

Determining the Effectiveness of Internal Controls in Enterprise Risk Management Based on COSO Recommendations

Thabit H. Thabit¹

Department of Computer Engineering and Information, College of Electronic Engineering, Ninevah University, Mosul, Iraq
Email: thabit.acc@gmail.com

Alan Solaimanzadah²

Department of Accounting, College of Administrative and Financial Sciences, Cihan University, Erbil, Iraq

Mohammed A. Mohammed³

Department of Information System, College of Administration and Economic, University of Mosul, Mosul, Iraq

DOI: 10.23918/ICABEP2019p43

Abstract:

The continuous risk assessment depends on the integration of the lines of defense (LOD), the main LOD are three lines (management control, risk and control monitoring, ensuring independence of the internal audit) which lead to the integration of enterprise risk management ERM. The cooperation among the LOD is not new in an environment of growing risk and limited resources. But for this collaboration to be effective, internal control bodies need to identify a methodology for evaluating the LOD and mitigating the challenges they face. This study aims to identify the most important internal control methods in assessing the risks facing the organization in accordance with the internal control framework issued by COSO in order to limit the obstacles that decrease the ability of the internal audit to rely on others for fear of low level of independence and objectivity, and to clarify the objectives and motives of internal control and its capability with the responsibility and authority of the internal auditor within the organization. The main problem of the study is the ability of internal control to regulate the activity of the organization's LOD in order to increase the effectiveness of ERM, reduce the cost of compliance and enhance the independence of the internal auditor of the organization. The researchers adopted COSO recommendations to determine the effectiveness of internal control in risk assessment of the organization by analyzing these recommendations and comparing them with the most important challenges facing internal auditing according to the related PwC reports of. The researchers concluded that the internal audit plays a major role in improving ERM of the organization and the integration of its LOD by enhancing the role of the internal auditor and raising the level of its independence and objectivity.

Keywords: Internal Control, Enterprise Risk Management, Internal Audit, COSO Framework

Introduction

Internal control is one of the most important components of ERM in the organization. So, COSO focused on this component and released many papers, frameworks, and reports in cooperation with PwC to enhance the effectiveness of internal control in organization. Many researchers and scholars have also presented papers on how to develop internal control and how to strengthen the LOD in the organization by employing internal control in the integration of LOD. Effective implementation of internal control in the organization can help to increase the level of compliance and enhance the independence of the internal auditor.

Research Methodology

The Study Problem

The Integration of (management control, risk monitoring and control, and ensuring the independence of the internal audit function) leads to enhanced ERM in the organization, and this cooperation is very important in an environment with growing risks and limited resources. In order for such cooperation to be effective, a methodology should be identified to evaluate the integration. So, based on the above, the study problem can be summarized in the following questions:

Do COSO recommendations and the related reports of PwC impact on the effectiveness of internal control in ERM?

Does internal control help to enhance the integration of LOD?

Does the integration of LOD lead to effective ERM?

The Study Importance

The research derives its importance from the significance role of internal control in evaluating the risks facing the organization and the positive impact of the recommendations of COSO framework and related PwC reports in enhancing the effectiveness of internal control and reducing the most important challenges facing the internal auditors in the organization.

The Study Objectives

The study aims to achieve the following objectives:

Present an introduction about COSO and its frameworks and clarify the most important ERM recommendations of COSO and related PwC reports.

Explain the concept of ERM and LOD in the organization and clarify the main ways of adopting them and reducing their negative effects.

Clarify the positive role of internal control in applying the effective ERM in the organization.

The Study Hypotheses

Basically, the study is based on the following hypotheses:

H₁: Internal control has a positive impact on the integration of LOD of the organization.

H₂: The COSO recommendations and related PwC reports positively affect the effectiveness of internal control in the organization.

H₃: ERM in the organization is directly affected by the functions of internal control function.

Theoretical Framework

Enterprises Risk Management:

The enterprises risk management can be defined as "an operation, implemented by an organization's board of directors, administration and other individuals, used in strategy-setting and within the organization, intended to recognize possible events that may impact on the organization, and treat risk to be within its risk appetite, to supply acceptable confirmation for achieving the organization aims"^[1].

The Three LOD in Effective Risk Management and Control:

The LOD was formed as a result of the global financial crisis to supply a coherent and arranged approach to risk and assurance by organizing main functions and duties into three lines of defense^[2].

The LOD has been generally accepted framework in industry to manage organizational risk at the strategic, tactical and operational levels and identify how risk management can be effectively managed. It is suitable for any organization, regardless of its size, type or complexity^[3].

The LOD can be classified to management control, risk and control monitoring, ensuring independence of the internal audit. Figure (1) illustrates the three lines of defense.

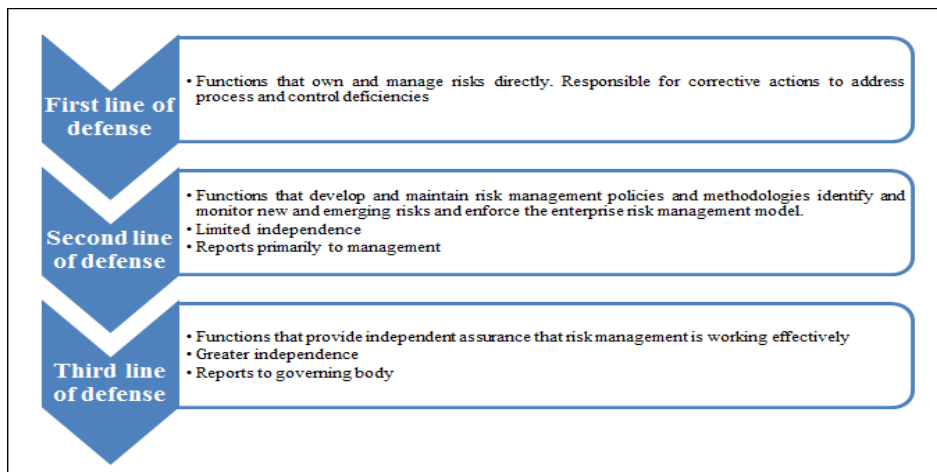


Fig. (1): The Three Lines of Defense

The Structure of LOD:

Each organization must carry out the three lines of defense in method that is appropriate for their type, size, structure, and way to risk management. Organizations must urge administration to create a complete structure for governance that is harmonic with the LOD so that all of them exist. These LOD must be independent with distinct responsibilities and strengthened out of strong tone from the top administration^[4].

The LOD must participate the same aim to aid the organization realize its aims through the active management of risk. Top administration alongside the board of directors must report the expectation of shared information and coordinated activities among the three lines of defense to back overall effectiveness^[2].

Also, this coordination is important to keep away from duplication of efforts while confirming management of important risks. Some cases may require coordination to expand beyond the LOD to contain other external parties (i.e. external auditors) to reinforce efficiency.

The Recommendations of COSO Framework for ERM:

The Description of COSO:

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) can be defined as “a common action of main five accounting and auditing private sector organization which are American Accounting Association (AAA), American Institute of CPAs (AICPA), Financial Executives International (FEI), The Association of Accountants

and Financial Professionals in Business (AAFPB), and The Institute of Internal Auditors (IIA) and is setting up to provide concept leadership by developing frameworks and guidance on ERM, internal control and fraud preventing [5].

The Integrated Framework of COSO for Internal Control:

The integrated framework of COSO for Internal Control defines internal control as "a system presenting the procedures, policies and plans performed by administration of organization to save its assets. It presents five components of internal control that administration sets and performs to supply rational assurance that its control aims will be met [6]. Each component includes many sub-components, but auditors focus on those set to reduce or detect fundamental misstatements in the financial statements.

The integrated framework of COSO for Internal Control components can be illustrated by COSO cube as shown in figure (2).

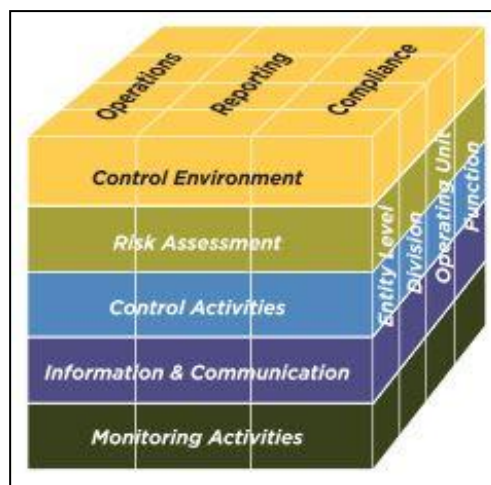


Fig. (2): COSO Cube for Internal Control

The Integrated Framework of COSO for ERM:

The integrated framework of COSO for ERM provides plain direction and instruction for realizing ERM. The framework requests that organizations test their plenary portfolio of risks think carefully about how those individual risks connect, and that administration evolves a suitable risk reduction approach to deal with these risks in a way that is compatible with their overall risk appetite and long term strategy [7]

The integrated framework of COSO for ERM components can be illustrated by COSO cube as shown in figure (3).

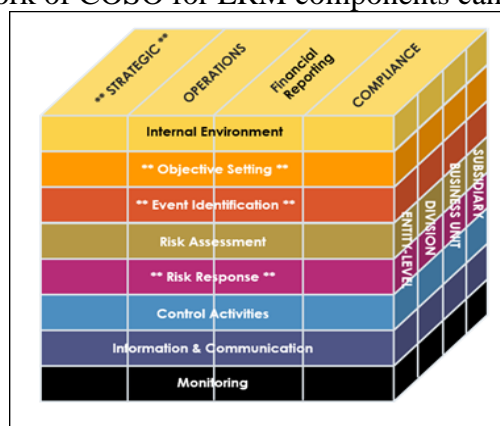


Fig. (3): COSO Cube for ERM

The influence of COSO frameworks on Internal Control

An Internal control is an essential part of ERM which is applied from strategy to execution, while depending on internal control at critical stages. ERM and Internal Control are connected, but not able to be interchanged. So, when applied together, they can be powerful supplements in supporting administration.

Internal control contains actions created to aid organizations realize compliance, reporting and operations aims. These aims can be effectively realized through integration between the three LOD of the organization and under the supervision of the internal control depending on The COSO framework of ERM^[8]. Internal control complements ERM, each boosts value of the other. So ERM aids the development of aim which used a base to develop controls, while internal control turns out ERM more effective when control actions are in place over risk reactions and other ERM operations^[13]. The connection between ERM and internal control was clear in past^[9]. COSO published its ERM Framework in 2004 in cooperation with PwC. This issue contained practices for internal control, and it was not a replacement of COSO internal control framework^[10]. After the evolving of internal control and its practice, COSO released an updated issue of internal control framework in 2013^[11]. Recently, COSO and PwC engaged to release draft ERM Framework update. So, all the actions of internal control still apply from the evaluation of fraud risk relating to financial reporting, to control actions relating to compliance^[12]. COSO updated its ERM frameworks by some drafts which can be summarized in recommendations. The recommendations of COSO stresses a shift in emphasis from assessing risks after setting of strategy to consider risk in the setting of strategy. Adopting the updated ERM framework and COSO recommendations will help organizations to be more closely align risk management to the strategy of the organization^[8]. So, the function of internal audit may also play an active role in supporting the adopting and implementing of the updated ERM Framework^[14]. It will put internal audit in better position to clarify and react to the most crucial risks related to the strategy.

Hypotheses Test

The Designed Index

To test the hypotheses of the study, the researchers designed an index to determine the Effectiveness of Internal Control in ERM according to the recommendations of COSO and related reports of PwC. Table (1) shows the Index. The researchers presented the index to (60) persons (20 managers and 40 auditors) in order to obtain their opinions about the role of the COSO framework in enhancing the effectiveness of internal control through the integration of the LOD, and measuring the effectiveness of internal control in ERM.

Table (1): The Index

	Chapter	Paragraph	Value
The Recommendations of COSO and Reports of PwC	Governance and Culture for ESG-related Risks	Define the organization's mandatory or voluntary ESG-related requirements.	
		Consider opportunities for embedding ESG in the organization's culture and core values.	
		Be informed of the ways to increase board awareness of ESG-related risks.	
		Map the operating structures, risk owners for ESG-related risks, reporting lines and end-to end ERM and strategic planning process to identify areas for improved oversight and collaboration.	
		Create opportunities for collaboration throughout the organization.	
		Embed ESG-related skills, capabilities and knowledge in hiring and talent management to promote integration.	
	Strategy and Objective-Setting for ESG-related Risks	Examine the value creation process and business model to understand impacts and dependencies on all capitals in the short, medium and long term.	
		Throughout the risk management process, align with the organization's strategy, objectives and risk appetite.	
		Consider the ESG-related risks that will impact the organization's strategy or objectives.	
	Performance for ESG-related Risks	Examine the organization's risk inventory to determine which ESG-related risks have or have not been identified	
		Involve ESG risk owners and sustainability practitioners in the risk identification process to leverage subject-matter expertise	
		Convene meetings with both risk management and sustainability practitioners to understand ESG-related risks	
		Identify the ESG-related risks that may impact the organization's strategic and operational plans	
		Define the impact of ESG-related risks on the organization precisely	
Use root cause analysis to understand drivers of the risk			
Supporting management policies, defining roles and responsibilities, and setting goals for implementation.			
Integration of LOD by Internal Control	1 st Line of Defense	Identifying shifts in the organization's implicit risk appetite.	
		Assisting management in developing processes and controls to manage risks and issues.	
	2 nd Line of Defense	Facilitating and monitoring implementation of effective risk management practices by operational management.	
		Alerting operational management to emerging issues and changing regulatory and risk scenarios.	
		Monitoring the adequacy and effectiveness of internal control, accuracy and completeness of reporting, compliance with laws and regulations, and timely remediation of deficiencies.	
	3 rd Line of Defense	Acting in accordance with recognized international standards for the practice of internal auditing.	
		Reporting to a sufficiently high level in the organization to be able to perform its duties independently.	
		Having an active and effective reporting line to the governing body.	

Analyzing the Efficiency of Internal Control in ERM

The Impact of COSO Recommendations and Related PwC Reports on Internal Control

Results of analysis the index paragraphs of the impact of governance and culture for ESG-related risks indicate that the average effect on enhancing the effectiveness of internal control (X₁₋₁ – X₁₋₆) in the study sample is (54%) as shown in table (2)

Table (2)

(X ₁) Governance and Culture for ESG-related Risks		
X ₁₋₁	Define the organization's mandatory or voluntary ESG-related requirements.	30
X ₁₋₂	Consider opportunities for embedding ESG in the organization's culture and core values.	34
X ₁₋₃	Be informed of the ways to increase board awareness of ESG-related risks.	21
X ₁₋₄	Map the operating structures, risk owners for ESG-related risks, reporting lines and end-to end ERM and strategic planning process to identify areas for improved oversight and collaboration.	44

X ₁₋₅	Create opportunities for collaboration throughout organization.	23
X ₁₋₆	Embed ESG-related skills, capabilities and knowledge in hiring and talent management to promote integration.	42
Total		194
Maximum Value		360
Percentage		54%

Results of analysis the index paragraphs of the impact of strategy and objective-setting for ESG-related risks indicate that the average effect on enhancing the effectiveness of internal control (X₂₋₁ – X₂₋₃) in the study sample is (41%) as shown in table (3)

Table (3)

(X ₂) Strategy and Objective-Setting for ESG-related Risks		
X ₂₋₁	Examine the value creation process and business model to understand impacts and dependencies on all capitals in the short, medium and long term.	22
X ₂₋₂	Throughout the risk management process, align with organization's strategy, objectives and risk appetite.	24
X ₂₋₃	Consider the ESG-related risks that will impact organization's strategy or objectives.	27
Total		73
Maximum Value		180
Percentage		41%

Results of analysis the index paragraphs of the impact of performance for ESG-related risks indicate that the average effect on enhancing the effectiveness of internal control (X₃₋₁ – X₃₋₆) in the study sample is (61%) as shown in table (4).

Table (4)

(X ₃) Performance for ESG-related Risks		
X ₃₋₁	Examine the organization's risk inventory to determine which ESG-related risks have or have not been identified	44
X ₃₋₂	Involve ESG risk owners and sustainability practitioners in the risk identification process to leverage subject-matter expertise	42
X ₃₋₃	Convene meetings with both risk management and sustainability practitioners to understand ESG-related risks	22
X ₃₋₄	Identify the ESG-related risks that may impact the organization's strategic and operational plans	45
X ₃₋₅	Define the impact of ESG-related risks on the organization precisely	37
X ₃₋₆	Use root cause analysis to understand drivers of the risk	29
Total		219
Maximum Value		360
Percentage		61%

Based on the above results, the average impact of COSO recommendations and related PwC reports on enhancing the effectiveness of internal control (X_1 , X_2 , and X_3) is (54%) as shown in table (6).

Table (5)

(X) The Recommendations of COSO and Reports of PwC		
X_1	Performance for ESG-related Risks	194
X_2	Strategy and Objective-Setting for ESG-related Risks	73
X_3	Governance and Culture for ESG-related Risks	219
	Total	486
	Maximum Value	900
	Percentage	54%

The Impact of Internal Control on Enhancing the Integration of LOD:

Results of analysis the index paragraphs of the impact of the internal control indicate that the average effect on integration of the first line of defense ($Y_{1-1} - Y_{1-3}$) in the study sample is (77%) as shown in table (6)

Table (6)

(Y ₁) 1 st Line of Defense		
Y_{1-1}	Supporting management policies, defining roles and responsibilities, and setting goals for implementation.	47
Y_{1-2}	Identifying shifts in the organization's implicit risk appetite.	51
Y_{1-3}	Assisting management in developing processes and controls to manage risks and issues.	40
	Total	138
	Maximum Value	180
	Percentage	77%

Results of analysis the index paragraphs of the impact of the internal control indicate that the average effect on integration of the second line of defense ($Y_{2-1} - Y_{2-3}$) in the study sample is (74%) as shown in table (7).

Table (7)

(Y ₂) 2 nd Line of Defense		
Y_{2-1}	Facilitating and monitoring implementation of effective risk management practices by operational management.	32
Y_{2-2}	Alerting operational management to emerging issues and changing regulatory and risk scenarios.	54
Y_{2-3}	Monitoring the adequacy and effectiveness of internal control, accuracy and completeness of reporting, compliance with laws and regulations, and timely remediation of deficiencies.	47

Total	133
Maximum Value	180
Percentage	74%

Results of analysis the index paragraphs of the impact of the internal control indicate that the average effect on integration of the third line of defense ($Y_{3-1} - Y_{3-3}$) in the study sample is (74%) as shown in table (8)

Table (8)

(Y ₃) 3 rd Line of Defense		
Y ₃₋₁	Acting in accordance with recognized international standards for the practice of internal auditing.	38
Y ₃₋₂	Reporting to a sufficiently high level in the organization to be able to perform its duties independently.	44
Y ₃₋₃	Having an active and effective reporting line to the governing body.	51
Total		133
Maximum Value		180
Percentage		74%

Based on the above results, the average impact of internal control on enhancing the integration of LOD (Y₁, Y₂, and Y₃) is (75%) as shown in table (9).

Table (9)

(Y) Integration of LOD by Internal Control		
X ₁	1 st Line of Defense	138
X ₂	2 nd Line of Defense	133
X ₃	3 rd Line of Defense	133
Total		404
Maximum Value		540
Percentage		75%

Conclusions

Based on the theoretical framework of the study, the researchers concluded the follows: There must be suitable coordination between the separate lines of defense to enhance efficiency and effectiveness of ERM by the internal control supervision. LOD must not be combined or arranged in a manner that decreased their effectiveness. The Adoption of the updated ERM framework, COSO recommendations, and related PwC reports will aid internal control to be more effective in aligning organizations with ERM. On the other hand, according to the practical part of the study, the researchers concluded the follows: The first hypothesis, which states that internal control has a positive impact on the integration of LOD of the organization, can be accepted whereas the average of respondents' opinions was (75%) The second hypothesis, which states that COSO recommendations and related PwC reports positively affect the effectiveness of internal control in the organization, can be accepted whereas the average of respondents' opinions was (54%)The third hypothesis, which states that ERM in the organization is directly affected by the functions of internal control function, can be accepted based on the literature review and previous studies.

References

- PwC (2015). Internal Audit and Enterprise Risk Management, PwC.
- Deloitte (2016). Project Risk Management: Applying the Three Lines of Defence Model to Project Risk Management, Deloitte Touche Tohmatsu.
- EY (2013). Maximizing value from your lines of defense, EYGM Limited.
- KPMG (2016). The three lines of defense: Making the transition to a mature risk management model, KPMG International.
- COSO (1992). Internal Control—Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission, COSO Report.
- COSO (2013). Internal Control — Integrated Framework: Executive Summary, Committee of Sponsoring Organizations of the Treadway Commission.
- COSO (2004). Enterprise Risk Management — Integrated Framework: Executive summary, Committee of Sponsoring Organizations of the Treadway Commission
- PwC (2017). COSO Enterprise Risk Management Framework Integrating Strategy and Performance, PwC.
- COSO (2018). Enterprise Risk Management: Applying enterprise risk management to environmental, social and governance-related risks, Committee of Sponsoring Organizations of the Treadway Commission.
- PwC (2016). Staying Ahead of the Curve Enterprise Risk Management, PwC.
- Thabit, Thabit H., Solaimanzadah, Alan (2018). The Role of SOX Act in Enhancing the Internal Control Systems of Kurdistan Banks, Proceedings of International Conference on Accounting, Business, Economics and Politics, Ishik University, pp. 288-300.
- Thabit, Thabit H., Solaimanzadah, Alan, and Al-abood, Muath T. (2017). The Effectiveness of COSO Framework to Evaluate Internal Control System: The Case of Kurdistan Companies. Cihan International Journal of Social Science, 1(1), pp. 44-54.
- IIA (2013) The Three Lines of Defense in Effective Risk Management and Control, The institute of internal auditors.
- Thabit, Thabit Hassan, Hadj Aissa, Sid Ahmed, and Harjan, Sinan Abdullah (2016). The Use of Fuzzy Logic to Measure the Risks of ICT in E-Audit, Revue des Recherches Economiques, No.15, pp. 30-46.