INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

The Importance of COSO Framework Compliance in Information Technology Auditing and Enterprise Resource Management

Oluwaseun Oladeji Olaniyi
Researcher, Department of Information Technology,
School of Computer and Information Sciences, University of the Cumberlands, USA
Dagogo Sopriala Omubo
Researcher, Department of Well Engineering and Information Technology,
Shell Petroleum Development Company, Nigeria

Abstract:
This article examines the significance of the COSO framework in managing risks and establishing effective control environments for organizations' IT systems. It delves into the five essential components of both the COSO frameworks for internal control and enterprise resource management. Furthermore, it outlines the principles that define each of the COSO frameworks for internal control and enterprise resource management components and elaborates on their impact on the COSO framework objectives. The authors also shed light on the paramount concerns of an auditor during an IT audit. In conclusion, the article provides several recommendations for integrating COSO framework compliance into an organization's information technology plan. This article is a valuable resource for auditors, administrators, and management seeking to develop an IT strategy that aligns with their business strategy and safeguards their information systems and data.

Keywords: *COSO framework, internal controls, risk management, IT strategy, risk assessment, IT audit, compliance, accountability, transparency, fraud, control exercises*

1. Introduction

Organizations around the globe are researching, exploring, and inventing technology-driven solutions to apprehend the impact of emerging technologies as it relates to internal controls and business risk (Vincent & Barkhi, 2021). However, to date, technology innovation, growth, execution, maintenance, processes, and risk assessment is about an organization and its association with other stakeholders like customers, suppliers, dealers, retailers, agents Etc. (Chiu & Wang, 2019). Thus, when evaluating the internal controls of an organization and its information systems using a designated framework, auditors, administrators, and management can accentuate an IT strategy that aligns reasonably with the business strategy (Vincent & Barkhi, 2021). An excellent example of such a framework is COSO.

2. The COSO Framework Internal Controls

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a private initiative established in the United States in 1985 to provide guidance on internal control, risk management, and fraud deterrence (Vincent & Barkhi, 2021). The COSO framework of internal control, based on five components - control environment, risk assessment, control activities, information and communication, and monitoring - is a widely recognized standard for designing, implementing, and evaluating internal control (Vincent & Barkhi, 2021). Organizations of all types and sizes use the framework to enhance their ability to manage risks, achieve operational excellence, and maintain financial reporting integrity. This article provides an overview of the COSO framework and its components (Vincent & Barkhi, 2021).

3. The Five Components of the COSO Framework Internal Controls

A set of rules reinforces the five components of the revised COSO internal controls framework (Chiu & Wang, 2019). The five crucial components: "control environment, risk assessment, control activities, information and communication, and monitoring," have corresponding 17 internal control principles that define them (COSO, 2013; Chiu & Wang, 2019, p. 91). Each principle describes the inputs required for each component to effectively steer the decision-making procedure from within the organization. Hence, the decision-makers in the organization can use these rules and principles to control or mitigate the risks related to their business strategy and goals (Chiu & Wang, 2019).

4. Components of Internal Control and Each Component's Impact on Each of the COSO Framework Objectives

4.1. Control Environment

The control environment collects norms, models, procedures, and establishments that require implementing internal control activities within the business structure (COSO, 2013). Hence, the board and executive management team dictate the accepted conduct from the top related to the significance of internal control and the anticipated standards of behavior (COSO, 2013). Here are the five principles associated with the control environment component:

- The institution exhibits a devotion to the integrity and moral values of the business and the framework permitting the board to discharge its governance oversight duties (COSO, 2013).
- The board affirms autonomy from executive management and exerts administration of the growth and implementation of internal control (COSO, 2013).
- In line with board oversight, the executive management institutes organization structures, controls, and obligations in pursuing the objectives (COSO, 2013).
- The institution is devoted to developing human resources and capital to align with the strategy and business goals (COSO, 2013).
- The institution holds everyone accountable for their internal control obligations in pursuing the objectives (COSO, 2013).

4.2. Risk Assessment

Organizations worldwide face risks within and without their business environment (COSO, 2013). Risk is the probability that an event will happen and negatively distort the accomplishment of objectives (COSO, 2013). Risk evaluation entails a vigorous and periodic procedure to pinpoint and evaluate the accomplishment of objectives; hence, risk appraisal constitutes the rationale for deciding risk management (COSO, 2013). Here are the four principles associated with the risk assessment component:

- The institution establishes objectives adequately to facilitate the designation and evaluation of risks associated with objectives (COSO, 2013).
- The institution pinpoints risks to accomplishing its objectives within the organization and evaluates risks as a rationale for deciding risk management (COSO, 2013).
- The institution assesses the possibility of fraud in evaluating risks to accomplish business objectives (COSO, 2013).
- The institution recognizes and evaluates transformations that could seriously affect internal control procedures (COSO, 2013).

4.3. Control Activities

These activities are founded on policies and processes to guarantee that the executive management mandate to alleviate risks to accomplish the objectives is perfectly executed (COSO, 2013). Thus, control exercises must be at every strategic business unit and different phases of the business procedure and the technology domain (COSO, 2013). The primary purpose is preventing, controlling, or detecting various manual and automated actions for potential risks. (COSO, 2013). Here are the three principles associated with the control activities component:

- The institution specifies and generates control exercises that aid the alleviation of risks to attain objectives at permissible grades (COSO, 2013).
- The institution specifies and generates unrestricted control actions on technology to sustain the accomplishment of objectives (COSO, 2013).
- The institution positions control activities through business policies that specify the expectations and practices that safeguard the policies (COSO, 2013).

4.4. Information and Communication

Collecting and transmitting critical information demands continuous action from within and without the organization to sustain the efficacy of other components of internal control (COSO, 2013). Hence, an institution must promptly apprehend, process, control, and communicate appropriate information to recognize inherent risks that could impact business objectives (COSO, 2013). Thus, it is essential to pinpoint the kind and range of data gathering based on its usefulness and priority (Jin & Kim, 2018). The COSO framework is only as potent as the procedures designed to observe, communicate, and inform on the position of the risk profile within the institution. This will permit the business to utilize relevant insights from the data-driven conclusions to attain its objectives (COSO, 2013). Here are the three principles associated with information and communication components:

- The institution receives, develops, and employs appropriate, accurate information to maintain the robustness of internal control (COSO, 2013).
- The institution internally disseminates information, including objectives and obligations for internal control, required to sustain the effectiveness of internal control (COSO, 2013).
- The institution relates issues impacting internal control activities and performance with external players (COSO, 2013).

4.5. Monitoring Activities

At this stage, the current assessment, independent appraisals, or mixtures of both will help determine if every one of the five components of internal control is correct, active, and influential on the business objectives (COSO, 2013). Therefore, ongoing appraisals are inculcated into the business procedure at various phases of the organization structure to give information promptly (COSO, 2013). However, independent routine appraisals differ in coverage and timing based on evaluating risks, the significance of the current assessment, and other administrative concerns (COSO, 2013). Here are the two principles associated with monitoring activities components:

- The institution chooses, designs, and conducts a continuous and independent assessment to prove if the components of internal control are current and influential (COSO, 2013).
- The institution promptly assesses and conveys internal control shortcomings to those liable for correcting the irregularities, including executive management and the board (COSO, 2013).

4.6. Objectives

An explicit connection exists between the objectives: what an organization aspires to accomplish. However, the components depict the conditions necessary to accomplish the objectives and the organization's business structure (COSO, 2013). The COSO 2013 revamped framework, best described through the COSO cube, integrates three objectives as its viewpoints, scilicet - operations, reporting, and compliance (Chiu & Wang, 2019).

The COSO framework includes three risk management objectives that permit the organizations to aim at different areas of internal control:

- Operations objectives – It focuses on the effectiveness and efficiency of business operations, including operational and financial performance objectives and protecting organization assets (COSO, 2013).
- Reporting objectives – It concentrates on internal and external reporting, financial and non-financial (COSO, 2013). The controls may contain dependability, promptness, transparency, or other concepts stipulated in guidelines (COSO, 2013).
- Compliance objectives address adherence to pertinent laws and regulations (COSO, 2013).

To reduce the risk of non-performance or inability to accomplish all the objectives satisfactorily (COSO, 2013). The organization must ensure that every five components and corresponding principles are present and performing (COSO, 2013). 'Present' guarantees that the business tenets are available and that the internal control system execution is precise to achieve established objectives (COSO, 2013). "Functioning" connotes the assurance that the components and applicable tenets endure in the reality of the operations and behavior of the internal control system to accomplish established objectives (COSO, 2013).

The five components operate together for effectiveness. "Operating together" connotes that the five components of internal control alleviate the risk of not attaining an objective satisfactorily (COSO, 2013). Components, although autonomous, function together as a joint system to accomplish established objectives (COSO, 2013).

5. Auditors' Most Concern during an IT Audit

Emerging technologies and innovation are critical for organizations to compete; however, the more sophisticated an organization becomes in embracing technology, the more challenge it creates for the IT audit industry (ISACA, 2019). The outcome of the survey response from 2,252 IT audit professionals and experts identified IT security and privacy as the number one issue IT auditors encounter (ISACA, 2019). Hence, IT auditors are concerned about understanding the complexities of new technologies and how they can manage them effectively to safeguard an organization's assets (ISACA, 2019). IT auditors must stay ahead of any risks or threats from emerging technologies (ISACA, 2019)

6. Recommendations for Integrating COSO Framework Compliance into an Organization Information Technology Plan

Here are the five steps:

6.1. Step 1: Planning and Scoping

Everyone in the management team must share the same mindset on adopting the framework and work to designate the implementation team (Schandl & Foster, 2019). The next move is to design an implementation plan comprising timing, resources required, risk assessment, functions, and duties of implementation team members (Schandl & Foster, 2019). The team needs to comprehend the COSO framework, its five components, and its principles (Schandl & Foster, 2019).

6.2. Step 2: Assessment and Documentation

The team will conduct a fraud risk assessment to understand how a malicious person may bypass the company's internal controls or attack the organization's network structure (Schandl & Foster, 2019). Other activities at this step will include assessing fraud risk, documenting existing processes and controls, and performing gap assessments (Schandl & Foster, 2019).

6.3. Step 3: Remediation Planning and Implementation

Immediately after the company pinpoints all its gaps, the amendments will begin by executing the COSO framework (Schandl & Foster, 2019).

6.4. Step 4: Design, Testing, and Reporting Controls

Testing will occur to check if the controls are adequate and repeatable. There will be a classification of controls as critical or non-critical, and the testing procedure for each control will be to inquire, observe, examine, and analyze (Schandl & Foster, 2019).

6.5. Step 5: Optimization of the Effectiveness of Internal Controls

At this point, we assume the COSO framework implementation is booming, and automation will become paramount to the business (Schandl & Foster, 2019).

7. The COSO Framework Enterprise Resource Management

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) released the revised version of Enterprise Risk Management - "Integrating with Strategy and Performance" in 2017 to manage the intricacies of risk that have increased within the business environment (COSO, 2017; Vincent & Barkhi, 2021). The COSO Framework is an approach to instituting internal controls to be infused into organizations' enterprise procedures. These controls aim to ascertain that the business is transparent, accountable, ethical, and responsible in its activities within the instituted enterprise norms (Chiu & Wang, 2019).

8. The Five Components of the COSO Framework Enterprise Resource Management

A set of rules reinforces the five components in the revised COSO framework for Enterprise Risk Management (ERM), covering everything from governance to monitoring (COSO, 2017). The revamped framework concentrates on five components: (1) governance and culture, (2) strategy and objective setting, (3) performance, (4) review and revision, and (5) information, communication, and reporting (COSO, 2017; Vincent & Barkhi, 2021, p. 61). These rules are nimble and valuable in many manners for businesses, no matter the size, kind, or industry. Also, a COSO ERM Framework has 20 principles that define the five components. The individual principle describes the inputs required for each component to steer the decision-making procedure from within the organization effectively. Hence, the decision-makers in the organization can use these rules and principles to control or mitigate the risks related to their business strategy and goals (COSO, 2017). Here are the five rules and twenty principles:

8.1. Governance and Culture

This component is vital to the framework of COSO ERM. Governance dictates the business responsibility by emphasizing the benefits of instituting administrative duties for ERM. However, culture sets the tone for expected conduct, moral values, and possessing the required knowledge of the risk to the institution. Here are the five principles associated with governance and culture framework component:

- Exercises Board Risk Oversight - The board of directors supervises strategy execution and oversees governance obligations to help executive management realize strategic and business goals.
- Establishes Operating Structures - The institution sets standard operating procedures and required working structures to enable the entire team to pursue the strategy and business goals effectively.
- Defines Desired Culture - The institution outlines the preferred demeanors and conducts representing the expected culture of the organization.
- Demonstrates Commitment to Core Values - The institution exhibits a commitment, devotion, and dedication to the organization's core values.
- Attracts, Develops, and Retains Capable Individuals - The institution is devoted to developing human resources and capital to align with the strategy and business goals.

8.2. Strategy and Objective-Setting

This component seeks to understand the business ecosystem where the business operates. Thus, strategy and objectives assist the organization in recognizing and describing a risk profile that will guide the business to achieve business objectives. The business risk profile will be the basis for the organization to develop business strategies that align with its risk profile and goals. Businesses must continuously seek other means to strategize and mitigate potential risks in their profiles. Here are the four principles associated with strategy and objective-setting framework component:

- Analyzes Business Context - The institution evaluates the possible influences of business context on its risk profile. The evaluation will drive the organization’s mission and core values effectively.
- Defines Risk Appetite - The institution outlines its risk appetite for maintaining, building, realizing, and recognizing value. Hence, the organization defines the amount and kinds of risk it is willing to tolerate to sustain a competitive edge.
- Evaluates Alternative Strategies - The institution weighs other strategies and likely outcomes on its risk profile to make salient business decisions that will contribute to its business objectives.
- Formulates Business Objectives - The institution evaluates risk while documenting the objectives of each strategic business unit of the organization that aligns its strategy with the business goals.

8.2.1. Performance

This component is vital in determining the effect of a particular risk that may hamper business growth and an organizational capacity to deliver on its business goals. Risks are itemized based on their stringency as classified by the organization's risk appetite. Thus, these guidelines permit an institution to pinpoint and prioritize risks that may interfere

with its business activities. A complete risk profile enables an institution to pinpoint, evaluate, prioritize, respond, and produce a portfolio hypothesis of risk, helping to mitigate recognized risks aggressively. Here are the five principles associated with the performance framework component:

- Identifies Risk - The institution pinpoints risk that hinders the implementation, execution, and performance of the strategy and business goals.
- Assesses Severity of Risk - The institution evaluates the stringency of risk that may hamper the attainment of business strategies and goals.
- Prioritizes Risks - The institution's priority is the rationale for choosing tenable actions to mitigate the risks. Therefore, the severity of the risk determines the appropriate response to help the organization reach its goals.
- Implements Risk Responses - The institution pinpoints, specifies, and chooses risk feedback based on an outline for risk identification.
- Develop Portfolio View - The institution plans, designs, and assesses a portfolio outlook of risk; hence, the business can manage risk effectively.

8.2.2. Review and Revision

This component ensures continuous assessment of an organization's performance benchmarked against the adopted framework based on the COSO ERM program. Thus, as the organization's business climate transforms, assessing the possible consequences of those transformations requires attention to guarantee the effectiveness of the established framework within the ERM program. The business will continue examining and modifying its ERM capacities and procedures based on strategy and business goal shifts. Here are the three principles associated with the review and revision framework component:

- Assesses Substantial Change - The institution pinpoints and evaluates shifts that may seriously impact strategy and business goals.
- Reviews Risk and Performance - The institution examines and reevaluates business effectiveness and performance while considering risk.
- Pursues Improvement in Enterprise Risk Management - The institution seeks continuous improvement and refinement of business risk administration.

8.3. Information, Communication, and Reporting

This component is crucial to the framework of the COSO ERM. Collecting and transmitting critical information within the Enterprise risk management demands continuous action from within and without the organization. Hence, an institution must promptly apprehend, process, control, and communicate appropriate information to recognize inherent risks that could impact strategy and business goals. A COSO ERM framework is only as practical and potent as the procedures designed to observe, communicate, and inform on the position of the risk profile within the institution, which will permit the business to utilize relevant insights gained from the data-driven conclusions to attain its objectives. Here are the three principles associated with information, communication, and reporting framework components:

8.3.1. Leverages Information and Technology

The institution utilizes business information technology (IT) strategies to support and manage the ERM. The transformation of IT system abilities with constant business process redesign will provide a business with an agile decision-making platform to adjust to a fiercely changing business environment.

8.3.2. Communicates Risk Information

The institution employs various communication media to brace its ERM.

8.3.3. Reports on Risk, Culture, and Performance

The institution analyzes, reviews, and reports on risk, organizational culture, and business performance at various levels of the organizational structure**.**

9. Conclusion

COSO frameworks furnish a way for organizations to oversee their business climate and provide more significant assurance to realize strategic objectives through their governing components, principles, and objectives that rely strenuously on risk management (Vincent & Barkhi, 2021). Organizational compliance using the Sarbanes-Oxley Act of 2002 (SOX) is another regulatory suggestion for an organization; SOX requires sufficient internal control measures to guarantee the exactness of all business activities from the start through subsequent processing and reporting (Schiff & Warren, 2017).

Vincent and Barkhi (2021) assert that the crucial linkage between internal control and IT systems lies in the provision of unambiguous directives regarding what the systems should or should not perform. Failure to establish such expectations may result in a significant adverse effect on the accuracy of a company's financial statements. Hence, IT control expectations must be given to the business and its regulators. The same perspective will be what an auditor expects: the systems of control function as intended, are effective, and completely cover the business or the regulator's requirements (Vincent & Barkhi, 2021). The COSO framework guidelines are valuable in many ways for institutions that want to remain competitive, no matter the size, kind, or industry (Schandl & Foster, 2019).

10. References

i. Calagna, K., Cassidy, B., & Park, A. (2021, September). Realize the full potential of artificial intelligence: Applying the COSO framework and principles to help implement and scale artificial intelligence. *Committee of Sponsoring Organizations of the Treadway Commission (COSO)*. Retrieved from https://www.coso.org/Shared%20Documents/Realize-the-Full-Potential-of-Artificial-Intelligence.pdf

ii. Chiu, T., & Wang, T. (2019). The COSO framework in emerging technology environments: an effective in-class exercise on internal control. *Journal of Emerging Technologies in Accounting*, 16(2), 89–98. https://doi.org/10.2308/jeta-52500

iii. *COSO*. (2013, May). Internal Control-Integrated Framework. *Committee of Sponsoring Organizations of the Treadway Commission*. Retrieved from https://www.coso.org/Shared%20Documents/Framework-Executive-Summary.pdf

iv. *IRM*. (2019). From the cube to the rainbow double helix: a risk practitioner's guide to the COSO ERM Frameworks. *Institute of Risk Management*. Retrieved from https://www.theirm.org/media/6909/irm-report-review-of-the-coso-erm-frameworks-v2.pdf

v. *ISACA*. (2019, October 30). The top challenges facing IT auditors. Retrieved from https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2019/volume-22/the-top-Mass-facing-it-auditors

vi. Jin, D.-H., & Kim, H.-J. (2018). An integrated understanding of big data, big data analysis, and business intelligence: a logistics case study. *Sustainability (Basel, Switzerland)*, 10(10), 3778–. https://doi.org/10.3390/su10103778

vii. Schandl, A., & Foster, P.L. (2019). COSO internal control – integrated framework: An implementation guide for the healthcare provider industry. *Crowe*. Retrieved from https://www.coso.org/Shared%20Documents/CROWE-COSO-Internal-Control-Integrated-Framework.pdf

viii. Schiff, A.D., & Warren, M. T. (2017). Implementing a business intelligence (BI)/corporate performance management (CPM) solution: challenges a major national retailer faces. *Journal of Business Case Studies*, 13(2), 63–72. https://doi.org/10.19030/jbcs.v13i2.9938

ix. Vincent, N.E., & Barkhi, R. (2021). Evaluating Blockchain Using COSO. *Current Issues in Auditing*, 15(1), A57–A71. https://doi.org/10.2308/CIIA-2019-509

x. Walker, P.L., & Schiro, J.J. (2022, February). Enabling organizational agility in an age of speed and disruption. *Committee of Sponsoring Organizations of the Treadway Commission (COSO)*. Retrieved from https://www.coso.org/Shared%20Documents/Enabling-Organizational-Agility-in-an-Age-of-Speed-and-Disruption.pdf