IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 1, January 2024

DOI: 10.17148/IARJSET.2024.11123

A Consideration of Practical Strategies when Implementing Information Technology General Controls in a Sarbanes Oxley Compliant Environment

Sulyman, D. Kehinde

London Metropolitan University

Abstract: The Sarbanes-Oxley (SOX) Act in the United States has fundamentally changed the Western World's business regulatory environment. The Act itself aims to enhance corporate governance through measures that will strengthen internal checks and balances and, ultimately, strengthen corporate accountability. However, it is important to emphasize that the Act not only requires that senior management and business process owners establish and maintain an adequate internal control structure, but also assess the effectiveness of such control(s) on an annual basis. It is against this background that this dissertation considers the formulation of a suitable set of strategies in the form of a policy document to act as a tool to assist and guide management and owners in implementing general Information Technology /Information System controls in a SOX compliant environment.

Keywords: Information Technology, Sarbanes-Oxley, Business Regulation, Corporate Accountability

I. INTRODUCTION

As a result of the financial scandals at major Fortune 100 companies in 2001, Congress enacted the Sarbanes-Oxley (SOX) Act of 2002 [1]. This act affects how public companies report financials and significantly impacts IT. Sarbanes-Oxley compliance requires more than documentation and/or establishment of financial controls; it also requires the assessment of a company's IT infrastructure, operations, and personnel [2]. Unfortunately, the requirements of the Sarbanes-Oxley Act of 2002 do not scale based on the size or revenue of a company [3]. Small to medium-sized companies (IT department) will face unique challenges, both budgetary and with personnel, in their effort to comply with the Sarbanes-Oxley Act of 2002 [1]. With the passage of legislation such as the Sarbanes-Oxley Act of 2002 (SOX), the notion of IT control has acquired a new importance for public companies [4]. The Act provides for new corporate governance rules and standards that mandate effective internal controls over financial reporting and establish clear executive accountability for the integrity of those reports [4].

Publicly traded U.S.-based companies must now be prepared for addressing SOX requirements, including SOX-compliant IT control processes, which could alter the claims that corporations make to upcoming annual reports. Companies must ensure their financial processes comply with SOX legislation, and senior executives must attest to the adequacy and effectiveness of their internal control of these processes [5]. Thus, achieving and maintaining compliance with the general IT controls specified in Section 404 of SOX involves far more than just establishing rigid control over various processes and access to information [6]. It requires merging people, processes and technology into a unified, enterprise-wide compliance effort.

II. RELATED STUDIES

SOX and IT

Sarbanes-Oxley compliance will significantly impact the IT organization of most public companies [1]. However, there is one enormous problem: there is no specific mention of IT in Section 404, and more importantly, there are no specifics as to what controls have to be established within an IT organization to comply with Sarbanes [3]- Oxley legislation. However, to comply with SOX 404, management needs to assess the design and operating effectiveness of internal controls over financial reporting. The relationship with IT has three characteristics [7]:

- The key controls can be manual, automated or a combination of both
- The PCAOB's Accounting Standard does not differentiate between manual or automated controls

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 1, January 2024

DOI: 10.17148/IARJSET.2024.11123

- All key controls for all relevant assertions relating to significant accounts and disclosure need to be assessed and an inventory of these controls created.

The United States Security Exchange Commission (SEC) considers a control to be 'key' if the organization relies on it to ensure that there are no material misstatements in the financial accounts [8]. Management is required to demonstrate that all key controls are operating effectively. This means that management must 'test' their controls on a yearly basis in order to satisfy this stipulation [3]. Although IT controls are deemed to be pervasive under the Act, an organization may choose to employ a layer of mitigating manual controls that effectively eliminate the reliance on automated technology-based controls [9]. Automated controls are considered to be repeatable under the Act and therefore only need to be tested on one transaction to prove effectiveness, as opposed to substantively (many transactions) for manual or semi-automated controls [9]. In practice, it is in all likelihood, as difficult to demonstrate that nothing has changed as it is to test the control [10].

However, the Act may well be amended to reflect this point of view. Although the SEC does not differentiate between manual and automated controls, there is clearly a case for arguing that automated controls will be more efficient in many circumstances [11]. Of course, the reality for most companies is that their key controls will consist of an amalgam of automated, semi-automated and manual controls [12]. Thus, whatever form this combination takes, the underlying technology/ infrastructure needs to be operating effectively for a company's key controls to be deemed effective.

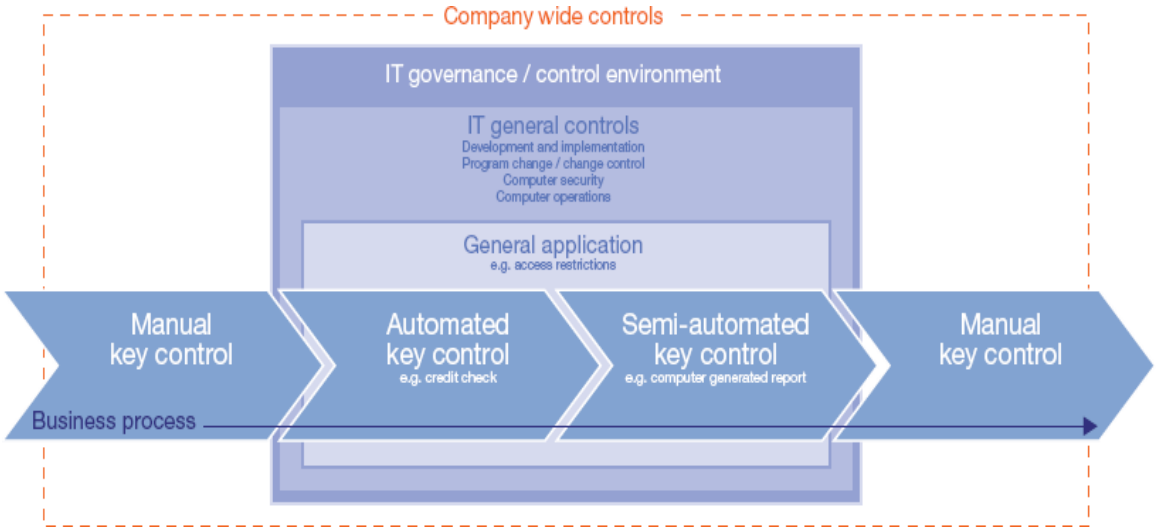
IT General Controls (ITGC)

IT General Controls are policies and procedures that relate to many applications and support the effective functioning of applications controls by helping to ensure the continued proper operation of information systems [13]. This are controls embedded within IT processes that provide a reliable operating environment and support the effective operation of application controls [14] include:

- Program Development
- Program Changes
- Access to Programs and Data
- Computer Operations

With widespread reliance on IT systems, controls are needed over such systems, large and small. IT controls commonly include controls over the IT environment, computer operations, access to programs and data, program development, and program changes [14]. These controls apply to systems that have been determined to be financially significant. The SEC considers IT General Controls (ITGC) to be pervasive in nature; that is to say, any deficiencies arising in any of these controls will undermine the validity of automated controls, meaning that they can no longer be relied upon in financial reporting.

Figure 1. Sarbanes Oxley views of Information Technology General Controls



Source: Lenn [1]

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 1, January 2024

DOI: 10.17148/IARJSET.2024.11123

ITGC can be divided into four domains [15]. These are:

- Development and Implementation
- Program Change or Change Control
- Computer Security
- Computer Operations

Development and Implementation

Software development may take place in a number of scenarios. It might occur as part of the development or enhancement of a generic software package, as local customization of a package during its implementation for an individual business, or as one-off in-house development for a specific business, whether performed by an external software house or by an internal IT department [15]. Whatever the scenario, the same control regime is required although the mechanism for monitoring them will vary.

Program Change or Change Control

Changes to an established system, whether due to a planned upgrade or to an emergency update will require verification that the controls already in place are not adversely impacted by the change [16]. Updates to packaged software and changes to locally developed software must follow the same cycle as initial development, including review of the changes, documentation and test of changed procedures and updates to documentation, as well as a review of the data security and control aspects [16].

Computer Security

The operation and administration of the security function of IT systems needs to be a key area of focus in a Sarbanes Oxley compliance programme [17]. The security system forms the first line of defense against inappropriate access. With this in mind, the security system should have a number of automated characteristics to mitigate risk [18]. For example, when new users are added to the system the default should be to grant them limited or no access, with any access having to be positively granted by an administrator. Periodic checks should be performed across all systems to report on and retire users that have been dormant [19]. Only appropriate levels within an organization should have access to duties that should otherwise be separated. Therefore. the security administration system should itself be controlled, capable of restricting access to certain functions, and reporting on who granted (and/or removed) access rights to a particular employee, where appropriate, controls should be included to ensure transactions cannot be denied by either party and provide non-repudiation of origin or receipt, proof of submission and receipt of transactions [19]. This is particularly important for transactions received electronically but might also be relevant to the recording of proof-of-delivery documentation.

Computer Operations

The day-to-day running of systems is an essential part of business continuity planning. This should include monitoring of attempted or actual security breaches, capacity and availability monitoring, as well as ensuring security backups [20].

In the Sarbanes Oxley era, it is important to identify the critical application programs, third party services, operating systems, personnel and supplies, data files, and time frames needed for recovery [2]. In addition to the more obvious concerns around continued availability of services, businesses may wish to consider a number of more specific items [1]. For example, escrow agreements can provide security in the event the software provider can no longer continue support, failsafe and/or fall-over systems may provide added security, and source documents must be retained or be reproducible for an adequate amount of time, with suitable backup procedures in cases where these are stored electronically.

Sarbanes-Oxley and its impact on IT General Controls

With the widespread use of IT systems, from mainframe through client-server environments, any system of internal controls must include Information Technology controls [13]. Sarbanes-Oxley Act makes corporate executives explicitly responsible for establishing, evaluating and monitoring the effectiveness of internal control over financial reporting [13]. For most organizations, the role of IT will be crucial to achieving these objectives. Some of the key areas of responsibility for IT [11] include:

- Understanding the organization's internal control program and its financial reporting process.
- Mapping the IT systems that support internal control and the financial reporting process to the financial statements.
- Identifying risks related to these IT systems.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 1, January 2024

DOI: 10.17148/IARJSET.2024.11123

- Designing and implementing controls designed to mitigate the identified risks and monitoring them for continued effectiveness.
- Documenting and testing IT controls.
- Ensuring that IT controls are updated and changed, as necessary, to correspond with changes in internal control or financial reporting processes.
- Monitoring IT controls for effective operation over time.
- Participation by IT in the Sarbanes-Oxley project management office.

To comply with Sarbanes-Oxley, organizations must understand how the financial reporting process works and must be able to identify the areas where technology plays a critical part. In considering which controls to include in the program [21], organizations should recognize that IT controls can have a direct or indirect impact on the financial reporting process [21]. For instance, IT application controls that ensure completeness of transactions can be directly related to financial assertions. Access controls, on the other hand, exist within these applications or within their supporting systems, such as databases, networks and operating systems, are equally important, but do not directly align to a financial assertion [22]. Application controls are generally aligned with a business process that gives rise to financial reports. While there are many IT systems operating within an organization, Sarbanes-Oxley compliance only focuses on those that are associated with a significant account or related business process [21].

Sarbanes-Oxley primarily affects public companies with a market capitalization of $75 million listed on U.S. exchanges [3]. Sarbanes-Oxley is strictly focused on financial reporting and does not specifically address IT [3]. However, IT does affect the reliability and security of systems in which companies keep their financial records. There are several titles and sections in the Sarbanes-Oxley Act that has a direct impact on internal controls (including IT controls) [16].

IT General Controls Problems

The Sarbanes-Oxley Act makes corporate executives explicitly responsible for establishing, evaluating and monitoring the effectiveness of internal control over financial reporting [16]. For most organizations, the role of IT is crucial to achieving this objective. Whether through a unified ERP system or a disparate collection of operational and financial management software applications, IT is the foundation of an effective system of internal control over financial reporting [23]. During the research for this project, it was discovered that this situation creates a unique challenge: many of the IT professionals being held accountable for the quality and integrity of information generated by their IT systems are not well versed in the intricacies of internal control [17]. This is not to suggest that risk is not being managed by IT, but rather that it may not be formalized or structured in a way required by an organization's management or its auditors.

While some industries, such as financial services, are familiar with stringent regulatory and compliance requirements of public market environments, most are not [24]. To meet the demands of the Sarbanes-Oxley Act, most organizations are in the process of a change in culture. Enhancements to IT systems and processes have been required, most notably in the design, documentation, retention of control evidence and evaluation of IT controls [22].

Overviews of Control Frameworks

Since corporate financial structures are so diverse, there is no single formula for compliance that would fit every affected public company [25]. However, general corporate control guidelines can help companies determine their necessary courses of action for complying with SOX Section 404. Per a report for Public Accounting Oversight Board (PCAOB [26]) 3 briefing paper:

"The SEC's final rules specified that management must base its evaluation of the effectiveness of the company's internal control over financial reporting *on a suitable, recognized control framework that is established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment. (p.*4)"

In a recent survey, 58 percent of respondents indicated that they leveraged the COBIT framework to reduce risk in key financial systems [27]. Thirty percent pointed to *IT Control Objectives for Sarbanes-Oxley*, a publication from the IT Governance Institute. COSO was used by 36 percent. Understanding these IT governance/control frameworks and how they fit into an internal control system is essential for every organization under SOX [28].

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 1, January 2024

DOI: 10.17148/IARJSET.2024.11123

IT Control Objective - COBIT

The Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for information (IT) management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992. COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company [29]. COSO does not provide specific IT control objectives. There are some generally recognized standards that provide guidance on IT control objectives [30]. Though Cobit is intended for use by business process owners as well as auditors, it occupies an important place among IT auditors. ISACA's objective in developing Cobit categorized IT processes into four domains [31]:

Domain 1: Plan and Organization

The Planning and Organization domain covers the use of information & technology and how best it can be used in a company to help achieve the company's goals and objectives. It also highlights the organizational and infrastructural form IT is to take in order to achieve the optimal results and to generate the most benefits from the use of IT. The following table lists the high-level control objectives for the Planning and Organization domain [31].

Table 1. High Level Control Objectives (Plan and Organise)

PO1	**Define a Strategic IT Plan and direction**
PO2	**Define the Information Architecture**
PO3	**Determine Technological Direction**
PO4	**Define the IT Processes, Organization and Relationships**
PO5	**Manage the IT Investment**
PO6	**Communicate Management Aims and Direction**
PO7	**Manage IT Human Resources**
PO8	**Ensure Compliance with External Requirements**
PO9	**Assess and Manage IT Risks**
PO10	**Manage Projects**
PO11	**Manage Quality**

Domain 2: Acquire and Implement

The Acquire and Implement domain covers identifying IT requirements, acquiring the technology, and implementing it within the company's current business processes. This domain also addresses the development of a maintenance plan that a company should adopt in order to prolong the life of an IT system and its components [31]. The following table lists the high-level control objectives for the Acquisition and Implementation domain.

Table 2. High Level Control Objectives (Acquire and Implement)

AI1	**Identify Automated Solutions**
AI2	**Acquire and Maintain Application Software**
AI3	**Acquire and Maintain Technology Infrastructure**
AI4	**Enable Operation and Use**
AI5	**Procure IT Resources**
AI6	**Manage Changes**
AI7	**Install and Accredit Solutions and Changes**

Domain 3: Delivery and Support

The Delivery and Support domain focuses on the delivery aspects of the information technology. It covers areas such as the execution of the applications within the IT system and its results, as well as the support processes that enable the effective and efficient execution of these IT systems [31]. These support processes include security issues and training. The following table lists the high-level control objectives for the Delivery and Support domain.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 1, January 2024

DOI: 10.17148/IARJSET.2024.11123

Table 3. High Level Control Objectives (Deliver and Support)

DS1	**Define and Manage Service Levels**
DS2	**Manage Third-party Services**
DS3	**Manage Performance and Capacity**
DS4	**Ensure Continuous Service**
DS5	**Ensure Systems Security**
DS6	**Identify and Allocate Costs**
DS7	**Educate and Train Users**
DS8	**Manage Service Desk and Incidents**
DS9	**Manage the Configuration**
DS10	**Manage Problems**
DS11	**Manage Data**
DS12	**Manage the Physical Environment**
DS13	**Manage Operations**

Domain 4: Monitor and Evaluate

The Monitoring and Evaluation domain deals with a company's strategy in assessing the needs of the company and whether or not the current IT system still meets the objectives for which it was designed and the controls necessary to comply with regulatory requirements. Monitoring also covers the issue of an independent assessment of the effectiveness of IT system in its ability to meet business objectives and the company's control processes by internal and external auditors [31]. The following table lists the high-level control objectives for the Monitoring domain.

Table 4. High Level Control Objectives (**Monitor and Evaluate)**

ME1	**Monitor and Evaluate IT Processes**
ME2	**Monitor and Evaluate Internal Control**
ME3	**Ensure Regulatory Compliance**
ME4	**Provide IT Governance**

For each high-level process, Cobit provides a set of control objectives with associated practices to mitigate risk related to the effectiveness, efficiency, confidentiality, integrity, availability, compliance, or reliability of IT systems and processes [32].

Internal Control Framework - COSO

Although SOX does not mandate detailed control activities, the SEC requires the use of a recognized internal control framework. In its final rule, the SEC specifically mentions the control framework from the Committee of Sponsoring Organizations of the Treadway Commission (COSO) as satisfying the controls requirement under SOX. COSO is the most commonly used control framework in the U.S. and has been adopted by most auditing organizations [33]. However, any framework, such as Cadbury or CoCo, that encompasses the same scope and general themes as COSO is acceptable.

COSO defines the internal control process as follows: Internal control is broadly defined as a process, affected by an entity's Board of Directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with laws and regulations [34]. The internal control process consists of five components:

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 1, January 2024

DOI: 10.17148/IARJSET.2024.11123

- **Control Environment** – the control environment is typically understood as the "tone at the top." Control environment factors include "the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility and organizes and develops its people; and the attention and direction provided by the board of directors [34].

- **Risk Assessment** – As we discussed above, internal control practices are responses to some risk. Consequently, the internal control process must include assessment of relevant risks. Risk assessment is the identification and analysis of relevant risks to the achievement of the organization's objectives [33].

- **Control Activities** – Control activities are mechanisms that help mitigate the risks uncovered by the risk assessment. They are the policies and procedures that "help ensure that necessary actions are taken to address risks to achievement of the entity's objectives [34].

- **Information and Communication** – The relevant information must be available to help people perform their duties. This includes reports that contain "operational, financial and compliance-related information, that make it possible to run and control the business [32]. It also includes information about external events and conditions necessary for informed business decision-making.

- **Monitoring** – Internal control systems must be monitored over time to ensure that their objectives are being met. This is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two. Control deficiencies must be identified and communicated up to the appropriate levels of management [34].

These components represent the important factors of a well-designed system of controls. The importance of each factor may vary depending upon the organization and the control objective, but the general principles should be present in every system of control [35].

Adopting a Control Framework

For years, IT has played an important role in the operation of strategic and managerial information systems. Today, these systems are inseparable from an organization's ability to meet the demands of customers, suppliers and other important stakeholders [36]. With widespread reliance on IT for financial and operational management systems, controls have long been recognized as necessary, particularly for significant information systems [37].

For Sarbanes-Oxley IT General Control compliance efforts, it is important to demonstrate how IT controls support the COSO framework. A successful organization is built on a solid framework of data and information. The Framework explains how IT processes deliver the information that the business needs to achieve its objectives [37].

For COBIT, this delivery is controlled through 34 high-level control objectives, one for each IT process, contained in the four domains [36]. The Framework identifies which of the seven information criteria (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability), as well as which IT resources (people, applications, technology, facilities and data) are important for the IT processes to fully support the business process [38].

For COSO, an organization should have IT control competency in all five of the components COSO identifies as essential for effective internal control [39]. They are: Control environment; Risk assessment; Control activities; Information and communication, and Monitoring [39].

Implementing a Control Framework

Major auditing firms agree that the most effective strategy for moving IT toward SOX compliance [40] involves:

- Assessing current IT controls against established COBIT standards
- Upgrading any IT controls identified as deficient to a COBIT maturity level 3 - Maturity level 3 equates to a Defined Process, which implies that 1) the need to act with regard to IT governance is widely accepted within an organization; 2) procedures have been standardized, documented, and implemented; and 3) tools have been standardized with the use of currently available technology.

Of course, any plan for SOX compliance needs to be reviewed and approved by an independent, external auditing firm. While the outside auditor cannot be responsible for designing or implementing the 404 systems, they should be involved early in the process. The outside auditor can evaluate, review, recommend, and weigh in on approach and process [40]. It is better to know what the outside auditor's views are on key controls and sample size, for example, from the start.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 1, January 2024

DOI: 10.17148/IARJSET.2024.11123

Gap and Conclusion in Literature Review.

Implementing IT General Controls for Sarbanes-Oxley, where few existed before, has become a significant challenge for most organizations. In many cases, the finance organization within a company has been familiar with the need for controls and related documentation because they have been part of financial audits for years. Much has been written about the challenges and problems that serve as impediments in the implementation of ITGC in a sox environment. However, IT organizations are less accustomed to these issues and, therefore, implementing controls that operate effectively over time has proven to be a difficult task.

Hence, to successfully implement and sustain ITGC controls, organizations first need to understand that compliance with Sarbanes-Oxley will likely involve change in current IT control practices.

III. METHODOLOGY

The study is of a qualitative character based on interviews, observations and my experience as part of a team that ITGC in a SOX compliant environment. Additionally, the quality of the study will be discussed based on the concepts validity and reliability. The analysis is based on the guidance presented by accounting firms as the solution to companies striving towards sustainable compliance to the Sarbanes-Oxley Act. Information from articles and literature on the topic is added to enrich the discussion. To obtain the desired result it is essential to select the proper approach (Patel, Davidson 2003).

The purpose of this study is to produce a best practice document, which will act as tool to assist and guide in the implementation of IT General Controls. To achieve this I intend to come out with a suitable strategy to follow when implementing ITGC in a SOX compliant environment. The research is designed to answer the question:

*"**Can the formulation of a set of suitable strategies in the form of a policy document act as a tool to assist and guide management and owners in implementing IT General Control in a SOX compliant environment*?"**

Research methodology therefore refers to the overall approach of the research process, from the theoretical underpinning to the collection and analysis of data (Collis & Hussey, 2003). One common classification of research methodology is a division into quantitative or qualitative studies, which refers to how information is gathered, processed and analyzed.

Policy Document
SOX ITGC Guidelines – Approach to IT General Controls
Objective

The objective of this document is to set out an approach to delivering Sarbanes- Oxley [Sox] compliance to IT General Controls [ITGC] that is tailored to the specific objectives and responsibilities of Information Technology. This document should not be regarded as definite steps to follow but each organization should carefully consider the appropriate approach necessary for its own circumstances.

Audience

This document will be distributed to and referenced by IT process owners and their respective project teams to understand the work needed to ensure Sarbanes-Oxley compliance for ITGC within the company. Any questions relating to content or use of this document should be referred via your process owner leader to your SOX Programme IT Co-ordinator.

Roadmap for IT General Control's compliance

This ITGC compliance roadmap provides directions and strategies for IT professionals on meeting the challenges of the SOX implementation. IT General Control's compliance is not a stand-alone process. It must be integrated within the over all business – led compliance process. IT General Controls support critical applications, underpin critical business Processes, and in turn are linked to financial reporting processes, risks and controls.

Plan and Scope

Scoping the project is one of the most important activities in the entire program. Organizations should form an IT control subcommittee that is integrated into, and reports to, the overall Sarbanes- Oxley steering committee. As a critical first step, organizations must understand how the financial reporting process works and identify where technology is critical in the support of this process. They should recognize that IT controls may have a direct or indirect impact on the financial reporting process.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 1, January 2024

DOI: 10.17148/IARJSET.2024.11123

Factors that should be considered when determining whether systems need to be reviewed and tested as part of a Sarbanes-Oxley compliance program include whether they process large volumes of transactions, process large dollar-value items, are used to process complex transactions or support highly sensitive financial data repositories.

Perform Risk Assessment

The next step in the road map is to perform risk assessments on the selected components. Risk assessment enables organizations to understand how events can inhibit the achievement of business objectives. The purpose of the risk assessment is to help determine the inherent and residual risks to establish the level of documentation and the extent of testing that needs to be performed.

Identify Significant Accounts/Controls

Organizations should first identify significant accounts that could have a material impact on the financial reporting and disclosure process. Once the significant accounts have been identified, application controls relevant to such accounts should be identified and documented. This should be done for application controls. IT general controls, organizations should assess those controls that support the quality and integrity of information and that are designed to mitigate the identified risks. Since company-level controls are primarily related to the control environment and risk assessment components of COSO, and their existence sets the tone for the effectiveness of all other controls, assessing company-level controls is a key objective for this phase

Document Control Design

Documentation should be prepared both at the entity level as well as the activity level regarding the objectives that the controls are designed to achieve to support the organization's internal control over financial reporting and disclosure controls and procedures. It is advisable that an organization document its approach to IT control, including the assignment of authority and responsibility for IT controls as well as their design and operation.

Evaluate Control Design

In this phase, an organization must step back and evaluate the ability of its control program to reduce IT risk to an acceptable level. More specifically, it requires that control attributes, including preventive, detective, automated and manual, be considered when designing an approach to effectively address risks. For example, if a change management risk is identified that would result in unauthorized programs being migrated into the production environment; a properly designed control would prevent this from occurring. In this example, a detective control that identifies unauthorized programs in production after the fact may not be appropriate.

Evaluate Operational Effectiveness

Once control design has been assessed, as appropriate, its implementation and continuing effectiveness must be confirmed. During this stage, initial and ongoing tests conducted by individuals responsible for the controls and the internal control program management team should be performed to check on the operating effectiveness of the control activities. Organizations should test controls upon which other significant controls depend more extensively (e.g., general controls as opposed to application controls) and with higher frequency. In making a judgment about the extent of testing that is appropriate, organizations should consider how the IT control impacts financial and disclosure reporting processes.

Build Sustainability

The final phase ensures that internal controls are sustainable. At this point, IT management should be in a position to sign off on the IT internal control program effectiveness. Control assessment and management competencies must become part of the IT department's organization and culture and must sustain themselves over the long term. Control is not an event; it is a process that requires continuous support and evaluation to stay current. To successfully sustain compliance, IT organizations are seeking to implement best practices that will help them become continuously high-performing organizations. In addition to simplifying audit readiness, this approach will also result in tighter security, increased system availability,

IV. CONCLUSION

Today, as every organization tries to deliver value from IT while managing an increasingly complex range of IT-related risks, the effective use of policy documents can help avoid re-inventing wheels, optimize the use of scarce IT resource and reduce the occurrence of major IT risks, such as: project failures; wasted investments; security breaches; system crashes; failures by service providers to understand and meet customer requirements IT best practices; IT policy documents; Management of IT; and governance of IT activities

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 1, January 2024

DOI: 10.17148/IARJSET.2024.11123

The growing adoption of IT best practices has been driven by a requirement for the IT industry to better manage the quality and reliability of IT in business and respond to a growing number of best practices, policy documents and regulatory requirements. There is a danger, however, that the implementation of this potential policy documents and best practices will be costly and unfocused if they are treated as a purely technical guidance. To be most effective, best practices and policy documents should be applied within the business context, focusing on where their use would provide the most benefit to their organization. Top management, business management, auditors, compliance officers and IT managers should work together to make sure that the IT implementation policy document leads to cost effective and well controlled implementation of IT general controls.

The growth in the use of policy documents and best practices creates new challenges and demands for implementation guidance. Implementation of the policy document should be consistent with the organization's risk management and control framework, appropriate for the organization and integrated with other methods and practices that are being used.

There is no doubt that effective management policies and procedures help ensure that IT is managed as a routine part of everyday activities. Adoption of standards and policy documents will help enable quick implementation of good procedures and avoid lengthy days in re-inventing the wheels and agreeing on approaches. The policy document is not a panacea, and its effectiveness depends on how it's been actually implemented and kept up to date. It is most useful when applied as a set of principles and as a starting point for tailoring specific procedures. Implementation should be tailored, prioritized and planned to achieve effective use and management and staff must understand what to do, how to do it and why it is important.

Finally, there is no such thing as risk free environment, and compliance with Sarbanes Oxley does not create such an environment. However, implementing a policy document where there is consistency in documented internal controls can help reduce the risk and create a more efficient working environment.

Unfortunately, the issue of SOX compliance is not that of debate and development, but rather one of accommodation and acceptance. It is important for organizations to search for approaches that would reduce the burden of SOX IT implementation and best serve the interest of the organization.

This research is based on the notion that is a way through, insights can be made, and benefits won and possibly even longer-term savings made from undertaking the compliance work. Therefore, the use of policy documents as an instrument that can be applied as an organization wide strategy in making compliance work effortless and more efficient is explored in this study.

This chapter concludes by critically evaluating the findings from this research and providing recommendations, based on the findings, on areas of improvement to the policy documents.

REFERENCES

[1]. Lenn, L. E. (2013). Sarbanes-Oxley act 2002 (SOX)-10 years later. *Journal of Legal Issues and Cases in Business*, *2*, 1.

[2]. Wallace, L., Lin, H., & Cefaratti, M. A. (2011). Information security and Sarbanes-Oxley compliance: An exploratory study. *Journal of Information Systems*, *25*(1), 185-211.

[3]. Ramos, M. J. (2006). *How to comply with Sarbanes-Oxley section 404: assessing the effectiveness of internal control*. John Wiley & Sons.

[4]. Shakespeare, C. (2008). Sarbanes-Oxley Act of 2002 Give Years on: What Have We Learned. *Journal of Business and Technology Law*, *3*, 333.

[5]. Frazer, L. (2016). Internal control: Is it a benefit or fad to small companies? A literature dependency perspective. *Journal of Accounting and Finance*, *16*(4), 149-161.

[6]. Graham, L. (2010). *Complying with Sarbanes-Oxley section 404: a guide for small publicly held companies*, 2. John Wiley & Sons.

[7]. Schroeder, J. H., & Shepardson, M. L. (2016). Do SOX 404 control audits and management assessments improve overall internal control system quality?. *The Accounting Review*, *91*(5), 1513-1541.

[8]. Wald, N. (2023). FTX—The Plausbility of an Unmodified Audit Opinion on an Organization That Lacks Internal Control; A Deep Dive into the Standards. *Open Journal of Accounting*, *12*(2), 26-35.

[9]. Pal, S., Hitchens, M., & Varadharajan, V. (2020). Access control for Internet of Things—Enabled assistive technologies: An architecture, challenges and requirements. In *Assistive technology for the elderly* (pp. 1-43).

DOI: 10.17148/IARJSET.2024.11123

Academic Press.

[10]. Hove, L. (2020). *Strategies Used to Mitigate Social Engineering Attacks* (Doctoral dissertation, Walden University).

[11]. Calo, R., & Citron, D. K. (2020). The automated administrative state: A crisis of legitimacy. *Emory Legal Journal*, *70*, 797.

[12]. Musarat, M. A., Khan, A. M., Alaloul, W. S., Blas, N., & Ayub, S. (2024). Automated monitoring innovations for efficient and safe construction practices. *Results in Engineering*, *22*, 102057.

[13]. Turner, L., Weickgenannt, A. B., & Copeland, M. K. (2022). *Accounting information systems: controls and processes*. John Wiley & Sons.

[14]. Rainer, R. K., Prince, B., Sanchez-Rodriguez, C., Splettstoesser-Hogeterp, I., & Ebrahimi, S. (2020). *Introduction to information systems*. John Wiley & Sons.

[15]. Mangundu, J. (2024). Exploring Factors Impacting Information Technology Governance Implementation Maturity In Institutions Of Higher Education, South Africa: Application Of The Will-Skill-Tool Model. *The African Journal of Information Systems*, *16*(1), 1.

[16]. Kasauli, R., Knauss, E., Horkoff, J., Liebel, G., & de Oliveira Neto, F. G. (2021). Requirements engineering challenges and practices in large-scale agile system development. *Journal of Systems and Software*, *172*, 110851.

[17]. Ilori, O., Nwosu, N. T., & Naiho, H. N. N. (2024). Optimizing Sarbanes-Oxley (SOX) compliance: strategic approaches and best practices for financial integrity: A review. *World Journal of Advanced Research and Reviews*, *22*(3), 225-235.

[18]. Westland, J. C. (2020). The information content of Sarbanes-Oxley in predicting security breaches. *Computers & Security*, *90*, 101687.

[19]. Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., & Vrontis, D. (2021). Internal auditing and cyber security: audit role and procedural contribution. *International Journal of Managerial and Financial Accounting*, *13*(1), 25-47.

[20]. Shukla, S., George, J.P., Tiwari, K. and Kureethara, J.V., 2022. Data security. In *Data Ethics and Challenges* (pp. 41-59). Singapore: Springer Singapore.

[21]. Power, M. (2021). The financial reporting system–what is it?. *Accounting and business research*, *51*(5), 459-480.

[22]. Chen, Y., Chen, S., Liang, J., Feagan, L. W., Han, W., Huang, S., & Wang, X. S. (2020). Decentralized data access control over consortium blockchains. *Information Systems*, *94*, 101590.

[23]. Tuli, F. A., & Kaluvakuri, S. (2022). Implementation of ERP Systems in Organizational Settings: Enhancing Operational Efficiency and Productivity. *Asian Business Review*, *12*(3), 89-96.

[24]. Li, J., Maiti, A., & Fei, J. (2023). Features and Scope of Regulatory Technologies: Challenges and Opportunities with Industrial Internet of Things. *Future Internet*, *15*(8), 256.

[25]. Christina, A., & Fort, T. L. (2020). Finding the fit: Why compliance and ethics programs should seek to match individual and corporate values. *Business Horizons*, *63*(4), 451-462.

[26]. Verret, J. W. (2021). A Regulatory Budget for the Public Company Accounting Oversight Board. *Ga. St. UL Rev.*, *38*, 881.

[27]. Amore, E., Dilger, T., Ploder, C., Bernsteiner, R., & Mezzenzana, M. (2023). Leverage the COBIT 2019 Design Toolkit in an SME Context: A Multiple Case Study. *KnE Social Sciences*, 73-101.

[28]. Alayasah, H. N. (2024). *The Effect of Internal Control Deficiencies on Financial Performance of Palestinian Companies* (Doctoral dissertation, Al-Quds University).

[29]. Tangka, G. M. W., Liem, A. T., & Mambu, J. Y. (2020, October). Information Technology Governance Audit Using the COBIT 5 Framework at XYZ University. In *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS)* (pp. 1-5). IEEE.

[30]. Olaniyi, O., & Omubo, D. S. (2023). The importance of COSO framework compliance in information technology auditing and enterprise resource management. *International Journal of Innovative Research & Development*, *12*(4).

[31]. Ratshitanga, N. T. (2021). *A systems perspective of information technology (IT) governance: A case of higher education institutions in South Africa* (Doctoral dissertation).

[32]. Al-Fatlawi, Q. A., Al Farttoosi, D. S., & Almagtome, A. H. (2021). Accounting information security and it governance under cobit 5 framework: A case study. *Webology*, *18*(Special Issue on Information Retrieval and Web Search), 294-310.

[33]. Weickgenannt, A. B., Hermanson, D. R., & Sharma, V. D. (2021). How US audit committees oversee internal control over financial reporting. *International Journal of Auditing*, *25*(1), 233-248.

[34]. Woods, M. (2022). Risk and Governance. In *Risk Management in Organisations* (pp. 4-20). Routledge.

[35]. Gericke, K., Eckert, C., & Stacey, M. (2022). Elements of a design method–a basis for describing and evaluating design methods. *Design Science*, *8*, e29.

DOI: 10.17148/IARJSET.2024.11123

[36]. Rainer, R. K., Prince, B., Sanchez-Rodriguez, C., Splettstoesser-Hogeterp, I., & Ebrahimi, S. (2020). *Introduction to information systems*. John Wiley & Sons.

[37]. Pearlson, K. E., Saunders, C. S., & Galletta, D. F. (2024). *Managing and using information systems: A strategic approach*. John Wiley & Sons.

[38]. Mishra, S., Alowaidi, M. A., & Sharma, S. K. (2021). Impact of security standards and policies on the credibility of e-government. *Journal of Ambient Intelligence and Humanized Computing*, 1-12.

[39]. Akinleye, G. T., & Kolawole, A. D. (2020). Internal controls and performance of selected tertiary institutions in Ekiti state: A committee of sponsoring organisations (coso) framework approach. *International Journal of Financial Research*, *11*(1), 405-416.

[40]. Ilori, O., Nwosu, N. T., & Naiho, H. N. N. (2024). Optimizing Sarbanes-Oxley (SOX) compliance: strategic approaches and best practices for financial integrity: A review. *World Journal of Advanced Research and Reviews*, *22*(3), 225-235.

