Information Technology in a SOX Environment

RISK ADVISORY
BACKGROUND

The Sarbanes-Oxley (SOX) Act of 2002 makes the evaluation of internal controls mandatory for SEC registrants. As part of the process for assessing the effectiveness of internal controls over financial reporting, management needs to consider controls related to the information systems that support relevant financial processes. These controls are known, collectively, as information technology general controls (ITGCs). ITGCs are IT processes and activities that are performed within the IT environment and relate to how the applications and systems are developed, maintained, managed, secured, accessed, and operated.

The objectives of ITGCs are to provide the proper development and maintenance of applications, as well as the integrity of the supporting IT infrastructure, data files and computer operations. ITGCs provide a basis for relying on the reports and data from these applications as well as a basis for concluding that other configurable and non-configurable system behavior (also known as business process automated controls) continues to function over time.

SOX authorizes the Public Company Accounting Oversight Board (PCAOB) to perform inspections of public accounting firms to assess compliance with certain laws, rules, and professional standards. The PCAOB identifies deficiencies in public accounting firms’ procedures and quality and then publishes certain of these issues in inspection reports, which are available to the public. The common IT issues and themes identified are summarized below. These issues stem from the lack of understanding in ITGCs and how to evaluate IT components of the internal control structure, as well as the impact of ITGCs on the overall internal control structure. The following are a few of these issues:

- Incomplete Information Produced by the Entity (IPE) testing: IPE are data and reports used in the execution of key controls or in conjunction with audit procedures. Controls were not designed to cover all the key data in the report or the IPE was not appropriately evaluated for completeness and accuracy of data. This key responsibility of management is often overlooked.
- Test performed was one-sided: Transactions processed by the system (application controls) are tested; however, the system parameters and configuration were not identified nor were they tested. Furthermore, the test performed did not include procedures to determine whether the control prevented the processing of transactions that did not match, as well as possible overrides to the system automation.
- Insufficient application control testing approach: The sample selection approach was based on the assumption that ITGCs were operating effectively, which is not always the case. For application controls, a “test of one” approach is generally only appropriate when ITGCs are deemed effective.
- Segregation of duties issues: The test performed did not evaluate the appropriateness of administrator-level access to the application and related infrastructure to determine whether there was adequate segregation of duties.
- Inappropriate “test of one” sample selection: While tests were performed over system functionality and calculations, the types of transactions tested were not relevant to the control, nor did the procedures cover all of the various relevant transaction types and configurations.
- Mis-scoping of IT environments: Organizations may have multiple production instances of an application and each instance could be configured differently. The test procedures performed over these systems were limited to one instance with the assumption that the configuration was consistent.

Companies should be aware of the aforementioned challenges and consider the issues as they implement and evaluate IT aspects of the business processes and the overall internal control environment. This publication provides an overview of the importance of IT in the internal control structure as well as the what to consider when evaluating ITGCs.

**RELATIONSHIP TO BUSINESS PROCESSES AND CONTROLS**

The relationship between business processes and IT goes hand-in-hand as applications and system hardware support critical processes for almost every company. Information systems and data support the flow of information from initiation to reporting and are, therefore, one of the most important and pervasive pieces of an organization's financial reporting system. Further, IT systems are also increasingly relied upon as tools to provide efficient processing and reporting for decision-making purposes. ITGC risk for SOX, therefore, is the risk to financial reporting associated with potential defects in the design and/or operation of ITGC process controls.

When identifying in-scope applications and systems for testing, a top-down approach emphasizing areas of higher propensity to error and/or fraud should be used in order to obtain a better understanding of potential risks. Once process controls and related financially relevant reports are identified, the applications that support any automated or application controls as well report and data generation would be included for ITGC testing. Although applications directly support the flow of transactions, several system layers within the IT environment are considered for scoping. These systems consist primarily of operating systems and databases; additional layers, such as network and internet level security, whether on-premises or hosted, may be important depending on the IT environment and business process risks.

It is important to understand the relationship and difference between ITGCs and application controls. ITGCs are based on IT process controls, apply across applications and related infrastructure and support the individual applications; whereas, application controls relate to the specific application functionality and reside within each application. Therefore, application controls are business process controls that ensure the completeness and accuracy of transactions processing as well as the validity of the accounting records within the applications.

Application controls will continue to perform the same until subject to change; thus, without effective ITGCs, reliance on the in-scope applications and systems may not be possible, unless additional procedures are performed. Deficiencies in the ITGCs may result in deficiencies in the operation of the application controls, manual controls reliant on reports / IT-Dependent Manual (ITDM) controls, as well as any IPE.
IMPORTANCE OF ITGCS

ITGCs are an essential component of a company’s internal controls infrastructure because of the pervasiveness of information systems across the enterprise. The accuracy and reliability of financial reporting are largely dependent upon the operational effectiveness of automated functionality embedded within critical business processes. ITGCs covering appropriate access restriction to system resources in addition to a well-controlled change control process provide a foundation upon which reliance on application controls and system reports rests. In addition, evaluation of ITGCs is important because the IT process controls provide a basis for concluding that applications (functionality and reports) function consistently over time.

Effective ITGCs also provide additional benefits such as:

- Reducing the extent of testing and reliance on manual transaction-level controls,
- Increasing the effectiveness and efficiency of internal controls and audit procedures by establishing a strong IT foundation and leveraging systems across the organization,
- Improving the consistency of control operation (i.e., automated processes vs. manual), and,
- Improving reliability of manual controls dependent on IT information (i.e., reports, IPE).

FRAMEWORK FOR EVALUATING ITGCS

ITGCs are an important component of internal controls but organizations require guidance to implement the right controls into the IT processes and evaluate the effectiveness of the controls. The Control Objectives for Information and related Technologies (COBIT) framework is a comprehensive framework for the governance and management of IT and is the most commonly used framework for evaluating ITGCs. The COBIT framework was designed by the Information Systems Audit and Control Association (ISACA) to address IT controls compliance and demonstrate strong IT controls over financial reporting.

COBIT is used in conjunction with COSO (business process and internal controls guidance) and is mapped to COSO for SOX reporting. COSO Principle 11 requires organizations to understand the IT systems and related ITGCs as well as assess the effectiveness of ITGCs considering applications and IT infrastructure, end-user computing and spreadsheets, IT service providers, etc. Although the COSO 2013 Framework includes more focus on IT at a high level, COSO is mainly focused on business process controls. COBIT is specifically focused on IT process controls and is widely used by organizations as a supplement to COSO.
DIGGING DEEPER INTO ITGCs

The high-level definition of ITGCs has been introduced, but it is important to further understand the detail of ITGCs to properly implement and evaluate the IT controls. ITGCs are IT processes and related controls that are applied broadly across IT systems, although their use may be application specific. ITGCs are designed to ensure that 1) changes to applications and related infrastructure are authorized, tested and approved before they are implemented in the production environment, 2) only authorized individuals are granted access to applications and data, and 3) transactions and jobs are processed completely and accurately and issues are identified and resolved.

ITGCs apply to the applications that are determined to be in scope, their database, operating systems and end-user environments. General IT controls are commonly broken into the following three areas of focus: Change Management; Access & Security; and IT Operations. The objectives of each area are outlined below:

- Controls around change management ensure that changes to systems are authorized, tested, and approved before the change is applied into the production environment. Additionally, there should be a clear separation of IT environments (the environment where changes are developed and tested versus the production environment) and a segregation of duties in development and administrative functions.

- Access and security controls ensure that only authorized individuals have physical and logical access to the system and data. Access restrictions should be in place to grant users access to only the specific tasks required to fulfill their job responsibilities. From a process perspective, user provisioning and termination controls define the process for adding, modifying and removing access to the systems. In addition, company policies around security configurations, such as password parameters, firewall rules, audit policy and anti-virus, provide preventive and detective security controls. Further, access to the systems should be monitored and security assignments reviewed periodically. Lastly, privileged user access should also be appropriately restricted and appropriate segregation of duties should exist between the administrators and system users.

- IT operations controls ensure that activities are in place to monitor, detect, and resolve incidents and failures of automated processes, such as backups and scheduled jobs. Additionally, access to manage the automated processes should be appropriately restricted.

Many business process controls are based on functionality residing in the in-scope applications or rely on system data; therefore, the effectiveness of ITGCs is important because they provide the basis needed to determine whether applications function consistently over time and the basis to rely on the data reported from the systems.

In conclusion, the concept of ITGCs is getting more and more important to IT governance. The increased regulatory focus on IT requires that organizations understand how to handle IT aspects in an internal control environment and have mature IT processes and controls.
WE CAN HELP

Even though it has been over a decade since SOX legislation was introduced, organizations continue to experience deficiencies in implementing and evaluating their control environment. Many of the issues relate to systems resulting from the misunderstanding of ITGCs and the miscalculation of IT components in the internal control structure.

We work with external audit, internal audit, IT departments and business functions to understand and rationalize IT processes and controls as well as implement and maintain the integrity and reliability of IT environments, systems and data. Our team of experienced IT SOX professionals are ready to answer your questions about how to implement and evaluate IT controls within your organization.
MBAF RISK ADVISORY OVERVIEW

MBAF's Risk Advisory team is comprised largely of former Big 4 professionals (CPAs, CISAs, MBAs). As a seasoned, accessible, and well-coordinated team, we execute efficiently and with a high level of quality. We have extensive experience with highly complex, technical accounting matters. We have worked successfully with all of the Big 4 firms and other large audit firms, including working with their respective national offices. Our experience encompasses a wide spectrum of projects ranging from assisting emerging growth companies with accounting consultations and policy writing, to large-scale Fortune 500 global internal control projects with complex coordination and execution efforts. Our high quality, dedicated Risk Advisory team has meaningful SEC and PCAOB experience.

Knowledge sharing and development are integral to our service delivery. Our investment in knowledge helps our engagement teams operate more efficiently and effectively, and we actively seek opportunities to share that knowledge and thought leadership with your management team. We manage our time in ways that are cost-effective to produce value for you, which we believe is derived from:

- The unparalleled advantage provided by our team's unique set of skills and experiences from the viewpoint of the external auditor
- Significant synergies and collaboration with your external auditor, which allows for maximum leverage of our work in preparation for the external audit
- Proactive sharing of relevant and practical thought leadership
- A strong, deep bench of professionals, including subject matter resources (IT, valuation, tax, litigation and others)

MBAF’s Risk Advisory practice creates value for emerging growth, mid-cap, and Fortune 500 companies.

- IPO readiness
- IT risk
- Enterprise risk management
- Sarbanes-Oxley
- SEC reporting
- Technical accounting

CONTACT:

Jesus Socorro  
Managing Principal - Risk Advisory  
212.931.9167  
jsocorro@mbafcpa.com

Alvaro Florez  
Principal - Risk Advisory IT  
786.507.5884  
Aflorez@mbafcpa.com

Kim Garcia  
Director - Risk Advisory IT  
786.709.9301  
Kgarcia@mbafcpa.com

Jorge Santiago  
Senior Manager - Risk Advisory IT  
786.347.3883  
Jsantiago@mbafcpa.com

Trevor Foo  
Senior Manager - Risk Advisory IT  
786.709.9228  
Tfoo@mbafcpa.com

LOCATIONS:

Miami  
Coral Gables  
Fort Lauderdale  
Boca Raton  
Palm Beach  
Orlando  
Naples  
New York City  
Valhalla  
Baltimore  
Boulder  
Las Vegas  
India
Assurance
Tax & Accounting
Advisory
Technology Consulting
Private Client Wealth

An independent member of Baker Tilly International