GTAG®

GLOBAL TECHNOLOGY AUDIT GUIDE

IPPF – Practice Guide

Information Technology Risk and Controls

2nd Edition

The Institute of Internal Auditors

Global Technology Audit Guide (GTAG®) 1
Information Technology Risk and Controls

2nd Edition

March 2012

GTAG — Table of Contents

Executive Summary

This GTAG helps chief auditing executives (CAEs) and internal auditors keep pace with the ever-changing and sometimes complex world of IT by providing resources written for business executives — not IT executives. Both management and the Board have an expectation that the internal audit activity provides assurance around all-important risks, including those introduced or enabled by the implementation of IT. The GTAG series helps the CAE and internal auditors become more knowledgeable of the risk, control, and governance issues surrounding technology. The goal of this GTAG is to help internal auditors become more comfortable with general IT controls so they can talk with their Board and exchange risk and control ideas with the chief information officer (CIO) and IT management. This GTAG describes how members of governing bodies, executives, IT professionals, and internal auditors address significant IT-related risk and control issues as well as presents relevant frameworks for assessing IT risk and controls. Moreover, it sets the stage for other GTAGs that cover in greater detail specific IT topics and associated business roles and responsibilities.

This guide is the second edition of the first installment in the GTAG series — GTAG 1: Information Technology Controls — which was published in March 2005. Its goal was, and is, to provide an overview of the topic of IT-related risks and controls.

1. Introduction

The purpose of this GTAG is to explain IT risks and controls in a format that allows CAEs and internal auditors to understand and communicate the need for strong IT controls. It is organized to enable the reader to move through the framework for assessing IT controls and to address specific topics based on need. This GTAG provides an overview of the key components of IT control assessment with an emphasis on the roles and responsibilities of key constituents within the organization who can drive governance of IT resources. Some readers already may be familiar with some aspects of this GTAG, but some segments will provide new perspectives on how to approach IT risks and controls. One goal of this GTAG, and others in the series, is that IT control assessment components can be used to educate others about what IT risk and controls are and why management and internal audit should ensure proper attention is paid to fundamental IT risks and controls to enable and sustain an effective IT control environment.

Although technology provides opportunities for growth and development, it also represents threats, such as disruption, deception, theft, and fraud. Research shows that outside attackers threaten organizations, yet trusted insiders are a far greater threat. Fortunately, technology also can provide protection from threats, as this guide will demonstrate. Executives should know the right questions to ask and what the answers mean. For example:

- Why should I understand IT risks and controls? Two words: assurance and reliability. Executives play a key role in assuring information reliability. Assurance comes primarily from an interdependent set of business controls as well as from evidence that controls are continuous and sufficient. Management must weigh the evidence provided by controls and audits and conclude that it provides reasonable assurance.
- What is to be protected? Trust should be protected because it ensures business and efficiency. Controls provide the basis for trust, although they often are unseen. Technology provides the foundation for many — perhaps most — business controls. Reliability of financial information and processes — now mandated for many organizations— is all about trust.
- Where are IT controls applied? Everywhere. IT includes technology components, processes, people, organization, and architecture, as well as the information itself. Many IT controls are technical in nature, and IT supplies the tools for many business controls.
- Who is responsible? Everyone. However, control ownership and responsibilities must be defined and disseminated by management. Otherwise, no one is responsible, and results could be quite severe.
- When should IT risks and controls be assessed? Always. IT is a rapidly changing environment that promotes process and organizational change. New risks emerge at a rapid pace. Controls must present continuous evidence of their effectiveness, and that evidence must be assessed and evaluated constantly.
- How much control is enough? Management must decide based on risk appetite, tolerance and mandatory regulations. Controls are not the objective; controls exist to help meet business objectives. Controls are a cost of doing business and can be expensive, but not nearly as expensive as the possible consequences of inadequate controls.

IT controls are essential to protect assets, customers, partners, and sensitive information; demonstrate safe, efficient, and ethical behavior; and preserve brand, reputation, and trust. In today's global market and regulatory environment, these things are too easy to lose. A CAE can use this guide as a foundation to assess an organization's framework and internal audit practices for IT risk and control, compliance, and assurance. It also can be used to meet the challenges of constant change, increasing complexity, rapidly evolving threats, and the need to improve efficiency.

IT controls do not exist in isolation. They form an interdependent continuum of protection, but they also may be subject to compromise due to weak links. IT controls are subject to error and management override, range from simple to highly technical, and exist in a dynamic environment. IT controls have two significant elements: the automation of business controls (which support business management and governance) and control of the IT environment and operations (which support the IT applications and infrastructures). The CAE needs to consider and assess both elements. The CAE may view the automated business controls as those controls where both business and IT audit skills work together in an integrated audit capacity. The CAE may want to separate the general IT controls or general computer controls (GCCs) based on the technical skills and competencies necessary to assess more technical applications, infrastructure, and operations. For example, an enterprise resource planning (ERP) application requires more technical knowledge to understand and assess controls over the ERP database structures, user access, system configuration, and financial reporting. The CAE will find that assessing infrastructure, such as networks, routers, firewalls, and wireless and mobile devices requires specialized skills and experience. The internal auditor's role in IT controls

begins with a sound conceptual understanding and culminates in providing the results of risk and control assessments. Internal auditing involves significant interaction with the people in positions of responsibility for controls and requires continuous learning and reassessment as new technologies emerge and as the organization's opportunities, uses, dependencies, strategies, risks, and requirements change.

IT controls provide for assurance related to the reliability of information and information services. IT controls help mitigate the risks associated with an organization's use of technology. They range from corporate policies to their physical implementation within coded instructions; from physical access protection through the ability to trace actions and transactions to responsible individuals; and from automatic edits to reasonability analyses for large bodies of data.

The following are examples of key control concepts:

- Assurance is provided by the IT controls within the system of internal controls. This assurance should be continuous and provide a reliable trail of evidence.
- The internal auditor's assurance is an independent and objective assessment that the IT-related controls are operating as intended. This assurance is based on understanding, examining, and assessing the key controls related to the risks they manage and performing sufficient testing to ensure the controls are designed appropriately and functioning effectively and continuously.

Many frameworks exist for categorizing IT controls and their objectives. This guide recommends that each organization use the applicable components of existing frameworks to categorize and assess IT risks and controls.

2. Introduction to the Basis of IT-related Business Risks and Controls

2.1 Key Concepts

Organizations continue to leverage the ever-changing capabilities of technology to advance their offerings and services in ways that challenge the internal audit profession. The IIA's International Standards for the Professional Practice of Internal Auditing (Standards) specifically notes that internal auditors must assess and evaluate the risks and controls for information systems that operate within the organization. The IIA has provided further perspective on assessing IT risks and controls through additional GTAGs. GTAG 4: Management of IT Auditing discusses IT risks and the resulting IT risk universe, and GTAG 11: Developing the IT Audit Plan helps internal auditors assess the business environment that the technology supports and the potential aspects of the IT audit universe. Additionally, GTAG 8: Auditing Application Controls covers the specific auditing aspects of application controls and the approach internal auditors can take when assessing the controls.

The term board is used in this GTAG as defined in the Standards glossary: "a board is an organization's governing body, such as a board of directors, supervisory board, head of an agency or legislative body, board of governors or trustees of a nonprofit organization, or any other designated body of the organization, including the audit committee to whom the chief audit executive may functionally report."

As this GTAG will explore further, the assessment of IT risks and controls in place to address them must be associated with the established business process environment and the specific organization objectives that need to be met as outlined by organization executives and the Board. IT risks are just one piece of the overall complex interconnectivity of people, processes, infrastructure, and enterprise risk environment that exists and should be managed as a whole by the organization.

Internal auditors need to understand the range of controls available for mitigating IT risks. The controls can be thought of as existing within a hierarchy that relies on the operating effectiveness interconnectivity of the controls as well as the realization that failure of a set of controls can lead to increased reliance and necessary examination of other control groups. Within this document, IT controls will be referred to in terms such as governance, management, technical, and application based on who in the organization implements and maintains them.

Another view of IT controls is in terms of general and application controls. General IT controls are typically pervasive in nature and are addressed through various audit avenues. Examples include IT operations, application development and maintenance, user management, change management, and backup and recovery. Application controls provide another category of controls and include controls within an application around input, processing, and output.

This GTAG also will explore the use of controls for managing and governing the infrastructure, processes, and personnel supporting the business through technology. IT governance continues to evolve within organizations because of the continued use of IT as well as increased oversight by management and the Board.

2.2 IT Governance

When addressing the topic of IT controls, an important consideration is IT governance, which provides the framework to ensure that IT can support the organization's overall business needs. It is important for IT management to possess a strong understanding of the organization's business processes used to meet its objectives and achieve the goals outlined by executive management and the Board. IT governance is not only composed of the controls needed to address identified risks but also is an integrated structure of IT practices and personnel that must be aligned closely with — and enable achievement of — the organization's overall strategies and goals.

A CAE needs to be able to evaluate the IT governance structure and its ability to deliver results for the organization and improve the efficiencies of the IT activity. Research efforts have indicated that IT governance does lead to improved business performance as well as better alignment of IT with the business in achieving strategic objectives.

IT governance consists of the leadership, organizational structures, and processes that ensure that the organization's IT sustains and supports the organization's strategies and objectives.

With the requirement of IIA Standard 2110.A2 stating that the internal audit activity must assess whether the IT governance of the organization supports the organization's strategies and objectives, CAEs need to be prepared to evaluate this key aspect of the overall IT landscape.

Proper application of IT governance principles has the ability to influence and impact the entire organization and how IT interacts with the business.

- **Identification and management of IT risks and enablement of improved IT operations:** IT governance helps ensure close linkage to an organization's

risk management activities, including enterprise risk management (ERM). IT governance needs to be an integral part of the overall corporate risk management efforts so that appropriate techniques can be incorporated into IT activities, including communication of risk status to key stakeholders, throughout the organization. A CAE should review the risk management activities being used by the overall organization and make sure linkage exists from IT risk management efforts to corporate risk activities and that appropriate attention is being placed on the IT risk profile.

- **Enhancing the relationship between the business and IT:** IT governance provides a mechanism to link the use of IT to an organization's overall strategies and goals. The relationship between the business and IT will make sure that IT resources are focused on doing the right things at the right time. The communication between IT and the business should be free flowing and informative, providing insight into what IT is delivering as well as the status of those efforts. A CAE should review the alignment and ensure that strong portfolio management processes exist, allowing the business and IT organizations to collaborate on resource priorities and initiatives and overall investment decisions.
- **Visibility into IT management's ability to achieve its objectives:** IT organizations will define their strategies to support the business, part of which is making sure the day-to-day IT operations are being delivered efficiently and without compromise. Metrics and goals are established not only to help IT execute on a tactical basis but also to guide the activities of the personnel to improve maturity of practices. The results will enable IT to execute its strategy and achieve its objectives established with the approval of organization leaders. A CAE should assess whether the linkage of IT metrics and objectives align with the organization's goals and become a measurement of the progress being made on approved initiatives. Additionally, the CAE can help validate that metrics are being measured effectively and represent realistic views of the IT operations and governance on a tactical and strategic basis.
- **Management of risks and identification of continuous improvement opportunities for business and IT outcomes:** Risk management is a key component of an effective IT governance structure within an organization. The identification and management of IT risks will enable the IT activity to run the business of IT more effectively while also identifying potential opportunities to improve its practices. IT risks should have defined owners who methodically communicate the status of the risk management efforts to all levels of management. The CAE provides a valuable role in validating the consistency of the IT risk universe and will use the information to help define the internal audit universe for independent risk assessment and audit planning efforts. The Risk IT Practitioner Guide developed by the IT Governance Institute (ITGI) and ISACA provides a framework for identifying and assessing IT risks while also providing a direct link to the Control Objectives for Information and Related Technology (COBIT) framework.
- **IT governance improving adaptability of IT to changing business and IT environments:** IT governance provides a foundation for IT to better manage its responsibilities and support of the business through defined processes and roles and responsibilities of IT personnel. By having such formality in place, IT has the ability to better identify potential anomalies on a daily and trending basis, leading to root cause identification of situations and issues. Additionally, IT has the ability to adapt more flexibly to ad hoc requests for new or enhanced business capabilities. Today's CAE can assess such data sources (e.g., help desk and problem management tickets) to evaluate how IT is addressing unknown issues. The CAE also can review IT portfolio management processes to understand how needs are prioritized and whether flexibility exists to reprioritize needs based on the organization's changing priorities.

As internal audit activities assess the organizations' IT governance structure and practices, several key components that lead to effective IT governance can be evaluated, including:

- **Leadership.** Evaluate the relationship between IT objectives and the organization's current/strategic needs. Assess the involvement of IT leaders in the development and ongoing execution of the organization's strategic goals. Review how roles and responsibilities are assigned within the IT activity and whether personnel perform them as designed. Also, review the role of senior management and the Board in helping establish and maintain strong IT governance.
- **Organization structures.** Review how the business and IT personnel are interacting and communicating current and future needs through the existing organizational structure. This should include the existence of necessary roles and reporting relationships to allow IT to adequately meet the needs of the business while giving the business the opportunity to have its requirements addressed through formal evaluation and prioritization.

- **IT processes.** Evaluate IT process activities and controls in place to manage the needs of the business while providing the necessary assurance over business processes and underlying systems. The IT activity uses the processes to support the IT environment and help with consistent delivery of expected services. Determine how IT will be measured in helping the organization achieve these goals.
- **Risk management.** Review the IT actvity's processes to identify, assess, and monitor/mitigate risks within the IT environment. Additionally, determine the accountability personnel have within the risk management process and how well these expectations are being met. Understand what events have occurred and impacted the IT activity to determine whether appropriate risk management practices are in place and whether risk demographics (e.g., risk frequency, impact, mitigation techniques) were appropriately documented and, if needed, updated after the event.
- **Control activities.** Assess the IT-defined key control activities to manage its business and the support of the overall organization. Internal audit should review ownership, documentation, and self-validation aspects. Additionally, the control set should be robust enough to address the identified risks.

3. Internal Stakeholders and IT Responsibilities

An organization must understand and manage its IT environment. Furthermore, it must understand and recognize the business processes' dependence on IT and the need to conform to regulatory compliance demands.
Business opportunities are exploited or lost as a consequence of success or failure in managing and using IT. Effective IT governance increases the likelihood that IT enables the business to meet its goals and that resources are prudently managed.
The following table[1] outlines a set of possible oversight functions and responsibilities with links to the Board, executive management, senior management, and internal auditors from an IT governance point of view.

Role	Responsibilities
The Board	**The Board should:** • Understand the strategic value of the IT function. • Become informed of role and impact of IT on the enterprise. • Set strategic direction and expect return. • Consider how management assigns responsibilities. • Oversee how transformation happens. • Understand constraints within which management operates. • Oversee enterprise alignment. • Direct management to deliver measurable value through IT. • Oversee enterprise risk. • Support learning, growth, and management of resources. • Oversee how performance is measured. • Obtain assurance.
Executive Management	**Executive management should:** • Become informed of role and impact of IT on the enterprise. • Cascade strategy, policies, and goals down into the enterprise, and align the IT organization with the enterprise goals. • Determine required capabilities and investments. • Assign accountability. • Sustain current operations. • Provide needed organizational structures and resources. • Embed clear accountabilities for risk management and control over IT. • Measure performance. • Focus on core business competencies IT must support. • Focus on important IT processes that improve business value. • Create a flexible and adaptive enterprise that leverages information and knowledge. • Strengthen value delivery. • Develop strategies to optimize IT costs. • Have clear external sourcing strategies.

[1] This table contains portions of the ITGI's *Board Briefing on IT Governance*, 2nd Edition, used with permission from ITGI and ISACA.

Senior Management	**Senior management should:** • Manage business and executive expectations relative to IT. • Drive IT strategy development and execute against it. • Link IT budgets to strategic aims and objectives. • Ensure measurable value is delivered on time and budget. • Implement IT standards, policies and control framework as needed. • Inform and educate executives on IT issues. • Look into ways of increasing IT value contribution. • Ensure good management over IT projects. • Provide IT infrastructures that facilitate cost-efficient creation and sharing of business intelligence. • Ensure the availability of suitable IT resources, skills, and infrastructure to meet objectives and create value. • Assess risks, mitigate efficiently, and make risks transparent to the stakeholders. • Ensure that roles critical for managing IT risks are appropriately defined and staffed. • Ensure the day-to-day management and verification of IT processes and controls. • Implement performance measures directly and demonstrably linked to the strategy. • Focus on core IT competencies.
The Internal Audit Activity	**The internal audit activity should:** • Ensure a sufficient baseline level of IT audit expertise in the department. • Include evaluation of IT in its planning process. • Assess whether IT governance in the organization sustains and supports strategies and objectives. • Identify and assess the risk exposures relating to the organization's information systems. • Assess controls responding to risks within the organization's information systems. • Ensure that the audit department has the IT expertise to fulfil its engagements. • Consider use technology-based audit techniques as appropriate.

In addition to internal stakeholders, it is also important to take into consideration external parties, such as the external auditor, national authorities, public expectations, and international organizations for standardization.

4. Analyzing Risks

IT controls are selected and implemented on the basis of the risks they are designed to manage. As risks are identified, suitable risk responses are determined and range from doing nothing and accepting the risk as a cost of doing business to applying a wide scope of specific controls. This section explains the concepts of when to apply IT controls.

It would be a relatively straightforward task to create a list of recommended IT controls that must be implemented within each organization. However, each control has a specific cost that may not be justified in terms of cost effectiveness when considering the type of organization and industry. Furthermore, no list of controls is universally applicable across all types of organizations. Although there is a lot of good advice available on the choice of suitable controls, strong judgment must be used. Controls must be appropriate for the level of risk the organization faces. The CAE should be able to advise the audit committee that the internal control framework is reliable and provides a level of assurance appropriate to the organization's risk appetite. In this respect, the Committee of Sponsoring Organizations of the Treadway Commission (COSO)[2] defines risk appetite as:

"... the degree of risk, on a broad-based level, that a company or other organization is willing to accept in pursuit of its goals. Management considers the organization's risk appetite first in evaluating strategic alternatives, then in the setting of objectives aligned with the selected strategy, and in developing mechanisms to manage the related risks."

In addition to risk appetite, the CAE should consider risk tolerance. COSO defines risk tolerance as:

"... the acceptable level of variation relative to the achievement of objectives. In setting specific risk tolerances, management considers the relative importance of related objectives and aligns risk tolerances with its risk appetite."

Therefore, the CAE should consider whether:

- The organization's IT environment is consistent with the organization's risk appetite.
- The internal control framework is adequate to ensure the organization's performance remains within the stated risk tolerances.

[2] The Committee of Sponsoring Organizations of the Treadway Commission, "Committee of Sponsoring Organizations for the Commission on Fraudulent Financial Reporting." www.coso.org.

4.1 Risk Considerations in Determining the Adequacy of IT Controls

Risk management applies to the entire spectrum of activity within an organization — not just to the application of IT. IT cannot be considered in isolation. Rather, IT must be treated as an integral part of all business processes. Choosing IT controls is not a matter of implementing those recommended as best practices; controls must add value to the organization by reducing risk efficiently and increasing effectiveness. When considering the adequacy of IT controls within the organization's internal control framework, the CAE should consider the processes established by management to determine:

- The use, value, and criticality of information.
- The organization's risk appetite and tolerance for each business function and process.
- IT risks faced by the organization and quality of service provided to its users.
- The complexity of the IT infrastructure.
- The appropriate IT controls and the benefits they provide.

The frequency of risk analysis is important and is influenced greatly by both internal and external changes. The speed of technological change will impact each organization differently. Some organizations will need to respond to the risks associated with technology changes rapidly while others may decide to respond at a more measured pace.

4.1.1 The IT Environment

Analyzing and assessing risk in relation to IT can be complex. The IT infrastructure comprises hardware, software, communications, applications, protocols (i.e., rules), and data, as well as their implementation within physical space, within the organizational structure, and between the organization and its external environment. Infrastructure also includes the people interacting with the physical and logical elements of systems.

Other areas to consider include project-related and provider risks. For example, project-related risk includes insufficient budget, resources, project management, and technical skills. For third-party provider and vendor risks, the IT auditor should analyze issues such as stability, financial strength, review of IT controls, and audit rights.

The inventory of IT infrastructure components reveals basic information about the environment's vulnerabilities. For example, business systems and networks connected to the Internet are exposed to threats that do not exist for self-contained systems and networks. Because Internet connectivity is an essential element of most business systems

and networks, organizations must make certain that their systems and network architectures include fundamental controls that ensure basic security.

The complete inventory of the organization's IT hardware, software, network, and data components forms the foundation for assessing the vulnerabilities within the IT infrastructure. Systems architecture schematics reveal the implementation of infrastructure components and how they interconnect with other components inside and outside the organization. To the information security expert, the inventory and architecture of IT infrastructure components, including the placement of security controls and technologies, reveal potential vulnerabilities. Unfortunately, information about a system or network also can reveal vulnerabilities to a potential attacker, so access to such information must be restricted to only those people who need it. A properly configured system and network environment will minimize the amount of information it provides to would-be attackers, and an environment that appears secure presents a less attractive target to attackers.

4.1.2 IT Risks Faced by the Organization

The CAE discusses IT risk issues with the CIO and process owners to assess whether all related parties have an appropriate awareness and understanding of the technical risks the organization faces through the use of IT as well as their roles in applying and maintaining effective controls.

4.1.3 Risk Appetite and Tolerance

Armed with the knowledge of IT risks, the auditor can validate the existence of effective controls to meet the organization's established risk appetite and its risk tolerance in relation to IT. The auditor's assessment will involve discussions with many members of management and —potentially — the Board. The level of detail of these discussions can be determined with input from the CIO, the chief information security officer (CISO), and process owners.

An organization's use of ERM must include IT risks as part of this process. ERM includes methods and processes to manage risks and seize opportunities in achieving the organization's objectives. It typically starts with identifying particular events or circumstances relevant to the organization's objectives (e.g., the risks of data breaches), assessing them in terms of likelihood and magnitude of impact (e.g., the inherent risk of a data breach is rated high, and the impact also is rated as high), determining a response (e.g., new policies to better secure the organization's data), and monitoring progress on the implementation of responses (e.g., the IT activity's implementation of new security measures to avoid data breaches). By identifying and proactively addressing risks and opportunities, organizations will be better suited to protect and create value for stakeholders. In this way, ERM assists the CAE in understanding the significant risks for the entire organization. Then, the CAE can use this perspective to set audit priorities, determine audit project activities, and establish risk appetite and tolerance.[3]

4.1.4 Performing a Risk Analysis

A risk analysis should be performed with involvement from various roles and departments within an organization, including the chief risk officer (CRO), CAE, IT activity, and business representatives.

Basic questions associated with the risk assessment process include:

- Which IT assets (this includes both tangible and intangible IT assets, such as information or reputation) are at risk, and what is the value of their confidentiality, integrity, and availability?
- What could happen to adversely affect that information's asset value (threat event)? Implicit to this question is the vulnerability analysis and mapping of vulnerabilities to threats and potentially impacted information assets.
- If a threat event happened, how bad could its impact be?
- How often might the event be expected to occur (frequency of occurrence)?
- How certain are the answers to the first four questions (uncertainty analysis)?
- What can be done to reduce the risk?
- How much will it cost?
- Is it cost-efficient?

Determining the value of the information processed and stored is not an easy task due to the multidimensional nature of value. The CAE will find it helpful to work with the CRO to coordinate and align the IT-related risks. Depending on the organization's size and risks, the CAE and CRO may want to share how they prioritize risk areas, risk coverage, or leverage resources.

[3] COSO, *Strengthening Enterprise Risk Management for Strategic Advantage*, Nov. 4, 2009.

4.2 Risk Mitigation Strategies

When risks are identified and analyzed, it is not always appropriate to implement controls to counter them. Some risks may have minor impact if they occur or may be extremely unlikely to occur, and it may not be cost-effective to implement expensive control processes.

In general, there are several ways to treat risks.

- **Accept the risk.** One of management's primary functions is managing risk. Some risks are minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate as well as periodically reviewing the risk to ensure its impact remains low.
- **Eliminate the risk.** It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.
- **Share the risk**. Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization. Risk also may be mitigated by transferring the risk to an insurance provider.
- **Control/mitigate the risk.** Instead of — or in combination with — other options, controls may be devised and implemented to prevent the risk from manifesting itself to limit the likelihood of this manifestation or to minimize its effects.

5. Assessing IT — An Overview

IT controls applied when controlling or mitigating the risks is the best option. While IT controls should be applied with due regard to the relevant risks, there is a basic set of controls that should be in place to provide a fundamental level of IT control.

IT controls should be part of major IT processes related to planning, organization, acquisitions, changes, delivery of IT services, and IT support and monitoring. IT controls supporting a wide range of these IT processes typically would be the IT infrastructure controls that cover areas such as network controls, database controls, operating system controls, and hardware controls, for example. IT controls that cover applications and, in many cases, important business areas could include input edit controls, process completion or reconciliation controls, and exception report controls. The CAE should gain an overview of the important controls and what business processes they support as a first step in understanding IT risks and controls. Process descriptions and organization charts are some of the tools that can be used to gain an overview. Additionally, the CAE should obtain an understanding of key IT initiatives to comprehend how the IT infrastructure and applications may be changing during a defined period of time. This information will enable the CAE to perform an initial risk assessment that allows for a deeper analysis.

Some questions can be considered when evaluating the control environment and selecting a suitable set of controls.

- Do IT policies — including IT controls — exist?
- Have responsibilities for IT and IT controls been defined, assigned, and accepted?
- Is the control designed effectively?
- Is the control operating effectively?
- Does the control achieve the desired result?
- Is the mix of preventive, detective, and corrective controls effective?
- Do the controls provide evidence when control parameters are exceeded or when controls fail? How is management alerted to failures, and which steps are expected to be taken?
- Is evidence retained (e.g., through an audit trail)?
- Are the IT infrastructure equipment and tools logically and physically secured?
- Are access and authentication control mechanisms used?
- Are controls in place to protect the operating environment and data from viruses and other malicious software?
- Are firewall-related controls implemented?
- Do firewall polices exist?
- Are external and internal vulnerability assessments completed, and have risks been identified and resolved appropriately?
- Are change and configuration management and quality assurance processes in place?
- Are structured monitoring and service measurement processes in place?
- Have the risks of outsourced services been taken into consideration? (For details on this, refer to *GTAG 7: IT Outsourcing*.)

The payment card industry publishes one of the more widely and broadly used data security standards — PCI Data Security Standards (PCI DSS). Launched in 2006, the PCI Security Standards Council represents an open, global forum that is responsible for the development, management, education, and awareness of the PCI Security Standards, including the PCI DSS, the Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements.

The CAE can use the PCI DSS at a high level to determine whether certain security activities should be considered for the organization (see the following PCI Data Security Standards High Level Overview).

Introduction and PCI Data Security Standard Overview

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing —including merchants, processors, acquirers, issuers, and service providers, as well as all other entities which store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholders data, and may be enhanced by additional controls and practices to further mitigate risks. Below is a high-level overview of the 12 PCI DSS requirements

PCI Data Security Standard – High Level Overview	
Build and maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to =cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

[4]

Assessing IT controls is a continuous process. Business procedures constantly change as technology continues to evolve, and threats emerge as new vulnerabilities are discovered. Audit methods improve as internal auditors adopt an approach where IT control issues in support of the business objectives are a top priority. Management provides IT control metrics and reporting, and auditors attest to their validity and opine on their value. The internal auditor should liaise with management at all levels to agree on the validity and effectiveness of the metrics and assurances for reporting.

The internal audit process provides a formal structure for addressing IT controls within the overall system of internal controls. Figure 1 – The Structure of IT Auditing, divides the assessment into a logical series of steps.

[4] PCI DSS Requirements and Security Assessment Procedures, V2.0, Copyright 2010 PCI Security Standards Council LLC

Figure 1 – The Structure of IT Auditing

Assessing It Controls		
	Understanding IT Controls	Governence - Management - Technical
		General Application
		Prevention, Detection, Correction
		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

The internal auditor's role in IT controls begins with a sound conceptual understanding and culminates in providing the results of risk and control assessments. The CAE should oversee the pursuit of continuous learning and reassessment as new technologies emerge and as dependencies, strategies, risks, and requirements change.

6. Understanding the Importance of IT Controls

Although this GTAG deals exclusively with IT risks and controls, the control environment within IT (e.g. tone at the top from the CIO, the ethical climate, management philosophy, and operating style) is critically important and should be evaluated. The IIA's Practice Guide, Auditing the Control Environment, should be consulted in addition to this GTAG when considering the control environment within IT.

COSO defines internal control as: "A process, effected by an entity's board of directors, management, and other personnel. This process is designed to provide reasonable assurance regarding the achievement of objectives in:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations."

IT controls encompass those processes that provide assurance for information and information services and help control or mitigate the risks associated with an organization's use of technology. These controls range from written corporate policies to their implementation within coded instructions; from physical access protection to the ability to trace actions and transactions to the individuals who are responsible for them; and from automatic edits to reasonability analyses for large bodies of data.

It is not necessary for the CAE to know everything about IT controls, including the full continuum or all the technical intricacies. Many of these controls are the domain of specialists who manage specific risks associated with individual components of the systems and network infrastructure.

6.1 IT General and Application Controls

Controls may be classified to help understand their purposes and where they fit into the overall system of internal controls (see Figure 2 – Some Control Classifications). By understanding these classifications, the control analyst and auditor are better able to establish their positions in the control framework and answer key questions such as: Are the detective controls adequate to identify errors that may get past the preventive controls? Are corrective controls sufficient to fix the errors once detected? A common classification of IT controls is general versus application. For further definition of IT related controls, refer to GTAG 8: Auditing Application Controls.

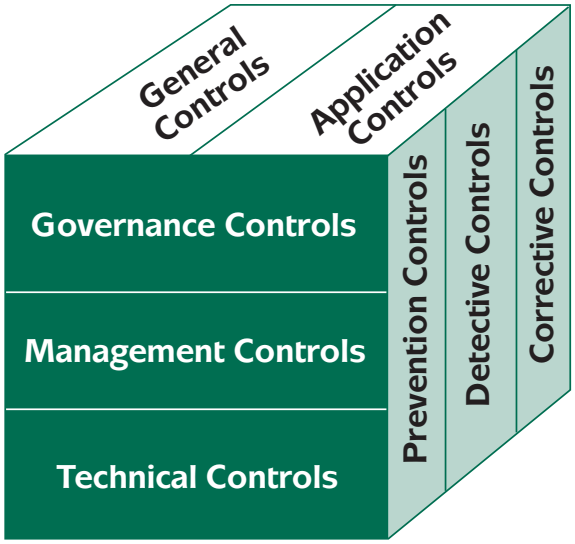

Figure 2 – Some Control Classifications

6.1.1 IT General Controls

General controls apply to all systems components, processes, and data for a given organization or systems environment. General controls include, but are not limited to, IT governance, risk management, resource management, IT operations, application development and maintenance, user management, logical security, physical security, change management, backup and recovery, and business continuity. Some general controls are business-related (e.g., segregation of duties or governance arrangements), whereas others are very technical (e.g., system software controls and network software controls) and relate to the underlying infrastructure. General controls are reviewed by internal audit because they form the basis of the IT control environment. If the general controls are weak and unreliable (e.g., change and access control) and cannot be relied on, the auditor may need to alter the testing approach for those areas impacted.

6.1.2 Application Controls

Application controls[5] pertain to the scope of individual business processes or application systems and include controls within an application around input, processing, and output. Application controls also can include data edits, segregation of business functions (e.g., transaction initiation versus authorization), balancing of processing totals, transaction logging, and error reporting.

[5] PCI Security Standards Council LLC, *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures*, Version 2.0., Oct. 2010.

The function of a control is highly relevant to the assessment of its design and effectiveness. Controls usually are classified as preventive, detective, or corrective. Preventive controls prevent errors, omissions, or security incidents from occurring. Examples include simple data entry edits that block alphabetic characters from being entered into numeric fields; access controls that protect sensitive data or system resources from unauthorized people; and complex and dynamic technical controls such as antivirus software, firewalls, and intrusion prevention systems.

Detective controls detect errors or incidents that elude preventive controls. For example, a detective control may identify account numbers of inactive accounts or accounts that have been flagged for monitoring of suspicious activities. Detective controls also can include monitoring and analysis to uncover activities or events that exceed authorized limits or violate known patterns in data that may indicate improper manipulation. For sensitive electronic communications, detective controls can indicate that a message has been corrupted or that the sender cannot be authenticated.

Corrective controls correct errors, omissions, or incidents once they have been detected. They vary from simple correction of data entry errors to identifying and removing unauthorized users or software from systems or networks to recovery from incidents, disruptions, or disasters.

Generally, it is most efficient to prevent errors or detect them as soon as possible to simplify correction.

Many other control classifications described in this document may be useful in assessing their effectiveness. For example, automated controls tend to be more reliable than manual controls, and nondiscretionary controls are more likely to be applied consistently than discretionary controls. Other control classifications may exist such as mandatory, voluntary, complementary, compensating, redundant, continuous, on-demand, and event-driven.

6.2 IT Governance, Management, and Technical Controls

Another common classification of controls is by the group responsible for ensuring they are implemented and maintained properly. For the purpose of assessing roles and responsibilities, this guide primarily categorizes IT controls as governance, management, technical, and application.

The first two levels — governance and management — are the most applicable to the scope of this guide. However, it also may be useful to understand how higher-level controls specifically are established within the technical and application IT infrastructures. Technical controls and application controls are the subject of GTAG 8: Auditing Application Controls.

6.2.1 IT Governance Controls

The primary responsibility for internal control oversight resides with the Board in its role as keeper of the governance framework. IT control at the governance level involves overseeing effective information management, principles, policies, and processes and ensuring that they are in place and performing correctly. These controls are linked with the concepts of governance, which are driven both by organizational goals and strategies and by outside bodies, such as regulators.

6.2.2 Management Controls

Management responsibility for internal controls typically involves reaching into all areas of the organization with special attention to critical assets, sensitive information, and operational functions. Management must make sure the IT controls needed to achieve the organization's established objectives are applied and ensure reliable and continuous processing. These controls are deployed as a result of deliberate actions by management in response to risks to the organization, its processes, and assets.

6.2.3 Technical Controls

Technical controls often form the backbone of management's control framework. Therefore, if the technical controls are weak, the impact affects the entire control framework. For example, by protecting against unauthorized access and intrusion, technical controls provide the basis for reliance on the integrity of information — including evidence of all changes and their authenticity. These controls are specific to the technologies in use within the organization's IT infrastructures. Examples of technical controls are operating system controls, database controls, encryption, and logging.

6.2.4 Application Controls

As already established, application controls pertain to the scope of individual business processes or application systems. They may be technical in nature but are also nontechnical depending on the area of control. They include controls of input, processing, and output. Section 6.3.7 of this document discusses application controls in more depth.

6.3 IT Controls — What to Expect

Individual controls within an organization can be classified within the hierarchy of IT controls — from the overall high-level policy statements issued by management and endorsed by the Board down to the specific control mechanisms incorporated into application systems.

Figure 3 – Hierarchy of IT Controls represents a logical "top-down" approach both when considering controls to implement and when determining areas on which to focus internal audit resources during reviews of the entire IT operating environment. The different elements of the hierarchy are not mutually exclusive; they connect with each other and often overlap and intermingle. Each of the control types within the hierarchy are described below.

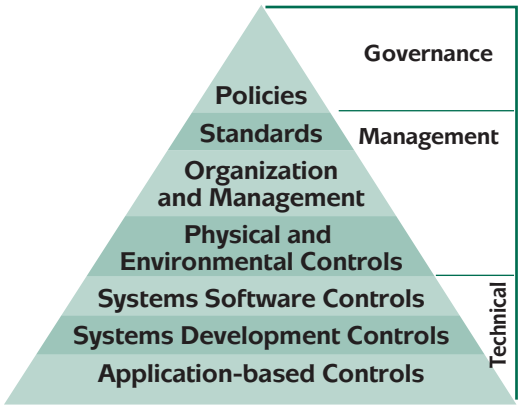

Figure 3 – Hierarchy of IT Controls

6.3.1 Policies

All organizations need to define their goals and objectives through strategic plans and policy statements. Without clear statements of policy and standards for direction, organizations can become disoriented and perform ineffectively.

Because technology is vital to virtually all organizations, clear policy statements regarding all aspects of IT should be devised and approved by management, endorsed by the Board, and communicated to staff. Many different policy statements can be required depending on the organization's size and the extent to which it deploys IT. For smaller organizations, a single policy statement may be sufficient — provided it covers all relevant areas. Larger organizations often will require more detailed and specific policies.

For example, IT policy statements may include, but are not restricted to:

- A general policy on the level of security and privacy throughout the organization. This policy should be consistent with relevant national and international legislation and should specify the level of control and security required depending on the sensitivity of the system and data processed.
- A statement on the classification of information and the rights of access at each level. The policy also should define any limitations on the use of this information by those approved for access.
- A definition of the concepts of data and systems ownership, as well as the authority necessary to originate, modify, or delete information. This should be a general policy that defines the extent to which users can create their own applications.
- Personnel policies that define and enforce conditions for staff in sensitive areas. This includes the positive vetting of new staff prior to joining the organization and requiring employees to sign agreements accepting responsibility for the required levels of control, security, and confidentiality. This policy typically would also detail related disciplinary procedures.
- Definitions of overall business continuity planning requirements. These policies should ensure that all aspects of the business are considered when an unexpected event or disaster happens.

6.3.2 Standards

The organization should have an IT blueprint that supports its overall strategy and sets the tone for the resultant IT policies and standards.[6]

The standards define ways of working to achieve the objectives of the organization. Adopting and enforcing standards promotes efficiency and ensures consistency in the IT operating environment.

Large organizations with significant resources are in a position to devise their own standards, but smaller organizations may not have sufficient resources. There are many sources of information on standards and best practice. For example, IT management should consider:

- **Systems development processes:** When organizations develop their own applications, standards apply to the processes for designing, developing, testing, implementing, and maintaining systems and programs. If organizations outsource application development or acquire systems from vendors, the CAE should ascertain that agreements require the providers to apply standards consistent with the organization's standards or are acceptable to the organization.
- **Systems software configuration:** Because systems software provides a large element of control in the

[6] The *Institute of Internal Auditors International Standards for the Professional Practice of Internal Auditing* ensures that the internal audit activity examines the IT strategy. IIA Standard 2110.A2 states: "The internal audit activity must assess whether the information technology governance of the organization sustains and supports the organization's strategies and objectives."

IT environment, standards related to secure system configurations are beginning to gain wide acceptance by leading organizations and technology providers. The way products — such as operating systems, networking software, and database management systems — are configured can either enhance security or create weaknesses that can be exploited.

- **Application controls:** All applications that support business activities need to be controlled. Standards are necessary for all applications the organization develops or purchases, and the standards should define the types of controls that must be present across the whole range of business activities as well as the specific controls that should apply to sensitive processes and information.
- **Data structures:** Having consistent data definitions across the full range of applications ensures that disparate systems can access data seamlessly and security controls for private and other sensitive data can be applied uniformly.
- **Documentation:** Standards should specify the minimum level of documentation required for each application system or IT installation, as well as for different classes of applications, processes, and processing centers.

As with policies, written standards should be approved by management and made available to everyone who implements them.

6.3.3 Organization and Management

Organization and management play a major role in the whole system of IT control in addition to every aspect of an organization's operations. An appropriate organization structure allows lines of reporting and responsibility to be defined and effective control systems to be implemented. Important controls typically could include segregation of incompatible duties, financial controls, and change management.

6.3.3.1 Segregation of Duties

Segregation of duties is a vital element of many controls. An organization's structure should not allow responsibility for all aspects of processing data to rest with one individual. The functions of initiating, authorizing, inputting, processing, and checking data should be separated to ensure no individual can create an error, omission, or other irregularity and authorize it and/or obscure the evidence. Segregation-of-duties controls for application systems are implemented by granting access privileges in accordance with job requirements for processing functions and accessing information.

Traditional segregation of duties within the IT environment is divided between systems development and IT operations. IT operations should be responsible for running production systems — except for change deployment — and should have little or no responsibility with the development process. This control includes restrictions preventing operators from accessing or modifying production programs, systems, or data. Similarly, systems development personnel should have little contact with production systems. By assigning specific roles during implementation and other change processes, segregation of duties can be enforced. In large organizations, many functions should be considered to ensure appropriate segregation of duties.

6.3.3.2 Financial Controls

Because organizations make considerable investments in IT, budgetary and other financial controls are necessary to ensure the technology yields the projected return on investment or proposed savings. Management processes should be in place to collect, analyze, and report on these issues. Unfortunately, new IT developments often suffer massive cost overruns and fail to deliver the expected cost savings or income because of wrong estimates or insufficient planning.

6.3.3.3 Change Management

Change management[7] processes ensure that changes to the IT environment, systems software, application systems, and data are applied in a manner that enforces appropriate segregation of duties; ensures that changes work and are implemented as required; and prevents changes from being exploited for fraudulent purposes. A lack of change management can seriously impact system and service availability.

6.3.4 Physical and Environmental Controls

IT equipment represents a considerable investment for many organizations. It must be protected from accidental or deliberate damage or loss. Physical and environmental controls, originally developed for large data centers that house mainframe computers, are equally important in distributed client-server and Web-based systems. Although the equipment commonly used today is designed for ease of use in a normal office environment, its value to the business and the cost and sensitivity of applications running business processes can be significant.

All equipment must be protected, including the servers and workstations that allow staff access to the applications. Some typical physical and environmental controls include:

- Locating servers in locked rooms to which access is restricted.
- Restricting server access to specific individuals.

[7] Refer to The IIA's GTAG 2: *Change and Patch Management Controls: Critical for Organizational Success*.

- Providing fire detection and suppression equipment.
- Housing sensitive equipment, applications, and data away from environmental hazards, such as low-lying flood plains, flight paths, or flammable liquid stores.

When considering physical and environmental security, it is also appropriate to consider contingency planning[8]. What will the organization do if there is a fire or flood or if any other threat manifests itself? How will the organization continue its operations? This type of planning goes beyond merely providing for alternative IT processing power to be available and routine backup of production data; it must consider the logistics and coordination needed for the full scope of business activity. Finally, history consistently demonstrates that business continuity planning that has not been tested successfully in a realistic simulation is not reliable.

6.3.5 Systems Software Controls

Systems software products enable the IT equipment to be used by the application systems and users. These products include operating systems (e.g., Windows and UNIX), network and communications software, firewalls, antivirus products, and database management systems (DBMS) (e.g., Oracle and DB2).

IT audit specialists should assess controls in this area. Small organizations are unlikely to have the resources to employ such specialists and should consider using external resources. Whether IT auditors are employed or outsourced, they require a highly specific set of knowledge. Much of this knowledge can come from experience, but such knowledge must be updated constantly to remain current and useful.

Systems software can be highly complex and can apply to components and appliances within the systems and network environment. Software may be configured to accommodate highly specialized needs and normally requires a high degree of specialization to securely maintain it. Configuration techniques can control logical access to the applications, although some application systems contain their own access controls and may provide an opening for unauthorized users to break into a system. Configuration techniques also provide the means to enforce segregation of duties, generate specialized audit trails, and apply data integrity controls through access control lists, filters, and activity logs.
Some key technical controls to be expected in a well-managed IT environment include:

- Access rights allocated and controlled according to the organization's stated policy.
- Division of duties enforced through systems software and other configuration controls.
- Intrusion and vulnerability assessment[9], prevention, and detection in place and continuously monitored.
- Intrusion testing performed on a regular basis.
- Encryption services applied where confidentiality is a stated requirement.
- Change management processes — including patch management — in place to ensure a tightly controlled process for applying all changes and patches to software, systems, network components, and data.[10]

6.3.6 Systems Development and Acquisition Controls

Organizations rarely adopt a single methodology for all system acquisitions or development. Methodologies are chosen to suit the particular circumstances. The IT auditor should assess whether the organization uses a controlled method to develop or acquire application systems and whether it delivers effective controls over and within the applications and data they process. By examining application development procedures, the auditor can gain assurance that application controls are adequate. Some basic control issues should be addressed in all systems development and acquisition work. For example:

- User requirements should be documented, and their achievement should be measured.
- Systems design should follow a formal process to ensure that user requirements and controls are designed into the system.
- Systems development should be conducted in a structured manner to ensure that requirements and approved design features are incorporated into the finished product.
- Testing should ensure that individual system elements work as required, system interfaces operate as expected, and that the system owner has confirmed that the intended functionality has been provided.
- Application maintenance processes should ensure that changes in application systems follow a consistent pattern of control. Change management should be subject to structured assurance validation processes.

Where systems development is outsourced, the outsourcer or provider contracts should require similar controls. Project management techniques and controls should be part of

[8] Refer to The IIA's *GTAG 10: Business Continuity Management*.

[9] Refer to The IIA's *GTAG 6: Managing and Auditing IT Vulnerabilities*.

[10] Refer to The IIA's *GTAG 2: Change and Patch Management Controls: Critical for Organizational Success*.

the development process — whether developments are performed in-house or are outsourced. Management should know whether projects are on time and within budget and that resources are used efficiently. Reporting processes should ensure that management understands the current status of development projects and does not receive any surprises when the end product is delivered.[11] The IIA's GTAG 12: Auditing IT Projects also should be considered when assessing development or acquisition projects.

6.3.7 Application Controls[12]

The objective of controls over application systems is to ensure that:

- All input data is accurate, complete, authorized, and correct.
- All data is processed as intended.
- All data stored is accurate and complete.
- All output is accurate and complete.
- A record is maintained to track the process of data from input to storage and to the eventual output.

Reviewing application controls traditionally has been the realm of the specialist IT auditor. However, because application controls now represent a large percentage of business controls, they should be a key concern of every internal auditor.

There are several types of generic controls that should exist in any application.

- **Input controls:** These controls are used mainly to check the integrity of data entered into a business application, whether the source is input directly by staff, remotely by a business partner, or through a Web-enabled application. Input is checked to ensure that it remains within specified parameters.
- **Processing controls:** These controls provide automated means to ensure processing is complete, accurate, and authorized.
- **Output controls:** These controls address what is done with the data. They should compare results with the intended result and check them against the input.
- **Integrity controls:** These controls can monitor data in process and/or storage to ensure that data remains consistent and correct.
- **Management trail:** Processing history controls, often referred to as an audit trail, enable management to track transactions from the source to the ultimate result and to trace backward from results to identify the transactions and events they record. These controls should be adequate to monitor the effectiveness of overall controls and identify errors as close as possible to their sources.

6.4 Information Security

Information security[13] is an integral part of IT controls. Information security applies to both infrastructure and data and is the foundation for the reliability of most other IT controls. The exceptions are controls relating to the financial aspects of IT (e.g., ROI and budgetary controls) and some project management controls. The generally accepted elements of information security are:

- **Confidentiality:** Confidential information must be divulged only as appropriate and must be protected from unauthorized disclosure or interception. Confidentiality includes privacy considerations.
- **Integrity:** Information integrity refers to the state of data as being correct and complete. This specifically includes the reliability of financial processing and reporting.
- **Availability:** Information must be available to the business, its customers, and partners when, where, and in the manner needed. Availability includes the ability to recover from losses, disruption, or corruption of data and IT services, as well as from a major disaster where the information was located.

6.5 IT Controls Framework

For the more than 50 years that organizations have used IT, controls have not always been the default condition of new systems hardware or software. The development and implementation of controls typically lag behind the recognition of emerging risks in systems and the threats that exploit such vulnerabilities. Furthermore, IT controls are not defined in any universally recognized standard applicable to all systems or to the organizations that use them.

A control framework is a structured way of categorizing and identifying controls to adequately secure an IT environment. The framework can be informal or formal. A formal approach will more readily satisfy the various regulatory or statutory requirements for organizations subject to them. The process of choosing or constructing a control framework should involve all concerned parties, including the business process owners and the parties responsible for performing the controls. The control framework should apply to, and be used by, the whole organization.

---

[11] Refer to The IIA's *GTAG 14: Auditing User-developed Applications*.

[12] Refer to The IIA's *GTAG 8: Auditing Application Controls*.

[13] Refer to The IIA's *GTAG 15: Information Security Governance*.

7. IT Audit Competencies and Skills

According to the IPPF, internal auditors are expected to apply and uphold four principles: integrity, objectivity, confidentiality, and competency. The principle of competency requires internal auditors to engage only in those services for which they have the necessary knowledge, skills, and experience. Furthermore, IIA Attribute Standard 1210: Proficiency states: "Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities."

The CAE must obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement. The IIA provides an Integrated Competency Framework to help identify the necessary competencies to maintain in the internal audit activity. This approach links the identified business risks to the related IT processes. Hence, the CAE should know what kind and level of IT skills and competencies are required for auditing the effectiveness of the controls over the identified business risks. The following table shows a few examples for mapping business risks and required IT controls as well as the skills/competencies needed to perform the audit.

Business Risk	IT Controls	IT Skills and Competencies
Information security management	A sound, logical security control	Security administration; access controls at network, operating system, database, and application levels
Critical business disruption	Ensuring availability of critical business applications	Business continuity and disaster recovery planning for the IT facilities (including network infrastructure, operating systems, databases, and applications)
Inaccurate and incomplete financial and management reporting	Securing data confidentiality and availability	Application controls, change controls, and system development life cycle (SDLC) controls

If the required IT skills and competencies are not available within the internal audit activity, the CAE may seek an external service provider to support or complement the internal staff (i.e., out-sourcing or co-sourcing).[14]

[14] Refer to IIA Practice Advisory 1210.A1-1: Obtaining External Service Providers to Support or Complement the Internal Audit Activity.

8. Use of Control Framework

Each organization should examine existing control frameworks to determine which of them — or which parts — most closely fit its needs. The process of choosing or constructing a control framework should involve all people in the organization with direct responsibility for controls. The internal audit activity will assess the framework's adequacy and use it as a context for planning and performing internal audit work.

The CAE needs an overall knowledge of IT risk issues to assess the effectiveness and appropriateness of IT controls. The CAE will base the internal audit plan and allocate resources on the IT areas and issues that merit attention due to their inherent levels of risk. Risk analysis and assessment cannot be viewed as a one-time process, especially when applied to IT. Technology changes constantly and rapidly as do the associated risks and threats. Categorizing IT controls according to their organizational placement, purpose, and functionality is useful in assessing their value and adequacy, as well as the adequacy of the system of internal controls. Knowledge of the range of available IT controls, the driving forces for controls, and organizational roles and responsibilities allows for comprehensive risk analyses and assessments. In assessing control effectiveness, it also is useful to understand whether the controls are mandated or voluntary, discretionary or nondiscretionary, manual or automated, primary or secondary, and subject to management override.

Finally, the assessment of IT controls involves selecting key controls for testing, evaluating test results, and determining whether evidence indicates any significant control weaknesses. The checklist included in the appendix can help ensure all relevant issues have been considered when planning and directing internal audit assessments of IT controls. Several existing frameworks and approaches can assist the CAE and other managers when determining IT control requirements. However, organizations should investigate enough frameworks to determine which one best fits their own needs and culture.

8.1 Computer Aided Audit Techniques and the Use of Data Analysis

CAEs should consider the use of computer aided audit techniques — especially data analysis tools — to obtain a more real-time perspective of the IT risk landscape and to potentially identify anomalies. In an environment where organizations and internal audit activities need to do more with less, data analysis provides an opportunity for the CAE to leverage information available throughout the organization and identify potential areas of focus for risk assessment or audit activities. Data analysis also can offer the CAE an approach to constantly assess the operating effectiveness of internal controls and review indicators of emerging risks. Available data analysis tools provide increased functionality for auditing the information and for efficiently processing larger amounts of data. However, there are key challenges: the CAE needs to obtain the technical skills, access the data analysis tools, leverage the reporting/extract tools, access the data sources, and develop a strategy that focuses on the highest organizational risks.

Continuous auditing is similar to continuous monitoring, as data is continually analyzed or assessed by the internal auditor. Continuous monitoring represents a management responsibility and function. Internal audit may test, review, or leverage the use of continuous monitoring. For more information, refer to The IIA's *GTAG 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment.*

8.2 Using Automated Risk Assessment

The CAE may find that strengthening his or her risk assessment requires numeric scoring or detailed risk assessment. Certain tools are available for automating the risk analysis process. These tools allow for risk scoring, annotating impact, and rating likelihood, among other factors. Automating the risk assessment allows for comparing and prioritizing risks. Collecting inherent and residual risk factors allows the CAE to provide summary information, such as heat maps or risk profiles that meet the organization's risk profile. The automation of internal audit management is a major topic in its

How Auditing Contributes to IT Controls

During the last few decades, there have been periods of reflection when management and auditors agreed the auditors could add value to the organization by contributing their controls expertise to development processes to ensure appropriate controls were incorporated into new systems, rather than adding controls after an audit revealed a deficiency. These activities coincided with the developments in control and risk self-assessment in the mainstream audit world. Audit consulting and risk-based auditing became widespread. The 1990s and beyond also saw dramatic increases in attention to information security management as cyberattacks increased in number and severity. These events have helped shape the role of the IT auditor as well as the businesses world's recognition of the importance of effective information security management.

own right, and one area of opportunity is automating the risk assessment process (e.g., using voting tools to allow management to record risk ratings).

8.3 Reporting on IT Controls

CAEs need to communicate to key stakeholders — such as the audit committee, executive management, regulators, external auditors, or the CIO — on the results of the assurance engagements. CAEs can use a number of report formats, and approaches can range from updates to balanced scorecards or to private executive session presentations.
One approach is to begin with simple updates on the assessment. The CAE should first determine the inherent level of risk over certain key IT processes. For example, the CAE can provide and verify with the CIO or key IT stakeholders the inherent risk over development, operations, business continuity planning, network, information security, and change management. Often, the inherent risk depends on the IT strategy and organization. Some IT organizations may be outsourced, centralized, or decentralized. The updates may take the form of audit projects in various functional IT areas. The update may include significant findings or issues. Progress on audit recommendations also might be part of the IT update.

Another approach is to report in a balanced scorecard. This may align with the CIO's reporting of IT strategy or operations using an IT balanced scorecard. The Balanced Scorecard Institute provides one template that views the IT activity from four perspectives: financial, internal business process, learning and growing, and customer. When the CAE reports on IT as part of the regular audit report to the Board, audit committee, or management, the report typically would include issues related to information security incidents, change management exceptions, project development status, operation incident reporting, capital spending, or other metrics that measure key IT risks and controls. Such an approach should provide an integrated and comprehensive approach of all risks and controls — from business to IT — in one format.

Sometimes the CAE may need to hold a private or executive session. This type of reporting generally covers significant issues. For example, it may include the internal audit team not being able to access requested data after repeated attempts, key IT individuals not providing complete or full disclosure, or IT leaders leaving the internal auditor out of key steering committee discussions (i.e., not having a seat at the table). Another challenging issue for a private session might be the lack of support by the CIO. This "tone at the top" may set the wrong culture and even block risk remediation or allow key IT controls to go unmonitored.

9. Conclusion

Assessing IT risks and controls represents — for both new and experienced CAEs — one of the first steps in gaining an understanding of the IT environment and its significance in business risk management. Reading and applying this GTAG provides guidance for CAEs and internal auditors to sufficiently understand IT risks and applicable controls. The CAE will then be able to guide IT risk and control discussions with key stakeholders.

The next step, assessing and understanding IT governance, permits the CAE to identify who is accountable for what in IT and how IT leadership, in cooperation with business leaders, deploys the IT strategy. In this context, CAEs should keep in mind that IIA Standard 2110.A2 calls for "assessing IT governance." Section 3 (Internal Stakeholders and IT Responsibilities) in this document provides a useful summary of key roles and responsibilities.

Once the CAE assesses IT governance, analyzing IT risks is a logical next step in the process. Unfortunately, there is no universal checklist for analyzing IT risks. Each organization — driven by the requirements of its nature and size of business — operates different technology infrastructure, applications, interfaces, and uses different policies to achieve IT strategy. The CAE should perform risk analysis by using a structured methodology, such as that outlined in ISO 31000 Risk Management Standardization, and leveraging knowledge from key IT leaders (e.g., the CIO and other executives) in the context of the overall enterprise risks. Developing solid and trusted relationships will allow for transparency when analyzing inherent and residual risks.

There are many models and approaches to analyzing IT risks, and the CAE should select the models that best fit his or her organization. Several key IT roles and functions are detailed in Section 6 (Understanding the Importance of IT Controls) in this document. The CAE rates the IT risk levels and determines what will be included in the overall audit plan.
The CAE must identify and assess what technical skills and competencies are required based on the overall audit plan. The CAE may consider The IIA's GAIT Methodology in using a top-down, risk-based approach. Some specializations, however, may not always be cost-effective to deploy on a full-time basis. CAEs can use internally developed technical skills, hired skills, or external providers. Co-sourcing provides an opportunity for organizations of all sizes to use outside expertise and gain perspective on the latest IT trends and risk impact.

Assessing the IT risks and controls requires a thoughtful and organized plan. CAEs should plan sufficient time and skilled resources to do a professional job and create a sustainable process for ongoing analysis.

10. Authors & Reviewers

Authors:

Steve Mar, CFSA, CISA
Rune Johannessen, CIA, CCSA, CISA
Stephen Coates, CIA, CGAP, CISA
Karine Wegrzynowicz, CIA
Thomas Andreesen, CISA, CRISC

Reviewers:

Steve Hunt, CIA
Steve Jameson, CIA, CCSA, CFSA, CRMA

Other Contributors:

Dragon Tai, CIA, CCSA

11. Appendix: IT Control Framework Checklist

CAEs can use this checklist to examine their IT control framework to ensure the organization has addressed all control elements. The checklist can help the CAE understand the issues and plan for full internal audit coverage of the control areas.

ACTIONS	QUESTIONS
1. Identify the IT control environment of the organization, including: a. Values. b. Philosophy. c. Management style. d. IT awareness. e. Organization. f. Policies. g. Standards.	• Do corporate policies and standards that describe the need for IT controls exist?
2. Identify relevant legislation and regulation impacting IT control, such as: a. Governance. b. Reporting. c. Data protection. d. Compliance.	• What legislation exists that impacts the need for IT controls? • Has management taken steps to ensure compliance with this legislation?
3. Identify the roles and responsibilities for IT control in relation to: a. Board of directors. i. Audit committee. ii. Risk committee. iii. Governance committee. iv. Finance committee. b. Management. i. CEO. ii. CFO and controller. iii. CIO. iv. Chief Security Officer (CSO). v. CISO. vi. CRO. c. Audit. i. Internal audit. ii. External audit.	• Have all relevant responsibilities for IT controls been allocated to individual roles? • Is the allocation of responsibilities compatible with the need to apply division of duties? • Are IT responsibilities documented? • Are IT control responsibilities communicated to the whole organization? • Do individuals clearly understand their responsibilities in relation to IT controls? • What evidence is there of individuals exercising their responsibilities? • Does internal audit employ sufficient IT audit specialists to address the IT control issues?

ACTIONS	QUESTIONS
4. Identify the risk assessment process. Does it address: a. Risk appetite? b. Risk tolerance? c. Risk analysis? d. Matching risks to IT controls?	• How is the organization's risk appetite and tolerance determined? • Is the organization's risk appetite and tolerance authorized at board level? • Are risk appetite and tolerance clearly understood by all those with a responsibility for IT control? • Does the organization use a formal risk analysis process? • Is the process understood by everyone responsible for IT control? • Is the process used consistently throughout the organization?
5. Identify all monitoring processes, including: a. Regulatory. b. Normal in-house. c. Other than internal auditing.	• What processes exist to monitor compliance with all relevant legislation plus internal policies and standards? • Does management carry out monitoring processes outside internal audit?
6. Identify information and communication mechanisms, such as: a. Control information. b. Control failures.	• What metrics are provided to the Board, its committees, and management in relation to IT security? • What additional reports are provided regularly to the Board and management? • Is management always provided with reports when IT control failures occur? • Do the Board and its committees receive similar reports of IT control failures?

About IPPF

The International Professional Practices Framework (IPPF) is the conceptual framework that organizes authoritative guidance promulgated by The Institute of Internal Auditors. IPPF guidance includes:

Mandatory Guidance

Conformance with the principles set forth in mandatory guidance is required and essential for the professional practice of internal auditing. Mandatory guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The three mandatory elements of the IPPF are the Definition of Internal Auditing, the Code of Ethics, and the *International Standards for the Professional Practice of Internal Auditing (Standards)*.

Element	Definition
Definition	The Definition of Internal Auditing states the fundamental purpose, nature, and scope of internal auditing.
Code of Ethics	The Code of Ethics states the principles and expectations governing behavior of individuals and organizations in the conduct of internal auditing. It describes the minimum requirements for conduct, and behavioral expectations rather than specific activities.
International Standards	*Standards* are principle-focused and provide a framework for performing and promoting internal auditing. The *Standards* are mandatory requirements consisting of: • Statements of basic requirements for the professional practice of internal auditing and for evaluating the effectiveness of its performance. The requirements are internationally applicable at organizational and individual levels. • Interpretations, which clarify terms or concepts within the statements. It is necessary to consider both the statements and their interpretations to understand and apply the *Standards* correctly. The *Standards* employ terms that have been given specific meanings that are included in the Glossary.

Strongly Recommended Guidance

Strongly recommended guidance is endorsed by The IIA through a formal approval processes. It describes practices for effective implementation of The IIA's Definition of Internal Auditing, Code of Ethics, and *Standards*. The three strongly recommended elements of the IPPF are Position Papers, Practice Advisories, and Practice Guides.

Element	Definition
Position Papers	Position Papers assist a wide range of interested parties, including those not in the internal audit profession, in understanding significant governance, risk, or control issues and delineating related roles and responsibilities of internal auditing.
Practice Advisories	Practice Advisories assist internal auditors in applying the Definition of Internal Auditing, the Code of Ethics, and the *Standards* and promoting good practices. Practice Advisories address internal auditing's approach, methodologies, and consideration, but not detail processes or procedures. They include practices relating to: international, country, or industry-specific issues; specific types of engagements; and legal or regulatory issues.
Practice Guides	Practice Guides provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables.

This GTAG is a Practice Guide under IPPF.

For other authoritative guidance materials, please visit www.theiia.org/guidance-standards.

TeamMate®

Building on Experience, Shaping the Future of Audit Technology

As the world's leading audit management software, TeamMate has revolutionized the audit industry, empowering audit departments of all sizes to do more with less. Introduced in 1994, TeamMate has a long standing commitment to advancing the audit profession. From consistently innovative product updates, to hosted solutions, and now mobile apps, we are dedicated to leveraging the latest technology for our clients. TeamMate's outreach extends beyond our customers to support and enrich the professional community through research projects, educational programs and initiatives such as our Open Audit Innovation Contest.

To learn about TeamMate, visit us on the web at CCHTeamMate.com or call 1.888.830.5559.

Don't take our word for it...
Check out what our customers are saying at
TeamMateSuccess.com

ARC Logics™
a Wolters Kluwer business

2119-ARC-TM-GTAG-AD 12/15/11

GTAG®

About the Institute

Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association with global headquarters in Altamonte Springs, Fla., USA. The IIA is the internal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, and principal educator.

About Practice Guides

Practice Guides provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables. Practice Guides are part of The IIA's IPPF. As part of the Strongly Recommended category of guidance, compliance is not mandatory, but it is strongly recommended, and the guidance is endorsed by The IIA through formal review and approval processes.

A Global Technologies Audit Guide (GTAG) is a type of Practice Guide that is written in straightforward business language to address a timely issue related to information technology management, control, or security.

For other authoritative guidance materials provided by The IIA, please visit our website at www.globaliia.org/standards-guidance.

Disclaimer

Copyright

The Institute of Internal Auditors

www.globaliia.org