International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V72I8P116

Volume 72 Issue 8, 109-113, August 2024

Original Article

Leveraging Technology for Financial Compliance Excellence

Mukta Sharma[1], Krunal Patel[2]

[1]*Sr. IT Compliance Analyst, Intercontinental Exchange, Virginia, USA.*
[2]*Lead Engineer, StitchFix, Virginia, USA.*

[1]*Corresponding Author : mucktasharma@gmail.com*

Received: 19 June 2024 Revised: 23 July 2024 Accepted: 11 August 2024 Published: 30 August 2024

Abstract *- Financial compliance is a critical aspect of any organization's operations, especially in regulated industries such as finance, healthcare, and publicly traded companies. Compliance ensures adherence to laws, regulations, and standards set by regulatory bodies, helping organizations avoid legal penalties and fostering trust and integrity in the marketplace. In today's advancing and evolving technological landscape, digital transformation is here to play a critical role in enhancing and strengthening an organization's prospects to achieve and maintain financial compliance. Automation ensures regulatory adherence with minimized errors, while Artificial Intelligence (AI) and Machine-Learning (ML) enable real-time anomaly detection. Big data analytics and cloud solutions secure compliance platforms, and advanced cybersecurity and integrated compliance systems streamline processes, supported by effective RegTech tools for regulatory compliance and risk management. Sarbanes-Oxley (SOX) Act of 2002 legislation significantly enhances financial integrity by enforcing rigorous standards for transparent financial reporting and proactive risk management within organizations.*

Keywords *- IT General Controls, SOX, IT Audits.*

1. Introduction

Transparency and accountability in corporate governance and financial reporting are essential to protect shareholders and the public from accounting errors and fraudulent practices. With the advent of technology, financial reporting and practices have become more efficient, accurate, and timely, enabling faster data processing, real-time reporting, and enhanced audit trails.

However, due to lack of absence of regulatory frameworks, organizations had the opportunity to operate with less stringent oversight, potentially leading to lax financial controls and accountability measures. To address the problem of financial inaccuracy with the advancement in technology and to ensure transparency in financial reporting, it became crucial to introduce regulatory obligations that enhance corporate governance and accountability, ensure transparency in financial reporting, and protect investors from fraudulent practices. Thus Sarbanes-Oxley (SOX) Act of 2002 was introduced. SOX was established as federal law in the United States by U.S. Senator Paul Sarbanes, and U.S. Representative Michael Oxley introduced the legislation, which became known as the Sarbanes-Oxley Act (SOX).

The act authorized the creation of the Public Company Accounting Oversight Board to further monitor corporate behaviour, especially in accounting and fines for non-compliance are enforced by the Security and Exchange Commission (SEC). The key sections of the Sarbanes-Oxley Act are Sections 302, 404, and 906. Section 302 requires CEOs and CFOs to personally attest to the effectiveness of internal controls over financial reporting. Section 404 mandates an annual independent audit on the effectiveness of IT controls, assessing their documentation and performance. Section 906 makes it a crime for executives to misrepresent the company's financial condition wilfully. Business organizations have been increasingly using various computerized Information Systems (IS) to support and improve the effectiveness and efficiency of their business operations. More importantly, with widespread reliance on IS for business analysis and operations, the accuracy, integrity, and completeness of essential financial and business data processed by IS become critical. [1] ITGC are “the controls embedded within IT processes that provide a reliable operating environment and support the effective operation of application controls” [1].

Technology advancements in IT infrastructure services and applications since then have facilitated automated auditing, improved data integrity through blockchain, and enhanced risk management through AI, all aimed at preventing similar fraudulent activities and ensuring

compliance with regulatory standards. This paper will give an overview of IT General Controls (ITGC) and explore its relevance to various industries as well as highlight the crucial role of engineering teams in implementing and maintaining these controls. While the act was aimed at the organization in the US, this goes the border due to an increase in certain recurring activities being outsourced and offshored. Thus, this paper also aims to bring a new perspective on how ITGC is applied beyond the US borders.

2. Overview of IT General Controls

The Sarbanes-Oxley Act of 2002 (SOX) made tremendous changes in regulations to improve corporate governance and accountability, particularly concerning financial reporting. A critical aspect of SOX compliance from a technology lens is ensuring the integrity of financial reports through robust Information Technology General Controls (ITGCs).

IT General Controls (ITGC) are the foundation controls embedded in the IT infrastructure services and applications such as operating systems, databases, and networks to ensure they can adequately provide reasonable assurance and support for the IT applications and business processes. [1]

ITGCs focus on IT systems that enable financial transactions or reporting, including applications, operating systems, databases, and the supporting IT infrastructure, to ensure their effective use and protection from risks. These controls are essential for the proper functioning of an organization's IT systems and for safeguarding sensitive information. The below section will go deeper into explaining the purpose of ITGC.

2.1. Purpose of ITGCs

ITGCs sole purpose is to provide assurance over the basis of any information systems – confidentiality (C), integrity (I), and availability (A), together often known as the CIA triad. This CIA foundation is addressed by encompassing a set of policies, procedures, and technologies aimed at managing and monitoring the use of IT systems, ensuring they operate effectively and efficiently.

The primary goals of ITGCs are to:

1. Protect Sensitive Information: ITGCs ensure that sensitive financial and operational data are secure from unauthorized access, misuse, and loss.
2. Ensure System Reliability: By implementing robust controls, organizations can maintain the reliability and accuracy of their IT systems, which are critical for generating financial reports.
3. Support Compliance: ITGCs help organizations comply with SOX and other regulatory requirements by maintaining strong IT controls.

The next section will explore the building blocks of ITGC that have their backbone connected to the purpose of.

2.2. Key Components of ITGCs

To ensure a set of ITGC that can be applied across the board, nine companies in 2004, exactly 10 years back, developed a methodology for evaluating ITGC. This methodology helps organizations identify deficiencies and detect major gaps, ensuring a more robust IT control environment. Below are some of the ITGC controls with objective and implementation examples:

1) Access Controls:
   - Objective: Ensure that only authorized and appropriate personnel can access critical financial data and systems.
   - Implementation: Use authentication and authorization methods such as passwords, biometrics, and multi-factor authentication to control access to IT resources. Regularly review and update access rights to ensure they align with current job responsibilities.
2) Change Management:
   - Objective: Manage and track changes to IT systems to ensure they are authorized, tested, and properly documented.
   - Implementation: Establish formal change management procedures, including approval workflows, testing protocols, and documentation requirements. This helps prevent unauthorized or erroneous changes that could compromise system integrity.
3) Data Backup and Recovery:
   - Objective: Protect against data loss through regular backups and a robust recovery plan.
   - Implementation: Implement automated backup solutions and regularly test data recovery processes to ensure they can be executed effectively in case of a disaster or data loss incident.
4) Security Controls:
   - Objective: Safeguard financial information from unauthorized access and cyber threats.
   - Implementation: Deploy and perform continuous checks on security measures such as firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), vulnerability management tools, and antivirus software. Performing patch management to ensure critical systems are running on up-to-date versions and vulnerabilities are addressed.
5) Audit Trails:
   - Objective: Maintain detailed logs of system activity to monitor and review access and changes to financial systems and data.
   - Implementation: Implement logging mechanisms to capture user activities, system logs, system changes, and access attempts. Regularly review audit logs to detect and investigate suspicious activities.

6) Segregation of Duties:
   - Objective: Reduce the risk of fraud and errors by ensuring no single individual has control over all aspects of a financial transaction.
   - Implementation: Design job roles and responsibilities to separate critical functions such as authorization, recording, and custody of assets. Regularly review role assignments to prevent conflicts of interest.
7) System Monitoring:
   - Objective: Continuously monitor IT systems for anomalies, performance issues, and potential security breaches.
   - Implementation: Use monitoring tools to track system performance, detect unusual activities, and generate alerts for immediate action. Conduct regular assessments to ensure monitoring processes remain effective.
8) Vendor Management:
   - Objective: Assess and manage vendor / third-party service providers to ensure they comply with SOX requirements and do not pose a risk to financial data security.
   - Implementation: Conduct thorough due diligence when selecting vendors, including security assessments and compliance checks. Establish contracts that outline security and compliance expectations and regularly review vendor performance.
9) Incident Response:
   - Objective: Address and mitigate IT security breaches or failures promptly.
   - Implementation: Develop an incident response plan that outlines procedures for detecting, reporting, and resolving security incidents. Conduct regular training and simulations to ensure staff are prepared to respond effectively.
10) Regular Testing and Review:
   - Objective: Ensure IT controls are effective and compliant with SOX regulations.
   - Implementation: Conduct regular tests and reviews of ITGCs, including vulnerability assessments, penetration testing, and compliance audits. As part of continuous improvement, it is necessary to document the corrective actions and findings.

The methodology developed gave a robust set of control area objectives and implementation that gave a kick start for any organization; the next step is to use this to perform an assessment, which is explained in the next section.

2.3. ITGC Assessment

An ITGC assessment is essentially an audit of an organization's ITGCs to confirm their design effectiveness in protecting information systems as well as the information they process. This type of audit can be performed by internal or external auditors and serves several purposes:

1. Identify Weaknesses: Detect any deficiencies or vulnerabilities in the ITGCs that could negatively impact system security and data integrity.
2. Recommend Improvements: Provide actionable recommendations to strengthen and improve IT controls that enhance overall security posture.
3. Ensure Compliance: Verify that the organization complies with SOX and other regulatory requirements, thereby avoiding legal penalties and maintaining stakeholder trust.

Engineering teams play a crucial role in implementing and maintaining ITGCs by ensuring robust access controls, effective change management, and reliable data backup and recovery processes. The engineering teams can be in-house /on-site, outsourced, and offshore, and their collaboration is a default requirement to ensure the integrity and security of an organization's IT infrastructure. Their expertise and proactive efforts are essential for safeguarding IT systems and ensuring compliance with regulatory requirements. The next section will give an overview of how engineering teams play a role in maintaining SOX compliance.

3. Engineering's Perspective in Ensuring SOX Compliance

Engineering teams, whether they are in-house /on-site, outsourced, or offshored, have vital SOX responsibilities, including establishing and maintaining strong IT General Controls (ITGCs) to ensure compliance. They are tasked with implementing robust access controls to secure financial data, managing and documenting changes to IT systems to prevent unauthorized modifications, and ensuring reliable data backup and recovery processes. Their role is critical in safeguarding IT systems, mitigating risks, and maintaining the integrity and accuracy of financial reporting in compliance with SOX requirements. This comprehensive approach enhances the organization's overall security posture and regulatory adherence.

From an engineering perspective within a company subject to the Sarbanes-Oxley Act (SOX), there are several key responsibilities that engineers and IT professionals need to consider to ensure compliance with SOX requirements. Here are some specific areas where engineering teams typically play a crucial role:

1. Security Controls: Engineers are responsible for implementing and maintaining robust security controls to protect financial data and systems. This includes:
   - Ensuring secure access controls: Adhering to the policy and implementing strong mechanisms such as role-based access controls (RBAC), least privilege

principles, and strong authentication mechanisms.
- Network security: Securing networks against unauthorized access and ensuring data transmitted over networks is encrypted and protected.
- Vulnerability management: Regularly assessing and patching systems to protect against vulnerabilities that could compromise financial data.
- Engineering Tools Examples: AWS Identity Access and Management, AWS Virtual Private Cloud, AWS Inspector, Qualys
- Scenario: For vulnerability management, the in-house engineering team can run the scanning tool, and the offshore/outsourced team can consume the report of the vulnerability management tool. They can be responsible for ensuring appropriate triaging and mitigation steps are performed. Thus, this responsibility can be shared within the US borders and outside.

2. Data Integrity and Availability: Engineers must ensure that financial data is accurate, reliable, and available when needed. This involves:
   - Implementing data integrity controls: Using checksums, hashes, or other methods to verify data integrity.
   - Backup and recovery: Establishing robust backup and disaster recovery procedures to ensure data availability and continuity in case of disruptions.
   - Engineering Tools Examples: AWS CloudHSM AWS CloudTrail
   - Scenario: For backup, the in-house engineering team can perform the backup as prescribed in the policy, and the offshore/outsourced team can perform the jobs to confirm that the backup meets the policy. Thus, this responsibility can be shared within the US borders and outside.
3. Change Management: Engineers play a crucial role in managing changes to IT systems and infrastructure. This includes:
   - Implementing a formal change management process: Documenting and reviewing changes before they are implemented to prevent unauthorized modifications that could impact financial reporting.
   - Version control: Maintaining version control of software and configurations to ensure changes are tracked and auditable.
   - Engineering Tools Examples: GitHub, ServiceNow
   - Scenario: For change management, the offshore team can kick off the ticket and automate a workflow that triggers appropriate approvals while the in-house engineering teams perform the change. Thus, this responsibility can be shared within the US borders and outside.
4. System and Application Controls: Engineers are responsible for implementing controls within systems and applications to support financial reporting. This includes:
   - Logging and monitoring: Implementing logging mechanisms to track access and changes to financial systems, with regular monitoring and review of logs.
   - Application security: Ensuring that applications handling financial data are secure, free from vulnerabilities, and adhere to coding best practices.
   - Engineering Tools Examples: GitHub, Splunk, DataDog, Synk, JFrog, Qualys
   - Scenario: For logging and monitoring, the in-house engineering teams can enable logging and create dashboards for monitoring. In contrast, the offshore team can be responsible for alerting if an anomaly is detected, thereby replicating the sun model to ensure systems are secure all the time. Thus, this responsibility can be shared within the US borders and outside.
5. Compliance Documentation: Engineers must document and maintain evidence of compliance with SOX requirements. This includes:
   - Documenting technical controls and procedures: Providing clear documentation of security controls, change management processes, and system configurations.
   - Supporting audits: Collaborating with auditors to provide evidence of compliance, such as access logs, configuration records, and security assessments.
   - Engineering Tools Examples: GitHub, Wolters-Kluwer, AuditBoard
   - Scenario: For maintaining the evidence repository, the in-house engineering teams can collaborate with the offshore team to ensure evidence related to access logs for certain financial applications is up to date. Thus, this responsibility can be shared within the US borders and outside.
6. Incident Response: Engineers should be prepared to respond to security incidents and breaches promptly. This involves:
   - Incident response planning: Developing and testing incident response plans to mitigate the impact of security breaches on financial systems and data.
   - Forensic analysis: Conducting forensic analysis to understand the scope and impact of incidents and to support investigations.
   - Engineering Tools Examples: ServiceNow, PagerDuty, DataDog, Splunk
   - Scenario: For incident management, the in-house engineering and offshore teams can be responsible for detecting incidents and engaging appropriate teams to resolve them. Using the sun model will ensure incidents are detected are solved in a timely manner, complying with policy and regulations. Systems are secure all the time. Thus, this responsibility can be shared within the US borders and outside.

Overall, engineers in organizations, whether it is in-house, offshore, or outsourced, are subject to SOX playing a critical role in maintaining the integrity, security, and availability of systems and data related to financial reporting. By implementing and adhering to these responsibilities, engineering teams contribute to the company's overall compliance with SOX regulations, ensuring transparency, accuracy, and reliability in financial reporting processes that result in the avoidance of legal penalties.

4. Conclusion

It is important to note that engineering teams are an enabler in meeting the Sarbanes-Oxley Act (SOX). The engineering efforts are aimed at ensuring that violations do not occur that can result in fines and impact the financial reporting integrity. For example, fines for minor infractions or failures to comply with specific provisions of SOX may result in penalties ranging from tens of thousands to hundreds of thousands of dollars. In more serious cases, where deliberate misconduct or fraud is involved, fines can escalate into the millions. These fines are intended not only to penalize non-compliance but also to deter future violations and maintain the credibility of financial reporting standards. Therefore, organizations subject to SOX regulations must prioritize compliance to avoid these potentially significant financial penalties and reputational damage.

References

[1] Wing Han Brenda Chan, and Son Kai Lao, "A Study of the Business Value of it General Controls," *Journal of Information Technology Management*, vol. 20, no. 4, pp. 22-36, 2009. [Google Scholar] [Publisher Link]

[2] Jabin Geevarghese George, "Leveraging Enterprise Agile and Platform Modernization in the Fintech AI Revolution: A Path to Harmonized Data and Infrastructure," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 6, no. 4, pp. 88-94, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Jabin G. George, Tlaltecatl T. Marín-Esponda, and Prabir Kumar-Dandpat, "Analyzing the Impact of Excess Inventory of California GLAM to Control the Inventories of Distributors by Integrating Product and Distributor Segmentation Concept in the Supply Chain," *Degree Work, Specialization in Supply Chain Management. Tlaquepaque, Jalisco, ITESO*, pp. 1-42, 2019. [Google Scholar] [Publisher Link]

[4] Olufunke Olawale et al., "RegTech Innovations Streamlining Compliance, Reducing Costs in the Financial Sector," *GSC Advanced Research and Reviews*, vol. 19, no. 1, pp. 114-131, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Todd Fitzgerald, *Leveraging IT Control Frameworks for Compliance*, 6th ed., Information Security Management Handbook, pp. 1-10, 2010. [Google Scholar] [Publisher Link]

[6] Jabin Geevarghese George, "Transforming Banking in the Digital Age: The Strategic Integration of Large Language Models and Multi-Cloud Environments," *International Journal of Computer Trends and Technology*, vol. 72, no. 4, pp. 77-86, 2024. [CrossRef] [Google Scholar] [Publisher Link]