RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES

Social Science Journal

Extent to which the internal control systems of Iraqi private banks are consistent with the principles of the COSO Committee 2017 framework

By

Dr. Mohanad Hadi AlHawazi
University of Basrah – College of Economics and Administration / Accounting Dpt./ Iraq.
Email: mo19741982@gmail.com

Dr. Mohanad Mohamed AlMudhafar
University of Basrah – College of Economics and Administration /Accounting Dpt./ Iraq.
Email: muhaned_ma@yahoo.com *

Abstract

In the last two decades, Iraq in general has faced many problems, the most prominent of which are financial problems, whose effects include many industrial, service and banking sectors. Banking services have had the greatest weight of these problems, with the many risks they carry that greatly threaten most of the banks operating in Iraq, and because government banks usually receive support and backing from the government, but private banks remain the weakest link in the face of these risks. Therefore, this research aims to find out the consistency of the concepts and procedures followed by Iraqi private banks with the principles of the COSO-2017 framework. To achieve this goal, the researchers designed a questionnaire to find out the opinions of the groups closest to these principles, and through which it was found that there are many shortcomings in the internal control systems used in Iraqi private banks. The researchers recommended the necessity of adopting quick procedures and decisions that help in improving and developing the internal control systems in private banks in order to face the many risks that could cause the collapse of these banks.

Introduction

At the end of the last century and the beginning of this century, the world witnessed the collapse of much more than a few major companies, which in turn caused a major crisis in several major global economies. Many professional bodies and committees, along with several academic studies and research, blamed the Internal Control Systems to be the reason behind this global crisis. Usually, control systems are seen as the first blocking line against the risks that organizations may face, given that this system is closer to the organization's activities than any other system. Therefore, it is the active element in ensuring the continuity of the organization's activities in accordance with the drawn plans, and it is regarded as an early warning bell in the event of any deviation from these plans. The inability of the Internal Control Systems to perform their tasks in the correct manner will undoubtedly lead to the occurrence of risks on the one hand and will also exacerbate these risks due to the increase of their negative effects because of the lack of early diagnosis on the other hand. As a result, many studies and solutions have emerged to confront the shortcomings in the control systems and develop them to ensure their ability to perform their function in a better way. The most prominent of these solutions is the COSO - Framework (The Committee of Sponsoring Organizations) issued in 1992.

COSO Framework

In 1985, the below five institutions reached an agreement and cooperation plan:

- American Institute of Chartered Public Accountants
- American Association of Accountants
- The Institute of Internal Auditors
- Institute of Management Accountants
- The International Association of Financial Directors

This agreement led to the formation of a committee named (The Committee of Sponsoring Organizations of the Tradway Commission), which stands for COSO. It is entrusted with the creation and development of a framework that helps those concerned in organizations' departments to design and implement efficient and effective Internal Control Systems to meet the challenges these organizations are facing. This committee has adopted the following definition of internal control systems:

"a process used by an entity's board of directors, management and other personnel, that is designed to provide a reasonable assurance regarding the completion of an organization`s objectives" (COSO, 1994).

The committee has identified three main objectives that must be achieved:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.

To achieve these goals, COSO issued an integrated framework for Internal Control Systems in 1992 called the (Internal Control-Integrated Framework), which divided the internal control system into five components: control environment, risk assessment, control activities, Information & communication systems, and monitoring. COSO has presented these objectives and components through the below cube:

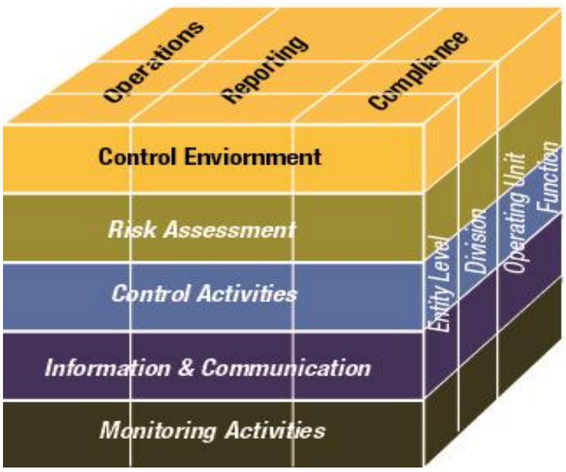

Figure 1. Internal Control-Integrated Framework
Source: COSO

Despite the importance of this framework, its increasing adoption by many institutions and its translation into many languages, the changes in the business environment and the development of several general concepts such as “technology” and “global trade” led to the creation of several modifications in the COSO Framework. Here, one of the most important updates in the COSO framework can be distinguished, which is the adoption of the ERM model according to the strategic perspective.

COSO Framework Amendments & Updates

Many researchers believe that Internal Control Systems are a dynamic process that must adapt to the requirements of the environment in which they operate. This applies to the model presented by COSO, which was first revised in 1994. Then, revisions and updates followed according to changes in the business environment and the organizations' need for such changes, in addition to the guidelines frequently issued by COSO to provide tools that enable organizations to use the COSO model in the best way. However, the most prominent change in this model is the Enterprise Risk Management - Integrated Framework. It was issued in 2004 and brought about a change in the basic concepts of this framework. It emphasized the main objective of the internal control system, which primarily revolves around increasing its ability to avoid risks, and therefore strengthening the capabilities of these systems in identifying and avoiding risks, which by itself a major function of these systems. Therefore, the COSO framework has adopted the Enterprise Risk Management (ERM) to be an intrinsic part of the integrated framework. According to the new framework presented by COSO, it has developed 17 principles that are distributed over the five components of the Internal Control System. Throughout these principles, it is possible to determine the best design for the Internal Control System in the organization to achieve the objectives of this system within the organization. COSO has introduced the new framework with the following cube:

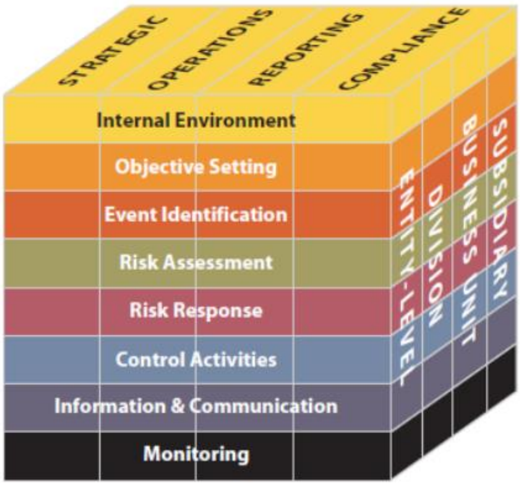

Figure 2. Enterprise Risk Management- Integrated Framework
Source: COSO

The ERM has emerged because of changing the basic concepts of Risk Management. The Traditional Risk Management (TRM) deals with each type of risk independently (Silos). This means a loss of coordination between the different risk management departments (Liebenberg & Hoyt, 2003). Whereas the ERM System works with the realization that the main results of each company are the results of the interaction of all the activities and parts of that company. Therefore, any activity or part of the company facing any kind of risks will inevitably cause threats and damage to the rest of the activities or other parts in that company. Thus, it became a necessity to deal with risks as a single entity which means each part of the organization looks at these risks from its angle without neglecting the rest of the angles.

The development of the concept of Risk Management in the ERM was not limited to the overall comprehensive view of risks as threats to the organization as a whole, but rather it went to see the development of this concept as a proactive system for identifying and confronting risks even before they emerge. With the increasing competition, Risk

Management had to transform from a defensive means in the face of risks to be an offensive means that identifies and analyzes risks in advance to prepare the requirements to confront them (Meulbroek, 2002). Considering a changing business environment that requires continuous adjustment of the organization's goals and strategy, it is illogical to believe in the possibility of separating the activities of ERM and the work of the basic organization, as both types of activities must overlap to ensure the continuous and consistent implementation of Risk Management functions by employees throughout the organization (COSO, Strengthening Enterprise Risk Management for Strategic Advantage, 2009).

It is known that every strategy has risks, some of which are stable, and they only require periodic follow-up and review from time to time while others are dynamic which require workers to be aware and able to confront them in a manner commensurate with the nature of these risks (Deloitte & Touche, 2012). Employees can face the first type of these risks by following the necessary policies and procedures, while the second type requires them to use their judgment to confront them because they often change in directions not calculated in advance and all employees need to understand the concept of Risk Management to achieve success in confronting these challenges. This can only take place in the organization and at various levels by making ERM an integral part in the organization’s culture and basic operations, so we find that COSO defined ERM as:

"The culture, capabilities, and practices, integrated with strategy-setting and its execution, that organizations rely on to manage risk in creating, preserving, and realizing value".

Knowing the individuals who are working in this system greatly helps in understanding the nature of the risks that can occur and the ways to confront them. The culture of the organization plays a major role in shaping the management’s philosophy towards developing strategies and understanding the risks and ways of making different decisions. The organization’s culture helps the workers to understand the strategies adopted by the organization’s management and also helps to apprehend the logic behind various decisions taken by that management especially when the management constantly adjust its objectives and then its strategy to face the rapidly changing risks in the business environment. Therefore, it was necessary to make ERM as a part of the organizational culture, because the ERM acts as a navigation system for the organization. It does not only provide warning signals when risks emerge, but rather guides management to the right path away from these risks or to reduce the risk level as soon as the signs of these risks are identified. The ERM supports management in choosing a strategy and determining the strengths and weaknesses of this strategy according to changing surrounding conditions, in addition to its ability to determine the suitability of this strategy with the mission and vision of the organization (COSO, Enterprise Risk Management Integrating with Strategy and Performance, 2017).

As per the aforementioned, COSO has concluded that the effects and role of the ERM is not limited only to the contribution of the strategy’s development, but it extends to assigning employees to provide better performance in light of reducing the impact of risks on day-to-day business. The risks are not directly related to the strategy, but with the results of implementing the strategy, which is performance. It would not suffice it to only take these risks into consideration when developing the strategy. In fact, these risks must be taken into consideration when implementing the strategy and achieving performance. This prompted COSO to update its framework in the year 2017 and to introduce it as “Enterprise Risk Management – Integrating with Strategy and Performance,”.

The COSO 2017 framework includes the following five interrelated components:
1. Governance and culture.
2. Develop strategies and objectives.
3. Performance.
4. Revision and revision.
5. Information, communication and preparing reports.

We note that these components represent the overlapping work between the main organization activities and ERM activities, as explained by COSO as follows:

Figure 3. Risk Management Components
Source: COSO

The COSO 2017 framework works towards integration from strategy to performance under ERM. This framework demonstrates how integrating ERM practices across the organization helps acceleration of growth and improvement of performance (COSO, Enterprise Risk Management Integrating with Strategy and Performance, 2017). The COSO 2017 framework works to ensure that strategy goes in accordance with the performance without causing any confusion or divergence between the two in order to reach the highest possible value. To achieve this coordination in the best way, COSO has developed twenty principles distributed over the five components, as shown below:

Figure 4. Component of Internal Control
Source: COSO

As these principles, when applied, ensure obtaining the best combination of the Internal Control System in a manner that commensurate with the capabilities of the organization in addition to the nature of its work and its size. Also, these principles can be used as a basis for evaluating the organizations' Internal Control Systems to know the strengths and weaknesses of these systems, and then to measure the extent to which they can be relied upon.

Methodology

The Sample

The study community includes most of the private banks located in Iraq/ Basra, where the questionnaire was directed to a sample of bank administration officials, department officials, control and auditing officials, in addition to those working in the field of accounting. Where 200 questionnaire forms were distributed to the recipient and valid for statistical analysis, 168 forms, with a response rate of 84%.

The Questionnaire

The questionnaire was divided into five main axes that represent the main elements of internal control systems in accordance with the COSO framework, and each axis includes a set of principles that were identified in accordance with the framework of COSO-2017. Some of these principles can be answered with one question, and others can be answered with more than one question to include all aspects and requirements of that principle. It was for the study Compliance Risk Management: Applying the COSO ERM Framework (COSO, 2020) in addition to the model presented in the following link:
https://assets.corporatecompliance.org/Portals/1/PDF/events/Brochures/SCCE-HCCA-Enteprise-Risk-Management-Compliance-Privacy-Risk-Example.pdf

"Enterprise Risk Management- Applying Enterprise Risk Management to Compliance Risks/ Example - General Privacy Risk in a Global Organization". It had a basic role in forming the questions of the questionnaire to determine the areas of evaluation in each of the twenty principles. The five-point Likert scale was used to express the answers of the study sample, which consisted of the following scores:

Strongly Low (1), Low (2), Medium (3), High (4), Strongly High (5)
Data Analysis Discussion
To analyze the data, the researchers used the statistical program SPSS v.24. Stages of the analysis and results were as follows:

Answer Strength Scale

Because the questionnaire seeks to know the opinions of bank employees about the twenty principles of COSO-2017, so the basis for analyzing the answers is the averages and the standard deviation to determine the direction of the sample's opinions about each principle. In order to determine the level of the answer, the severity of the answer will be adopted as follows:

Table 1. Response Scale

Likert Scale	Interval	Difference	Descriptions
1	1.00 – 1.79	0.79	Strongly High
2	1.80 – 2.59	0.79	High
3	2.60 – 3.39	0.79	Medium
4	3.40 – 4.19	0.79	Low
5	4.20 – 500	0.80	Strongly Low

Compare Means for Principles

It was found through the SPSS program that the averages and standard deviations of each component of the internal control systems, as well as the severity of the answer, whether at the level of separate phrases or at the level of the principle as a whole, as they are in Tables 2, 3, 4, 5 and 6 and as follows:
First: Governance & Culture

Table 2. Descriptive Statistics of "Governance & Culture"

	Statements	Mean	Std. Deviation	Response Scale
	Principle 1: Exercises board risk oversight			
1	The Board of Directors has knowledge and awareness regarding the assessment of the risks facing the bank and the nature of response to them	3.61	0.811	High
2	The Board of Directors continuously receives all emerging matters related to changes in legal, regulatory and professional matters and the risks related to them and how the bank deals with those risks.	3.80	0.816	High
	Exercises board risk oversight	3.7054	0.5799	High
	Principle 2: Establishes operating structures			
1	There is a special risk department within the functional structure of the bank that has unrestricted access and is linked to the board of directors	1.94	0.809	Low
2	There are representatives from all over the bank in the risk management	1.52	0.656	Strongly Low
	Establishes operating structures	1.7321	0.6331	Strongly Low
	Principle 3: Defines desired culture			
1	There is a code of conduct and policies related to the application of risk management standards and systems and expectations	1.63	0.808	Strongly Low
2	The Bank's risk management standards, appropriate practices and related expectations are clearly defined	2.99	0.851	Medium
3	The Bank's risk management standards are available to all employees and customers	3.40	0.821	High
4	There is a list of accountability and consequences of non-compliance with risk management standards	4.01	0.826	High
	Defines desired culture	3.0104	0.3833	Medium
	Principle 4: Demonstrates commitment to core values			
1	The bank’s management emphasizes and clarifies the importance of adhering to a culture of risk management and preserving the privacy and personal information of its employees and customers	2.07	0.906	Low
2	The Bank's management publishes the standards of risk management culture and its expectations for compliance with these standards on a regular basis throughout the Bank	1.73	0.713	Strongly Low
3	There are clear and public channels for reporting cases of non-compliance with risk management standards that maintain the confidentiality of the person of the whistleblower	3.39	0.935	Medium
4	The risk management culture standards and compliance expectations are periodically evaluated	1.96	0.829	Low
	Demonstrates commitment to core values	2.2887	0.4470	Low
	Principle 5: Attracts, develops and retains capable individuals			
1	The management of the bank seeks to appoint employees of integrity	3.99	0.762	High
2	The management of the bank seeks to appoint employees who meet the requirements of the job description	3.79	0.813	High
3	The management of the bank provides training on risk management for employees in accordance with the responsibility they bear	2.27	0.809	Low
4	The bank's management motivates employees to abide by the laws and privacy policies related to the bank and customers through periodic performance evaluation	2.24	0.798	Low
	Attracts, develops and retains capable individuals	3.0729	0.3996	Medium

Second: Strategy and Objective Setting

Table 3. *Descriptive Statistics of " Strategy and Objective Setting"*

	Statements	Mean	Std. Deviation	Response Scale
	Principle 6: Analyzes business context			
1	The bank's management evaluates the level, probability and impact of risks, whether internal or external	3.52	0.909	High
2	The bank's management evaluates business strategy, plans operations and monitors changes in applicable laws and regulations, professional practices and business sector trends	3.83	0.819	High
3	The bank's management carefully considers commercial operations and their associated risks and analyzes the current and future needs related to individuals, operations and technology	3.55	0.867	High
4	The bank's management performs the necessary assessments that help identify potential risks in the data flow analysis activities of the proposed and current business	2.84	0.776	Medium
	Analyzes business context	3.4345	0.4464	High
	Principle 7: Defines Risk Appetite			
1	The bank's management determines the extent of its ability to endure risks and non-compliance with the professional standards and regulations in force locally and globally and evaluates it regularly	2.47	0.826	Low
	Principle 8: Evaluates alternative strategies			
1	The bank's management evaluates alternative strategies and the potential effects of the risks on the Bank	2.86	0.728	Medium
	Principle 9: Formulates business objectives			
1	The bank's management considers the implications of setting business objectives on privacy risks by assessing the impact of privacy	2.08	0.855	Low
2	Establish performance measures, taking into account their potential impact on privacy risks	2.07	0.827	Low
	Formulates business objectives	2.0714	0.5772	Low

Third: Performance

Table 4. *Descriptive Statistics of "Performance "*

	Statements	Mean	Std. Deviation	Response Scale
	Principle 10: Identifies risk			
1	The bank's management classifies risks according to their priority and the extent of their impact on the performance of the strategy and business objectives	2.11	0.862	Low
2	The bank's management analyzes the privacy risks on the performance of the strategy and business objectives through the identification of risks and evaluation activities periodically	1.85	0.723	Low
3	The Bank's management identifies sub-categories of performance risks as well as non-traditional risks	1.98	0.713	Low
	Identifies risk	1.9802	0.4667	Low
	Principle 11: Assesses severity of risk			
1	The bank's management assesses the severity of the risks by using a manner and methodology that is consistent with the manner and methodology of other risk assessment	1.71	0.693	Strongly Low
2	The Bank's management reassesses the risks on a regular basis or when circumstances indicate a change in risk	1.81	0.734	Low
3	The bank's management assesses risks at multiple levels or in different places in the bank or based on certain factors that indicate non-compliance with risk management standards.	1.82	0.677	Low
	Assesses severity of risk	1.7817	0.4316	Strongly Low
	Principle 12: Prioritizes risks			
1	The bank's management determines the priorities of risks using specific criteria according to the bank's position in relation to risks	1.73	0.654	Strongly Low
2	The bank's management prioritizes risks differently according to the circumstances and specificity of the site, region or operating group	1.70	0.617	Strongly Low
	Prioritizes risks	1.7113	0.4220	Strongly Low
	Principle 13: Implements risk responses			
1	The bank's management implements risk management plans and adopts various controls and strategies to effectively reduce and treat risks	2.88	0.820	Medium
2	If the risks exceed the acceptable level, the bank management has new or modified policies and procedures and updated training and awareness efforts to prevent failure in facing the risks	2.83	0.841	Medium
3	The bank's management adopts reform efforts after any failure in facing specific risks in order to reduce the risks of recurring this failure	1.92	0.721	Low
4	The bank's management documents all types of risks identified through risk management assessments	1.70	0.732	Strongly Low
	Implements risk responses	2.3289	0.3928	Low
	Principle 14: Develops portfolio view			
1	The bank's management creates a risk portfolio that includes all types of risks that may face the bank's work	1.66	0.699	Strongly Low
2	The bank's management is constantly updating the risk portfolio	1.67	0.689	Strongly Low
	Develops portfolio view	1.6637	0.4594	Strongly Low

Fourth: Review and Revision

Table 5. *Descriptive Statistics of "Review and Revision"*

	Statements	Mean	Std. Deviation	Response Scale
	Principle 15: Assesses substantial change			
1	The bank's management evaluates and updates risk management efforts throughout the Bank in accordance with the changes that occur in the internal and external business environment to develop and improve these efforts.	1.7083	0.6506	Strongly Low
	Principle 16: Reviews risk and performance			
1	The bank’s management carries out audit and follow-up activities to assess and monitor risk management	2.54	0.788	Low
2	The Bank's management periodically conducts a privacy impact check in order to evaluate risk reduction and management activities throughout the Bank	2.60	0.783	Medium
3	The bank's management integrates risk control activities with the traditional activities of functional and operational units	1.87	0.671	Low
4	The bank's management receives periodic updates on the status of risks and the results of the performance review	2.12	0.772	Low
5	The risk management periodically receives follow-up reports through the internal audit	1.96	0.757	Low
	Reviews risk and performance	2.2190	0.3299	Low
	Principle 17: Pursues improvement in ERM			
1	The bank's management periodically evaluates risk management efforts to ensure its readiness and effectiveness	2.4464	0.8244	Low

Fifth: Information, Communication, and Reporting

Table 6. *Descriptive Statistics of " Information, Communication, and Reporting*"

	Statements	Mean	Std. Deviation	Response Scale
	Principle 18: Leverages information and technology			
1	The bank's management uses technology and internal and external data to conduct analyzes aimed to identifying violations and problems in internal control related to the bank's privacy	2.83	0.672	Medium
2	The bank's management seeks to take advantage of technology to provide effective training to preserve the privacy of employees and related parties	3.66	0.741	High
3	The bank's management uses technology and information to assess sensitive information flows across systems and databases	2.45	0.788	Low
4	The bank's management periodically evaluates systems and processes to verify the effectiveness of the procedures and measures in place to protect data	3.39	0.834	Medium
	Leverages information and technology	3.0848	0.4183	Medium
	Principle 19: Communicates risk information			
1	The risk management officer includes the results of privacy risks, priority arrangements, efforts and strategies to reduce risks in the periodic reports submitted to the management of the bank.	3.45	0.853	High
2	Risk management officials receive relevant information and undergo continuous education to develop their skills	3.46	0.833	High
	Communicates risk information	3.4554	0.5939	High
	Principle 20: Reports on risk, culture, and performance			
1	The bank’s management determines the appropriate categories to receive periodic reports on privacy risk management and risk mitigation efforts and related information	4.00	0.709	High
2	The bank's management prepares periodic reports on culture assessment, including culture related to risk management and compliance with risk management standards	1.83	0.629	Low
3	The bank's management presented a list of measures that determine accountability and the consequences of non-compliance with risk management policies	4.01	0.679	High
4	Risk management officials report to the bank's management regarding accountability and non-compliance with risk management policies	3.99	0.709	High
	Reports on risk, culture, and performance	3.4554	0.4051	High

Table 7. Statistically significant of Principles

	Statements	F	Sig.	Decision
		Principle 1: Exercises board risk oversight		
1	Gender	0.159	0.691	No statistically significant differences between the means
2	Qualification	6.154	0.003	Statistically significant differences between the means
3	Duration	3.107	0.028	Statistically significant differences between the means
		Principle 2: Establishes operating structures		
1	Gender	1.234	0.268	No statistically significant differences between the means
2	Qualification	2.927	0.056	No statistically significant differences between the means
3	Duration	6.049	0.001	Statistically significant differences between the means
		Principle 3: Defines desired culture		
1	Gender	2.499	0.116	No statistically significant differences between the means
2	Qualification	0.032	0.968	No statistically significant differences between the means
3	Duration	3.977	0.009	Statistically significant differences between the means
		Principle 4: Demonstrates commitment to core values		
1	Gender	5.128	.025	Statistically significant differences between the means
2	Qualification	6.054	.003	Statistically significant differences between the means
3	Duration	2.218	.088	No statistically significant differences between the means
		Principle 5: Attracts, develops and retains capable individuals		
1	Gender	5.079	0.026	Statistically significant differences between the means
2	Qualification	6.887	0.001	Statistically significant differences between the means
3	Duration	1.157	0.328	No statistically significant differences between the means
		Principle 6: Analyzes business context		
1	Gender	7.724	0.006	Statistically significant differences between the means
2	Qualification	2.050	0.132	No statistically significant differences between the means
3	Duration	4.984	0.002	Statistically significant differences between the means
		Principle 7: Defines Risk Appetite		
1	Gender	4.514	0.035	Statistically significant differences between the means
2	Qualification	12.861	0.000	Statistically significant differences between the means
3	Duration	1.568	0.199	No statistically significant differences between the means
		Principle 8: Evaluates alternative strategies		
1	Gender	1.240	0.267	No statistically significant differences between the means
2	Qualification	5.341	0.006	Statistically significant differences between the means
3	Duration	0.731	0.535	No statistically significant differences between the means
		Principle 9: Formulates business objectives		
1	Gender	1.178	0.279	No statistically significant differences between the means
2	Qualification	2.264	0.107	No statistically significant differences between the means
3	Duration	0.385	0.764	No statistically significant differences between the means
		Principle 10: Identifies risk		
1	Gender	1.901	0.170	No statistically significant differences between the means
2	Qualification	1.094	0.337	No statistically significant differences between the means
3	Duration	1.225	0.302	No statistically significant differences between the means
		Principle 11: Assesses severity of risk		
1	Gender	0.001	0.976	No statistically significant differences between the means
2	Qualification	1.946	0.146	No statistically significant differences between the means
3	Duration	3.704	0.013	Statistically significant differences between the means
		Principle 12: Prioritizes risks		
1	Gender	0.188	0.665	No statistically significant differences between the means
2	Qualification	7.867	0.001	Statistically significant differences between the means
3	Duration	3.404	0.019	Statistically significant differences between the means
		Principle 13: Implements risk responses		
1	Gender	0.016	0.898	No statistically significant differences between the means
2	Qualification	0.880	0.417	No statistically significant differences between the means
3	Duration	1.981	0.119	No statistically significant differences between the means
		Principle 14: Develops portfolio view		
1	Gender	0.198	0.657	No statistically significant differences between the means
2	Qualification	3.118	0.047	Statistically significant differences between the means
3	Duration	0.928	0.429	No statistically significant differences between the means
		Principle 15: Assesses substantial change		
1	Gender	3.181	0.076	No statistically significant differences between the means
2	Qualification	1.772	0.173	No statistically significant differences between the means
3	Duration	0.801	0.495	No statistically significant differences between the means
		Principle 16: Reviews risk and performance		
1	Gender	0.069	0.793	No statistically significant differences between the means
2	Qualification	0.893	0.412	No statistically significant differences between the means
3	Duration	1.043	0.375	No statistically significant differences between the means
		Principle 17: Pursues improvement in ERM		
1	Gender	1.579	0.211	No statistically significant differences between the means
2	Qualification	0.876	0.418	No statistically significant differences between the means
3	Duration	0.776	0.509	No statistically significant differences between the means
		Principle 18: Leverages information and technology		
1	Gender	0.385	0.536	No statistically significant differences between the means
2	Qualification	0.471	0.625	No statistically significant differences between the means
3	Duration	1.548	0.204	No statistically significant differences between the means
		Principle 19: Communicates risk information		
1	Gender	2.650	0.105	No statistically significant differences between the means
2	Qualification	0.721	0.488	No statistically significant differences between the means
3	Duration	5.224	0.002	Statistically significant differences between the means
		Principle 20: Reports on risk, culture, and performance		
1	Gender	0.064	0.801	No statistically significant differences between the means
2	Qualification	3.535	0.031	Statistically significant differences between the means
3	Duration	0.244	0.866	No statistically significant differences between the means

Statistical Differences

To find out if there are differences in the averages of the answers to the statements presented in the questionnaire, whether at the level of gender, academic qualifications or the period of functional service, the researchers used ANOVA analysis to determine the presence or absence of these differences, which can be illustrated through Table No. 7:

Discussion & Conclusion

Through the previous analysis, we conclude that there is a low consistency of Iraqi private banks' applications, regarding internal control systems in general and risk management in particular, with the principles of COSO-2017 framework. As most of the principles laid down by the COSO framework were not achieved in these banks, especially 2, 4, 7, 9, 10, 11, 12, 13, 14, 15, 16, 17, their levels were low and very low. This explains the inability of Iraqi private banks to provide more banking services to customers, especially since these banks still live in an increasingly risky environment that requires a lot of efforts to gain the confidence of customers and investors. Therefore, the researchers advise Iraqi private banks to make more efforts in order to develop and implement a clear road map to correct the risk management path to achieve better benefits, both from investors and customers.

References

COSO. (1994). *Internal Control – Integrated Framework.*

COSO. (2009). *Strengthening Enterprise Risk Management for Strategic Advantage.*

COSO. (2017). *Enterprise Risk Management Integrating with Strategy and Performance.* COSO.

Deloitte, & Touche. (2012). *Risk Assessment in Practice.* COSO.

Liebenberg, A. P., & Hoyt, R. E. (2003). THE DETERMINANTS OF ENTERPRISE RISK MANAGEMENT:EVIDENCE FROM THE APPOINTMENT OF CHIEF RISK OFFICERS. *Risk Management and Insurance Review*, *6*(1), 37-52.

Meulbroek, L. K. (2002). Integrated Risk Management for the Firm: A Senior Manager’s Guide. *Journal of Applied Corporate Finance*, *14*, 56-70.