties and role in achieving the general vision of cybersecurity (Al-Saeed, 2019)

The importance of cybersecurity for banks: One of the most important reasons for the necessity of having a cybersecurity concept and calling for creating legislative and regulatory frameworks commensurate with the challenges faced by society or organizations and banks It can be summarized as follows: (Abd Al-Reda and Al-Mamouri, 2020)

1- The need to be linked to communication systems and the Internet, and the inability to isolate devices from the local networks and large-scale networks they need

2- The reliance of various institutions and banks on the effectiveness of information, which increases with the increase in technological developments and with the increase in the requirements of these institutions and banks.

3- The difficulty of challenging and controlling dangers or following criminals and punishing them, due to the lack of geographical borders when using the Internet and electronic communications because they provide an opportunity to penetrate spatial borders.

4- The steady growth in electronic uses and applications, and the emergence of electronic commerce, network shopping, e-government and electronic management, which need a secure information environment.

5- The relationship between security and technology has become a direct relationship with the possibility of exposing strategic interests of a cyber nature to electronic dangers and rethinking the concept of national security, which means protecting the basic values of society, and then it is considered a new tributary to national security.

6- Cybersecurity is concerned with the process of developing standards and procedures to prevent non-peaceful uses of cyberspace and what constitutes threats to global security and information infrastructure. Therefore, state security has become part of collective security.

7- The issue of cybersecurity has become an international issue that requires flexible strategies that are adapted to the continuous changes, whether in security mechanisms or tactics, in exchange for the continuous development of threats.

8- The interest in cybersecurity was not limited to the technical dimension only, but went beyond to other dimensions that have become relevant in explaining the issue, such as the cultural, social, economic and military dimensions.

9 - The role of non-state actors in international relations has increased, which in turn affected the sovereignty of the state, especially with the emergence of technology companies that cross borders.

**Real conditions for cyber governance in commercial banks Based on central bank instructions, 2018 Conditions of cybersecurity governance**:

Banks must adhere to the following (Central Bank of Jordan, 2018)

A- The board of directors, as well as those delegated from its committees and senior executive management, must include persons with appropriate skills and knowledge to understand and manage cyber risks.

B- The council or whoever delegated from its committees shall undertake the following responsibilities and tasks, each according to his position:

1- Adoption of the Cyber Security Policy.
2- Accreditation of the Cyber Security Program.
3- Examine compliance with the cybersecurity policy and program.

C- The higher executive management shall assume the following responsibilities and tasks, each according to his position:

1- Ensuring the application and updating of the cybersecurity policy.
2- Ensuring the implementation of the cybersecurity program so that it is integrated with the general framework for managing information technology risks, and continuing to update and develop it.
3- Ensuring the existence of a comprehensive Cyber Risk Register and ensuring that it is updated continuously and in compliance with the Company's Risk Profile IT.

4- Continuous monitoring of the level of cyber risks.

5- Adopting lists of authorities related to the management of security and cyber risks in terms of determining the entity, entities, person, or parties primarily(Responsible)And that is ultimately responsible (Accountable), and those that are(Consulted), and those that are(Informed), for all Management processes, controlling these risks, controlling and auditing them.
Thus it becomes clear to the researcher the extent of the need for an intellectual integration between the internal control system in light of the applications of COBIT 5 and COSO information technology governance in order to reach the correct application of cyber governance in banks, which needs the following points:

1. Separation of ownership from management.
2. The organizational structure and branching of the project.
3. The government agencies 'need for data and information.

Also, the researcher believes that the use of information technology in accordance with the COBIT5 framework in the process of auditing accounting information systems leads to a reduction in the time spent, thus reducing costs and improving the quality and efficiency of cyber governance in banks. The presence of computer information security risks calls for providing the appropriate degree of information security and electronic protection for information systems. Accounting and internal control systems for banks, so as to ensure that the information technology used in banks helps to achieve its strategy, expand it, achieve its objectives, build relationships and operations to direct it to monitor banks' business in order to achieve its goals by maximizing the results of implementing cyber governance in them, taking into account the balance of risks against The expected return from information technology as a result of the use of the two frameworks of COSO and COBIT 5 in them.

**The practical side:**

Statistical methods used To answer the questions and hypotheses of the study, **the Statistical Package for Social Sciences - SPSS** was used, as follows:

First: Descriptive Statistic Measures: for the purpose of describing the characteristics of the demographic and functional study sample, which include: - The arithmetic mean: to measure the average of the respondents' answers to the paragraphs of the questionnaire. Standard Deviation: to measure the dispersion of the answers from their mean.

Second: Internal consistency coefficient Cronbach Alpha: To identify the stability of the study tool.

Third: Choosing the phenomenon of multiple linear correlation multicollinearity based on the Pearson correlation coefficient: to test the validity of the study model.

Fourth: Hierarchical Regression: To test the hypotheses of the study.

Fifth: The relative importance: which was determined according to the following formula and according to Likert's five-point scale for alternatives to answering each paragraph, where the number of levels are: low, medium, and high.

$$\text{Materiality} = \frac{\text{Alternative Upper Limit - The Alternative Lower Limit}}{\text{The number of levels}} = \frac{\mathbf{5 - 1}}{\mathbf{3}} \quad \mathbf{1.33}$$

Where the level is considered:
Low if the arithmetic average is from -1.00 to less than 2.33.
average if the arithmetic mean was from -233 to less than 3.66.
Increased if it reached the arithmetic average from -3.66 to 5.00

Stability test of the study tool

To test the reliability of the instrument used to measure the variables included in the study, the Cronbach Alpha Coefficient test was used, where the result of the scale is statistically acceptable if the value of Cronbach Alpha is greater than (0.60) (Sekaran, 2006, 311), and the closer The value of (100%) this indicates higher stability scores for the study tool, and by looking at the data presented in the following table, the Cronbach alpha internal consistency coefficient was measured for the study variables and their dimensions and for the study tool as a whole, to see the extent of consistency in the answers And that is as follows:

Table (1): the values of the internal consistency coefficient for the study tool items

| Number | Dimension | Numberof Paragraphs | Alpha value |
|---|---|---|---|
| 1 | Regulatory environment | 9 | 0.817 |
| 2 | Risk assessment | 7 | 0.719 |
| 3 | Regulatory activities | 9 | 0.652 |
| 4 | Information and communications | 9 | 0.761 |
| 5 | surveillance | 7 | 0.668 |
| Components of internal control systems in accordance with the COSO model | | 41 | 0.912 |
| 6 | Planning and organization | 9 | 0.735 |
| 7 | Possession and execution | 6 | 0.724 |
| 8 | Support and delivery | 7 | 0.828 |
| 9 | Follow-up and evaluation | 7 | 0.759 |
| 10 | Guidance and monitoring | 5 | 0.642 |
| COBIT5 system | | 34 | 0.911 |
| 11 | Cybersecurity governance requirements | 7 | 0.732 |
| 12 | Cybersecurity Program | 8 | 0.708 |
| 13 | Cybersecurity policy | 6 | 0.716 |
| 14 | Cyber Information Security Administration | 7 | 0.779 |
| 15 | Cyber risk assessment and management | 4 | 0.686 |
| Cyber governance | | 32 | 0.903 |
| All paragraphs | | 107 | 0.967 |

We note from Table (1) that the values of the Cronbach alpha coefficient of internal consistency for the paragraphs of the study tool ranged from (0.642-0.912), and the value of the Cronbach alpha coefficient for all paragraphs of the study tool was (0.967), and therefore all values are greater than (0.60) and this is an indication of consistency Among the items of the study tool, the reliability of the study tool and its reliability for performing statistical analysis. Description of the respondents' answers The arithmetic means, standard deviations, and ranks of relative importance were relied upon in describing the responses of the sample members to the questionnaire's paragraphs and their axes, and the results were as follows: First: the components of internal control systems according to the COSO model The dimensions included the following: the control environment, risk assessment, control activities, information and communication, and monitoring.

Table (2): Arithmetic averages, standard deviations, ranks and the relative importance of the components of internal control systems according to the COSO model

| Axis | Arithmetic average | Standard deviation | Rank | Relative importance |
|---|---|---|---|---|
| Regulatory environment | 3.87 | 0.535 | 4 | high |
| Risk assessment | 3.929 | 0.484 | 3 | high |
| Regulatory activities | 3.986 | 0.385 | 2 | high |
| Information and communications | 3.856 | 0.462 | 5 | high |
| surveillance | 4 | 0.428 | 1 | high |
| Components of internal control systems in accordance with the COSO model | 3.928 | 0.368 | | high |

Table (2) indicates that the trends of the sample members were towards the high relative importance of the components of the internal control systems according to the COSO model, where the arithmetic mean was (3.928), with a standard deviation (0.368). (4.000), a standard deviation (0.428), and a high relative importance, while the (information and communication) dimension ranked last, with an arithmetic average (3.856), a standard deviation (0.462), and a high relative importance as well. All the dimensions of the internal control systems components according to the COSO model appeared with high relative importance.

Second: COBIT5 systems These risks included the following dimensions: planning and organizing, acquisition and implementation, support and delivery, monitoring and evaluation, and direction and control.

Table (3): The arithmetic means, standard deviations, ranks and the relative importance of COBIT5 systems

| aspect | Arithmetic average | Standard deviation | Rank | Relative importance |
|---|---|---|---|---|
| Planning and organization | 3.927 | 0.484 | 2 | high |
| possession and implementation | 3.928 | 0.572 | 1 | high |
| Support and delivery | 3.848 | 0.659 | 5 | high |
| Follow-up and evaluation | 3.888 | 0.516 | 4 | high |
| Guidance and monitoring | 3.912 | 0.502 | 3 | high |
| COBIT5 systems | 3.901 | 0.432 | | high |

Table (3) indicates that the trends of the sample members were towards the high relative importance of COBIT5 systems, with the arithmetic mean (3.901), a standard deviation (0.432), and after (possession and implementation) ranked first, with an arithmetic mean (3.928), and with a deviationStandard (0.572), with high relative importance, while the (support and delivery) dimension ranked last, with an arithmetic average (3.848), a standard deviation (0.659), and a high relative importance as well.All dimensions of COBIT5 systems appeared to be of high relative importance.

Third: Cyber Governance These risks included the following dimensions: cybersecurity governance requirements, cybersecurity program, cybersecurity policy, cyber information security management, and assessment and management of cyber risks.

Table (4): The arithmetic means, standard deviations, ranks, and the relative importance of cyber governance

| aspect | Arithmetic average | Standard deviation | Rank | Relative importance |
|---|---|---|---|---|
| cybersecurity governance requirements | 3.821 | 0.478 | 5 | high |
| Cybersecurity Program | 4.01 | 0.437 | 1 | high |
| Cybersecurity policy | 3.926 | 0.542 | 3 | high |
| Cyber Information Security Administration | 3.983 | 0.566 | 2 | high |
| Cyber risk assessment and management | 3.89 | 0.668 | 4 | high |
| Cyber governance | 3.926 | 0.424 | | high |

Table (4) indicates that the attitudes of the sample members were towards the high relative importance of cyber governance, where the arithmetic average was (3.926), a standard deviation (0.424), and after ( cybersecurity program) ranked first, with an arithmetic average (4.010).With a standard deviation (0.437), and with a high relative importance, while the (cybersecurity governance requirements) ranked last, with an arithmetic average (3.821), a standard deviation (0.478), and a high relative importance as well.All dimensions of cyber governance have emerged with high relative importance.

The hypotheses of the study Test

Multiple correlation test

The study relied on testing hypotheses on multiple regression analysis, in order to answer the study questions, and before starting the analysis, it was ascertained that the data was free from the phenomenon of multiple correlation, as this phenomenon indicates the presence of an almost perfect linear correlation between two or more variables that amplify the valueThe coefficient of determination R2 makes it greater than its actual value, and for this the linear correlation coefficient was calculated, and the value of the variance inflation coefficient for each variable that is being tested, the results were as follows:

Table (5): Correlation matrix for COSO decision variables

| Variable | Regulatory environment | Risk assessment | Regulatory activities | Information and communications | surveillance |
|---|---|---|---|---|---|
| Regulatory environment | 1 | | | | |
| Risk assessment | 0.345** | 1 | | | |
| Regulatory activities | 0.407** | 0.380** | 1 | | |
| Information and communications | 0.477** | 0.424** | 0.390** | 1 | |
| surveillance | 0.438** | 0.317** | 0.269** | 0.427** | 1 |

** Indicator at a significance level of 0.01

Table (5) shows that the highest value of the correlation coefficient appeared between the two independent variables (Regulatory environment) and (information and communication), which amounted to (0.477), while the value of the correlation coefficient between the variables of other COSO decisions was less than that, and this indicatesThe absence of the phenomenon of multiple linear correlation between the variables of the independent study, related to the decisions of the COSO Committee. Table (6): Correlation matrix for COBIT5 decision variables

| Variable | Regulatory environment | Risk assessment | Regulatory activities | Information and communications | surveillance |
|---|---|---|---|---|---|
| Planning andorganization | 1 | | | | |
| possession and implementation | 0.504** | 1 | | | |
| Support and delivery | 0.473** | 0.442** | 1 | | |
| Follow-up and evaluation | 0.488** | 0.286** | 0.462** | 1 | |
| Guidance and monitoring | 0.400** | 0.306** | 0.403** | 0.398** | 1 |

** Indicator at a significance level of 0.01

Table (6) shows that the highest value of the correlation coefficient appeared between the two independent variables (planning and organizing) and (possession and implementation), which amounted to (0.504), while the value of the correlation coefficient between the variables of other COBIT5 decisions was less than that, and this indicates The absence of the phenomenon of multiple linear correlation between the variables of the independent study, related to the decisions of the COBIT5 committee. Based on the results of the correlation matrix for the variables of COSO and COBI5 decisions, it can be said that the study sample is free from the multiple high linear correlation problem, as the linear correlation coefficient values that exceed (0.80) may be considered an indicator of the existence of multiple linear correlation (Guajarati, 2004, 359).

**Results:**

The results of the hypothesis test of the first main study The first main hypothesis, H01, states that: There is no statistically significant effect at a significant level ($\alpha \leq 0.05$) for the supervisory integration of decisions of COSO (control environment, risk assessment, control activities, information and communication, and control) and COBIT5 (planning and organizing, owning and implementing, Support, delivery, monitoring and evaluation, guidance and monitoring) in the correct implementation of cyber governance in Jordanian commercial banks. To test the first main hypothesis, Hierarchical Regression was used, and the results were as follows:

Table (7): * The results of the hierarchical regression to demonstrate the effect of integration of oversight of the decisions of COSO and COBIT5 on the correct application of cyber governance

| **Dependent variable** | **Independent variables** | **Step 1** | | | **Step 2** | | |
|---|---|---|---|---|---|---|---|
| | | **B** | **computed t value** | **Sig t** | **B** | **computed t value** | **Sig t** |
| Cyber governance | Regulatory environment | 0.231 | 6.462 | 0 | 0.125 | 3.454 | 0.001 |
| | Risk assessment | 0.034 | 0.905 | 0.366 | 0.069 | 1.828 | 0.069 |
| | Regulatory activities | 0.056 | 1.215 | 0.225 | 0.085 | 1.989 | 0.048 |
| | Information and communications | 0.302 | 6.923 | 0 | 0.264 | 6.492 | 0 |
| | surveillance | 0.255 | 5.659 | 0 | 0.219 | 5.218 | 0 |
| | COBIT5 Decisions | | | | 0.353 | 7.302 | 0 |
| | $R^2$ Selection factor | 0.553 | | | 0.618 | | |
| | $\Delta R^2$ | 0.553 | | | 0.065 | | |
| | $\Delta$ F | 77.598 | | | 53.315 | | |
| | Sig $\Delta$ F | 0 | | | 0 | | |

* The effect is statistically significant at ($\alpha \leq 0.05$).

The above table displays the results of the hierarchical regression based on two models, as the results of the first model based on the first step reflected the presence of a statistically significant effect of the dimensions (decisions of the COSO Committee) combined in (the correct application of cyber governance), where the value of (F = 77.598) and with a significant level ( Sig $\Delta$ F = 0.000), which is less than 0.05, and the value of the coefficient of determination was (R2 = 0.553), and this indicates that the dimensions of the (decisions of the COSO Committee) as a whole explain (55.3%) of the variance in (the correct application of cyber governance). ). In the second step, a

variable (decisions of COBIT5) was introduced to the regression model, where the value of the coefficient of determination R2 increased by (6.5%), and this ratio is statistically significant as the value of (F = 53.315) and the level of significance (Sig Δ F = 0.000), which is Less than 0.05, as was the value of (B = 0.353) at (decisions of COBIT5), and the level of significance (Sig t = 0.000), and this confirms the difference in the significant impact of the dimensions of the decisions of the COSO Committee in the correct application of cyber governance according to the different decisions of the COBIT5 committee. Accordingly, we conclude that: There is a statistically significant effect at a significant level (α≤0.05) for the supervisory integration of decisions of COSO (control environment, risk assessment, control activities, information and communication, and control) and COBIT5 (planning and organizing, owning and implementing, support and delivery, monitoring and evaluation, guidance and control) In the correct application of cyber governance in Jordanian commercial banks.

Results of the hypothesis test of the second main study

The second main hypothesis H02 states that: There is no statistically significant effect at a significant level (α≤0.05) for the supervisory integration of the decisions of COBIT5 (planning and organizing, owning and implementing, support and delivery, follow-up and evaluation, direction and control) and COSO (control environment, evaluation Risks, supervisory activities, information and communication, and monitoring) in the correct application of cyber governance in Jordanian commercial banks. To test the second main hypothesis, Hierarchical Regression was used, and the results were as follows:

Table (8): * The results of the hierarchical regression to show the effect of integration of oversight of decisions of COBIT5 and COSO on the correct application of cyber governance

| Dependent variable | Independent variables | Step 1 | | | Step 2 | | |
|---|---|---|---|---|---|---|---|
| | | B | computed t value | Sig t | B | computed t value | Sig t |
| Cyber governance | Planning and organization | 0.398 | 10.158 | 0 | 0.319 | 8.325 | 0 |
| | Possession and execution | 0.08 | 2.16 | 0.031 | 0.076 | 2.181 | 0.03 |
| | Support and delivery | 0.057 | 1.91 | 0.057 | 0.053 | 1.913 | 0.057 |
| | Follow-up and evaluation | 0.209 | 5.968 | 0 | 0.127 | 3.639 | 0 |
| | Guidance and monitoring | 0.032 | 0.897 | 0.37 | 0.023 | 0.972 | 0.502 |
| | COSO decisions | | | | 0.387 | 6.899 | 0 |
| | $R^2$ Selection factor | 0.593 | | | 0.647 | | |
| | $\Delta R^2$ | 0.593 | | | 0.054 | | |
| | Δ F | 91.663 | | | 47.596 | | |
| | Sig Δ F | 0 | | | 0 | | |

* The effect is statistically significant at (α≤0.05).

The above table presents the results of the hierarchical regression based on two models, as the results of the first model based on the first step reflected the presence of a statistically significant effect of the dimensions (decisions of COBIT5) combined in (the correct application of cyber governance), where the value of (F = 91.663) and with a significant level ( Sig Δ F = 0.000), which is less than 0.05, and the value of the coefficient of determination was (R2 = 0.593), and this indicates that the dimensions of (decisions of the COBIT5 Committee) in its society explain (59.3%) of the variation in (the correct application of cyber governance) ). In the second step, a variable (COSO decisions) was introduced to the regression model, where the value of the coefficient of determination R2 increased by (5.4%), and this ratio is statistically significant as the value of (F = 47.596) and the level of significance (Sig Δ F = 0.000) Less than 0.05, as was the value of (B = 0.387) at (COSO decisions), and at the level of significance (Sig t = 0.000), and this confirms the difference in the significant impact of the dimensions of the decisions of COBIT5 in the correct application of cyber governance according to the different decisions of the COSO Committee. Accordingly, we conclude that: There is a statistically significant effect at the level of significance (α≤0.05) for the regulatory integrity of the decisions of COBIT5 (planning and organizing, owning and implementing, support and delivery, monitoring and evaluation, directing and monitoring) and COSO (control environment, risk assessment, control activities, information and communication, and monitoring) In the correct application of cyber governance in Jordanian commercial banks.

**Recommendations**

Based on the findings of the study, it recommends the following:

1. The Jordanian commercial banks administration set up rules by which the duties and responsibilities concerned with all departments and individuals working in them are determined according to the directions of the COSO and Cobit 5 decisions, and to rely on standards directed at their decisions to achieve the correct implementation of cyber governance in them.
2. The administration of Jordanian banks applies preventive control measures to reduce potential risks according to the directions of the Coso and Cobit 5 decisions, and adopting all appropriate measures to confront them in order to achieve the correct application of cyber governance in them.
3. The management of Jordanian banks conducts more evaluation processes for their supervisory activities, periodically and continuously, and adheres to the application of the principle of separation of tasks more in order to achieve the correct application of cyber governance in them.
4. Increasing the level of interest of Jordanian commercial banks in providing modern and developed means and technologies that help in the delivery of information to all administrative levels in a timely manner, and taking into account the needs and requirements of users of information and communication systems when updating the internal control system according to the directions of the Coso and Cobit 5 decisions, in order to reach the correct application of cyber governance. In which .
5. Increasing the level of interest of the Jordanian commercial banks 'management in conducting a periodic and continuous evaluation process for the level of effectiveness of its internal control system, and taking into account the results of control reports when improving and developing work.
6. The Jordanian commercial banks 'management conducting a process of updating and developing the information technology infrastructure to increase the efficiency of the information systems used in it, and relying on the operational processes manual in the use of information technology to reach the correct application of cyber governance in it.
7. The banking administration applies the appropriate security measures in accordance with the directions of cyber governance for banks that ensure the safety and protection of their information security, and determine the level of security and safety required in their internal control.

**Resources and references:**

Abdulbasset, A. (2014). **Cobit 5 as A mechanism for it governance a case study of state oil company**, Dissertation submitted in partial fulfillment of the requirements for the degree of Magister in management,AbouBekrBelkidUniversty – Tlemcen, Algeria.

Abdul Ridha Asaad Tarish;Al-Maamouri, Ali Ibrahim.International Studies (2020) Cybersecurity and a course on the spread of the phenomenon of terrorism in Iraq after the year 2003, University of Baghdad, Center for International Studies.Issue 80, p.149-190.

Ahmed, Ashraf (2017). Examination and evaluation of the internal control system in accordance with the framework (COSO) in the national university education. Muthanna Journal of Administrative and Economic Sciences, 8 (2), 156-140.

Al-Basri, Abdul Rida Shafiq, Mohammed and Adnan Yasser (2019). The impact of the application of a framework (COBIT5) on the efficiency and effectiveness of INFORMATION TECHNOLOGY: an applied analytical study of a sample of Iraqi private equity banks. Technical Magazine, 2 (2), 1-15.

Al-Husseini, Mortada, and Al-Sabri, Ibrahim (2017). Employing internal control components to enhance the quality of external auditing - applied research in a sample of private Iraqi banks. Babylon Journal / Pure and Applied Sciences, 25 (4).

Al-Saeed, Fadi, (2019), Letters on Cybersecurity Governance, https://www.linkedin.com/

Al Shammari ،M. & Khalawi ،S. (2018). The impact of using SWOT analysis on improving the efficiency and effectiveness of the internal control system according to the COSO model. Al Kut Journal of Economics Administrative Sciences30 ،.

COSO, URL:http://www.coso.org/documents/COSO,2020

COSO, URL:http://www.coso.org/documents/COSO,2012

Haes ،Steven De. & Grembergen ،Wim Van (2015). Enterprise Governance of Information Technology Achieving Alignment and Value ،Featuring COBIT 5 (2nd ed). USA ،New York ،Springer.

Hamdan، K.، (2018). Applying COSO Internal Control Framework toDisasterManagement Evaluation According to HyogoFramework for Action (HFA) In Iraq. DOI: 10.18081/MJAES/2019-9/125-152.

Hammoudi, Ahmed, al-Jawhar, Karima (2019). Measure it governance performance in cobit 5 with balanced tag card. Journal of Accounting and Financial Studies (JAFS), 14.47.

Hussein, Wissam, and Khalaf, Alaa (2019).The Impact of Information Technology Governance in Accordance with the Framework (COBIT) in Enhancing the Quality of Internal Auditing An Applied Study in the Iraqi Banking Sector, Takbat Journal of Economic and Administrative Sciences, 15 (48).

Majid, Abdelkader (2019). The role of internal control components in accordance with coso framework in enhancing the quality of banking services. A survey of the opinions of a sample of department managers, people and oversight officials in some government banks in Nineveh province. Tikrit Journal of Administrative and Economic Sciences, 15 (45) C1.

Megasyah، Y. & Arifnur، A. (2020). Academic Information System Security Audits Using COBIT 5 - Framework Domains، APO12، APO13 and DSS05. ***Journal of Applied Engineering and Technological Science***، 2، 124-135.Saleh, Ahmad Ali and Al-Salehi, Nazal Amin, (2018), University Governance Models and their Impact on Building Strategic Orientation - An Applied Study in Private Jordanian Universities in Amman, Journal of the Association of Arab Universities for Research in Higher Education, 28 (2)

Saleh, Walid (2014). Faculty of Management and Economics, Issue 40, Anbar University, Iraq.

The Central Bank of Jordan, (2018), Instructions for Adaptation to Cyber Risks https://www.cbj.gov.jo/Default.aspx

Zambrano، T. (2017). *COBIT 5 Implementation COBIT 5 Case Study in Aetna Inc*. Louvain School of Management، Universite catholique de Louvain