



## A Fresh Look at Information Technology Controls

### Overview

The Institute of Internal Auditors (IIA) recently published the Global Technology Audit Guide (GTAG) to address issues related to information technology management, control, and security. The guide is designed for a wide audience, including executives, board members, management, process owners, and others. GTAG provides needed strategic direction and interpretation for management seeking to improve the ability of the IT environment to support business objectives.

### GTAG 1 Significance

*Information Technology Controls* introduces the outline for “The Structure of IT Auditing”, a six-part series providing steps for assessing IT controls within the overall system of internal controls. IIA’s presentation is unique as it provides useful and appropriately high-level discussion of the role of IT controls in accomplishing business objectives. In most organizations, IT controls are a primary control for ensuring users cannot exceed their approved authorities and maintaining separation of incompatible duties. The GTAG repeatedly states that management oversight of sound IT controls does not require intimate knowledge of all aspects of the technical environment. However, the first step to effective IT control depends on understanding which controls require the expertise of IT controls specialists, and which controls fall into the user administration category.

GTAG breaks the IT control environment into several key processes:

#### **Understanding IT Controls**

- Governance, Management, Technical
- General/Application
- Preventive, Detective, Corrective
- Information Security

#### **Importance of IT Controls**

- Reliability and Effectiveness
- Competitive Advantage
- Legislation and Regulation

#### **Roles and Responsibilities**

- Governance
- Management
- Audit

#### **Based on Risk**

- Risk Analysis
- Risk Response
- Baseline Controls

#### **Monitoring and Techniques**

- Control Framework
- Frequency

#### **Assessment**

- Methodologies
- Audit Committee Interface



GTAG provides much needed guidance and direction with regard to the definition and evaluation of IT control processes. Below is a summary of the recommendations made in GTAG; more detail can be obtained from the IIA at [www.theiia.org](http://www.theiia.org).

### **The Importance of IT Controls**

IT controls are a vital component in the internal control structure, and despite their technical nature, the control objectives addressed by IT controls are the responsibility of senior management. This has always created somewhat of a paradox: IT controls address critical control objectives at a system or organization-wide level, however, the technical issues surrounding the implementation and operation of those controls are often beyond the grasp of senior management. Management must rely on the work of technical experts to evaluate such controls. However, IT controls include much more than technology; they also include written policies and procedures, physical access protection, and procedural rules for change management related to the IT environment.

GTAG examines and explains the IT control structure in terms of strategic management objectives, and provides excellent guidance for management seeking to evaluate the functioning of detailed technical controls within those objectives. Currently, management must evaluate such strategic objectives as compliance with Sarbanes-Oxley requirements related to internal control evaluation and documentation; effective implementation of IT controls can substantially help with these initiatives. One Big 4 accounting firm detailed the current relationship between IT controls and Sarbanes-Oxley compliance in a letter to the S.E.C.:

- **Development of operating efficiencies**  
One Big 4 client noted that as a result of their efforts to document and assess business processes and internal controls, management had realized that there were many redundant processes scattered throughout the organization. As a result, the company plans to implement a shared service center to centralize many of the redundant functions, thus reducing overall overhead costs.
- **Increased due diligence**  
Another Big 4 client delayed the cutover to production of a new software system until substantial testing of system controls was completed to ensure that all required control objectives were satisfied within the new processing environment. Management was concerned that the implementation would otherwise result in the identification of internal control deficiencies that would need to be disclosed. Management had commented that before the new internal control requirements those precautions may not have taken place.
- **Implementation of standard processes**  
A different Big 4 client had acquired over 200 companies over many years but had had failed to fully integrate the operation of those subsidiaries into the parent organization, or to even implement a standard set of business processes. The documentation and assessment of the control processes, including the IT control processes, resulted in accelerating the



efforts and the resources allocated to achieve consistency throughout the organization.

A critical aspect of Sarbanes-Oxley compliance is to define accepted processes and authorities within the organization, and ensure that those processes and authorities are universally enforced. In most organizations, IT systems are fundamental to the business transaction and financial reporting processes. IT controls are a management tool that provides management assurance that transactions within the domain of those systems are performed correctly, consistently, and only by authorized individuals.

### **Roles and Responsibilities**

Many different organizational roles have emerged that include responsibilities and ownership of IT controls, however, no standard has developed for defining the organizational structure best-suited to manage those IT controls. In determining the specific job duties of those individuals responsible for control implementation and administration, the IIA recommends basing role expectations on the business objectives for the use of IT (in other words, what do the IT controls need to accomplish). Then it is possible to assign the required technical resources and management oversight to ensure those objectives are met. As with other control processes, the management of IT itself must be planned and continuously assessed against relevant control objectives to ensure those objectives are accomplished. A complete review of IT control objectives and the processes to achieve those objectives should take place at least once per year.

### **Analyzing Risk**

IT controls should be selected, implemented and evaluated in relation to the risks they are designed to manage. Choosing suitable controls requires an experienced team and careful control system planning because of the inherent level of judgment built into the risk management process. The adequacy of IT controls depends greatly on the processes established by management to determine:

- Value and criticality of information
- Organizational risk appetite (i.e. the amount of residual risk that management is willing to accept) for each business area
- The required level of service to support business operations
- Complexity of the IT infrastructure
- Options for IT control and their associated benefits
- Experienced system failures in the recent past (e.g. 2 years)
- The frequency of risk assessment activities

In discussing risk mitigation through the use of information security, GTAG 1 includes reference material in Appendix I, classifying topics by governance, management, and technical issues. GTAG 1 underscores the role of internal audit in risk management, but internal auditors should be involved in the risk assessment process to ensure independence and objectivity of the results. Ultimately, internal audit must provide an opinion on the effectiveness of the internal control framework and how management identified and evaluated risk and implemented controls to mitigate that risk.



For those risks that management identifies and attempts to control, evaluation should occur to address such questions as:

- Is the control effective?
- Does it achieve the desired result?
- Is the mix of preventive, detective, and corrective controls appropriate?
- Do the controls provide evidence when control parameters fail?
- Is evidence of a control lapse retained?

While there is no single list of IT controls applicable to all organizations, there does exist a fundamental set of expected IT control requirements, including:

- Establishment of IT policies
- Definition of roles and responsibilities
- IT infrastructure equipment security
- Access, authentication, and firewall mechanisms
- Vulnerability assessments
- Change and configuration management definitions
- IT environment and service monitoring
- Use of IT audit specialists as needed

### **Monitoring and Techniques**

Adoption of a formal control framework is paramount to the organization's success in identifying and implementing the right IT controls. Such a framework should be owned by the entire organization, not just internal audit; it provides a structured way of categorizing controls to ensure that the spectrum of at-risk business areas is adequately covered. Most frameworks, including COSO - a suitable and recognized framework - only cover IT areas at a high-level and leave the customization and detailed build-out of the framework to management. GTAG provides much needed guidance in the development of such a framework.

Once all controls are in place, management must monitor and assess the controls to ensure control performance is not degraded; the frequency with which controls should be verified is determined by management. Within the IT control system it should be clear where ongoing monitoring (Daily/Periodic, Event-driven, Continuous) and special review (attestation, internal audit) monitoring take place so that this information can be summarized and reported to the appropriate oversight bodies.

### **IT Control Assessment**

Because no single methodology exists for IT control assessment, internal auditors should adopt specialized practices based on the objectives of the controls under consideration. This may require a systems-based approach to satisfy Sarbanes-Oxley, a risk-based approach for "regular" audit work, or targeted analyses where fraud is expected. This approach variability requires an adaptive internal audit. For example, as operational audits of automated business processes identify control deficiencies, the focus of the audit may need to shift to the IT system design, development, or maintenance aspects of those processes.



Audit reports that summarize findings, conclusions, and opinions regarding IT controls should be prepared regularly. The frequency of that reporting should be based on organizational needs and the environment in question.

**Conclusion**

Despite the technical issues involved with the control of the IT environment, senior management needs to ensure controls are implemented to manage the risk associated with IT systems. Assessing IT controls is an evolutionary process and should be kept near the top of the audit agenda. A properly functioning internal audit program should be able to consistently communicate clear summaries to senior management and various board committees so that they understand key IT issues and can respond accordingly. The Global Technology Audit Guide provides management with an objective based approach to understanding the requirements for assessing the IT control environment.