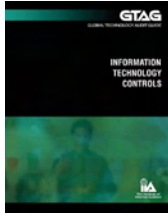


# Developing the IT Audit Plan

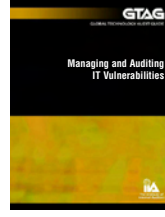


## Global Technology Audit Guide (GTAG)

Written in straightforward business language to address a timely issue related to IT management, control, and security, the GTAG series serves as a ready resource for chief audit executives on different technology-associated risks and recommended practices.



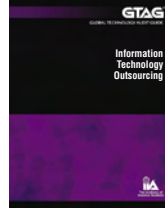
**Information Technology Controls:** Topics discussed include IT control concepts, the importance of IT controls, the organizational roles and responsibilities for ensuring effective IT controls, and risk analysis and monitoring techniques.



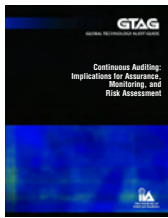
**Managing and Auditing IT Vulnerabilities:** Among other topics, discusses the vulnerability management life cycle, the scope of a vulnerability management audit, and metrics to measure vulnerability management practices.



**Change and Patch Management Controls:** Describes sources of change and their likely impact on business objectives, as well as how change and patch management controls help manage IT risks and costs and what works and doesn't work in practice.



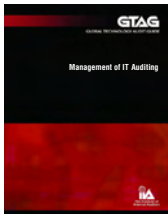
**Information Technology Outsourcing:** Discusses how to choose the right IT outsourcing vendor and key outsourcing control considerations from the client's and service provider's operation.



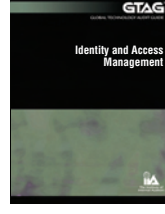
**Continuous Auditing:** Addresses the role of continuous auditing in today's internal audit environment; the relationship of continuous auditing, continuous monitoring, and continuous assurance; and the application and implementation of continuous auditing.



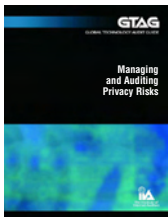
**Auditing Application Controls:** Addresses the concept of application control and its relationship with general controls, as well as how to scope a risk-based application control review.



**Management of IT Auditing:** Discusses IT-related risks and defines the IT audit universe, as well as how to execute and manage the IT audit process.



**Identity and Access Management:** Covers key concepts surrounding identity and access management (IAM), risks associated with IAM process, detailed guidance on how to audit IAM processes, and a sample checklist for auditors.



**Managing and Auditing Privacy Risks:** Discusses global privacy principles and frameworks, privacy risk models and controls, the role of internal auditors, top 10 privacy questions to ask during the course of the audit, and more.



**Business Continuity Management:** Defines business continuity management (BCM), discusses business risk, and includes a detailed discussion of BCM program requirements.

# **Developing the IT Audit Plan**

## **Authors**

Kirk Rehage, Chevron Corporation

Steve Hunt, Crowe Chizek and Company LLC

Fernando Nikitin, Inter-American Development Bank

July 2008

Copyright © 2008 by The Institute of Internal Auditors, 247 Maitland Avenue, Altamonte Springs, Fla., 32701-4201. All rights reserved. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means — electronic, mechanical, photocopying, recording, or otherwise — without prior written permission from the publisher.

The IIA publishes this document for informational and educational purposes. This document is intended to provide information, but is not a substitute for legal or accounting advice. The IIA does not provide such advice and makes no warranty as to any legal or accounting results through its publication of this document. When legal or accounting issues arise, professional assistance should be sought and retained.

## Table of Contents

1.	EXECUTIVE SUMMARY .....	1
2.	INTRODUCTION.....	2
2.1	IT Audit Plan Development Process.....	3
3.	UNDERSTANDING THE BUSINESS.....	4
3.1	Organizational Uniqueness .....	4
3.2	Operating Environment.....	4
3.3	IT Environment Factors .....	4
4.	DEFINING THE IT AUDIT UNIVERSE.....	9
4.1	Examining the Business Model.....	9
4.2	Role of Supporting Technologies .....	9
4.3	Annual Business Plans.....	9
4.4	Centralized and Decentralized IT Functions.....	9
4.5	IT Support Processes.....	10
4.6	Regulatory Compliance .....	10
4.7	Define Audit Subject Areas.....	10
4.8	Business Applications .....	11
4.9	Assessing Risk .....	11
5.	PERFORMING A RISK ASSESSMENT .....	12
5.1	Risk Assessment Process.....	12
5.1.1	Identify and Understand Business Objectives.....	12
5.1.2	Identify and Understand IT Strategy .....	12
5.1.3	IT Universe .....	12
5.2	Ranking Risk.....	13
5.3	Leading IT Governance Frameworks .....	14
6.	FORMALIZING THE IT AUDIT PLAN .....	16
6.1	Audit Plan Context .....	16
6.2	Stakeholder Requests.....	17
6.3	Audit Frequency .....	17
6.4	Audit Plan Principles.....	18
6.5	The IT Audit Plan Content .....	18
6.6	Integration of the IT Audit Plan.....	19
6.7	Validating the Audit Plan .....	19
6.8	The Dynamic Nature of the IT Audit Plan.....	20
6.9	Communicating, Gaining Executive Support, and Obtaining Plan Approval.....	21
7.	APPENDIX: HYPOTHETICAL COMPANY EXAMPLE .....	22
7.1	The Company .....	22
7.2	The IT Audit Plan .....	22
8.	GLOSSARY OF TERMS .....	27
9.	GLOSSARY OF ACRONYMS .....	28
10.	ABOUT THE AUTHORS.....	29

### 1. Executive Summary

As technology becomes more integral to the organization's operations and activities, a major challenge for internal auditors is how to best approach a companywide assessment of IT risks and controls within the scope of their overall assurance and consulting services. Therefore, auditors need to understand the organization's IT environment; the applications and computer operations that are part of the IT infrastructure; how IT applications and operations are managed; and how IT applications and operations link back to the organization.

Completing an inventory of IT infrastructure components will provide auditors with information regarding the infrastructure's vulnerabilities. "The complete inventory of the organization's IT hardware, software, network, and data components forms the foundation for assessing the vulnerabilities within the IT infrastructures that may impact internal controls."<sup>1</sup> For example, business systems and networks connected to the Internet are exposed to threats that do not exist for self-contained systems and networks.<sup>2</sup> Once an adequate understanding of the IT environment has been achieved, the chief audit executive (CAE) and the internal audit team can perform the risk assessment and develop the audit plan.

Many organizational factors are considered when developing the audit plan, such as the organization's industry sector, revenue size, type, complexity of business processes, and geographic locations of operations. Two factors having a direct impact on the risk assessment and in determining what is audited within the IT environment are its components and role. For example:

- What technologies are used to perform daily business functions?
- Is the IT environment relatively simple or complex?
- Is the IT environment centralized or decentralized?
- To what degree are business applications customized?
- Are some or all IT maintenance activities outsourced?
- To what degree does the IT environment change every year?

These IT factors are some of the components CAEs and internal auditors need to understand to adequately assess risks relative to the organization and the creation of the annual audit plan.

In addition to factors impacting the risk assessment, it is important for CAEs and internal auditors to use an approach that ascertains the impact and likelihood of risk occurrence; links back to the business; and defines the high-, medium-,

and low-risk areas through quantitative and qualitative analyses.

IT is in a perpetual state of innovation and change. Unfortunately, IT changes may hinder the IT auditor's efforts to identify and understand the impact of risks. To help IT auditors, CAEs can:

- Perform independent IT risk assessments every year to identify the new technologies that are impacting the organization.
- Become familiar with the IT department's yearly short-term plans and analyze how plan initiatives impact the IT risk assessment.
- Begin each IT audit by reviewing its risk assessment component.
- Be flexible with the IT audit universe — monitor the organization's IT-related risk profile and adopt audit procedures as it evolves.<sup>3</sup>

Several IT governance frameworks exist that can help CAEs and internal audit teams develop the most appropriate risk assessment approach for their organization. These frameworks can help auditors identify where risks reside in the environment and provide guidance on how to manage risks. Some of the most common IT governance frameworks include COBIT, the UK's Office of Government Commerce IT Infrastructure Library (ITIL), and the International Organization for Standardization's (ISO's) 27000 Standard series.

Mapping business processes, inventorying and understanding the IT environment, and performing a companywide risk assessment will enable CAEs and internal auditors to determine what needs to be audited and how often. This GTAG provides information that can help CAEs and internal audit teams identify audit areas in the IT environment that are part of the IT audit universe.

Due to the high degree of organizational reliance on IT, it is crucial that CAEs and internal auditors understand how to create the IT audit plan, the frequency of audits, and the breadth and depth of each audit. To this end, this GTAG can help CAEs and internal auditors:

1. Understand the organization and the level of IT support received.
2. Define and understand the IT environment.
3. Identify the role of risk assessment in determining the IT audit universe.
4. Formalize the annual IT audit plan.

Finally, this GTAG provides an example of a hypothetical organization to show CAEs and internal auditors how to execute the steps necessary to define the IT audit universe.

<sup>1</sup> GTAG: *Information Technology Controls*, p. 15.

<sup>2</sup> GTAG: *Information Technology Controls*, p. 15.

<sup>3</sup> GTAG: *Management of IT Auditing*, pp. 6 and 7.

## 2. Introduction

One of the main responsibilities and more difficult tasks of CAEs is to create the organization’s audit plan. As The Institute of Internal Auditors’ (IIA’s) Standard 2010: Planning explains, CAEs should establish risk-based plans on at least an annual basis to determine the priorities of the internal audit activity, which, in turn, should be consistent with the organization’s goals and strategies. Furthermore, CAEs should consider consulting engagements based on their potential to add value and improve the organization’s operations and risk management activities. These activities have been documented by The IIA Research Foundation’s Common Body of Knowledge 2006 study, which found that nearly all CAEs interviewed plan their audit activities at least annually, including 36.4 percent who update their audit plan multiple times per year. (Figure 1)

To develop a risk-based audit plan, CAEs should first perform a companywide risk assessment. The proper execution of an appropriate IT risk assessment — that is part of the overall risk assessment — is a vital component of companywide risk management practices and a critical element for developing an effective audit plan. “For many organizations, information and the technology that supports it represent the organization’s most valuable assets. Moreover, in today’s competitive and rapidly changing business environment,

management has heightened expectations regarding IT delivery functions: Management requires increased quality, functionality and ease of use; decreased delivery time; and continuously improving service levels while demanding that this be accomplished at lower costs.”<sup>4</sup>

Regardless of the methodology or frequency of audit planning activities, the CAE and the internal audit team should first gain an understanding of the organization’s IT environment before performing the audit. The use of technology is an essential part of an organization’s activities. From the collection, processing, and reporting of accounting information to the manufacturing, sales, and distribution of products, virtually every business activity relies on the use of technology to some extent. The use of technology also has evolved to where it is not only supporting a business process but, in many cases, it is integral to controlling the process. As a result, internal controls in processes and activities are becoming more technology-based, while deficiencies and lack of integrity in supporting technologies are impacting the organization’s operations and business objectives significantly.

However, the development of an effective, risk-based IT audit plan has been a difficult task for internal auditors, especially when auditors do not have sufficient background in IT.

<sup>4</sup> IT Governance Institute’s Control Objectives for Information and Related Technology (COBIT), Third Edition, p. 5.

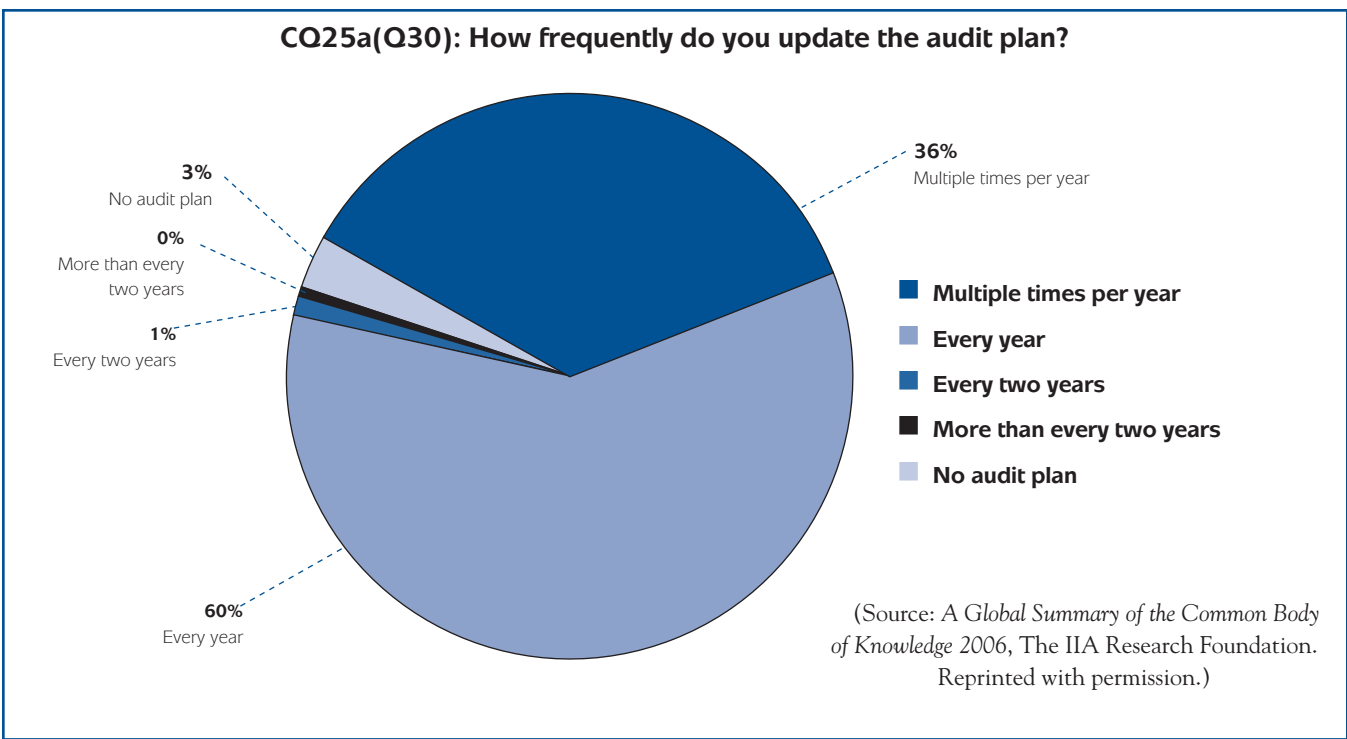


Figure 1. Frequency of audit plan updates



Results from several IIA external quality assessment reviews (QARs) reveal that developing an appropriate IT audit plan is one of the weakest links in internal audit activities. Many times, instead of doing risk-based auditing, internal auditors review what they know or outsource to other companies, letting them decide what to audit.

This guide offers techniques in how to address this challenge — how to determine what should be included in the IT audit scope and how these audit areas could be organized into manageable audit units — to create an effective IT audit plan for the organization.

## 2.1 IT Audit Plan Development Process

Defining the annual audit plan should follow a systematic process to ensure all fundamental business aspects and IT-service support activities are understood and considered. Therefore, it is essential that the foundation for the plan be rooted in the organization's objectives, strategies, and business model. Figure 2 depicts a logical work-flow progression using a top-down approach to define the IT audit plan that will be used in this guide.

The first step in defining the annual IT audit plan is to understand the business. As part of this step, auditors need to identify the strategies, company objectives, and business models that will enable them to understand the organization's unique business risks. The audit team also must understand how existing business operations and IT service functions support the organization.

Next, auditors need to define the IT universe. This can be done through a top-down approach that identifies key business objectives and processes, significant applications that support the business processes, the infrastructure needed for the business applications, the organization's service support model for IT, and the role of common supporting technologies such as network devices. By using these technical components, along with an understanding of service support processes and system implementation projects, auditors will be able to create a comprehensive inventory of the IT environment. This inventory, in turn, forms the foundation for assessing the vulnerabilities that may impact internal controls.

After auditors have a clear picture of the organization's IT environment, the third step is to perform the risk assessment — a methodology for determining the likelihood of an event that could hinder the organization from attaining its business goals and objectives in an effective, efficient, and controlled manner.

The information and analysis gained by understanding the organization, inventorying the IT environment, and assessing risks feeds into the final step, formalizing the audit plan. The objective of the audit plan is to determine where to focus the auditor's assurance and consulting work to provide management with objective information to manage the organization's risks and control environment.

The remainder of this guide follows these four steps and discusses how to define an effective IT audit plan.

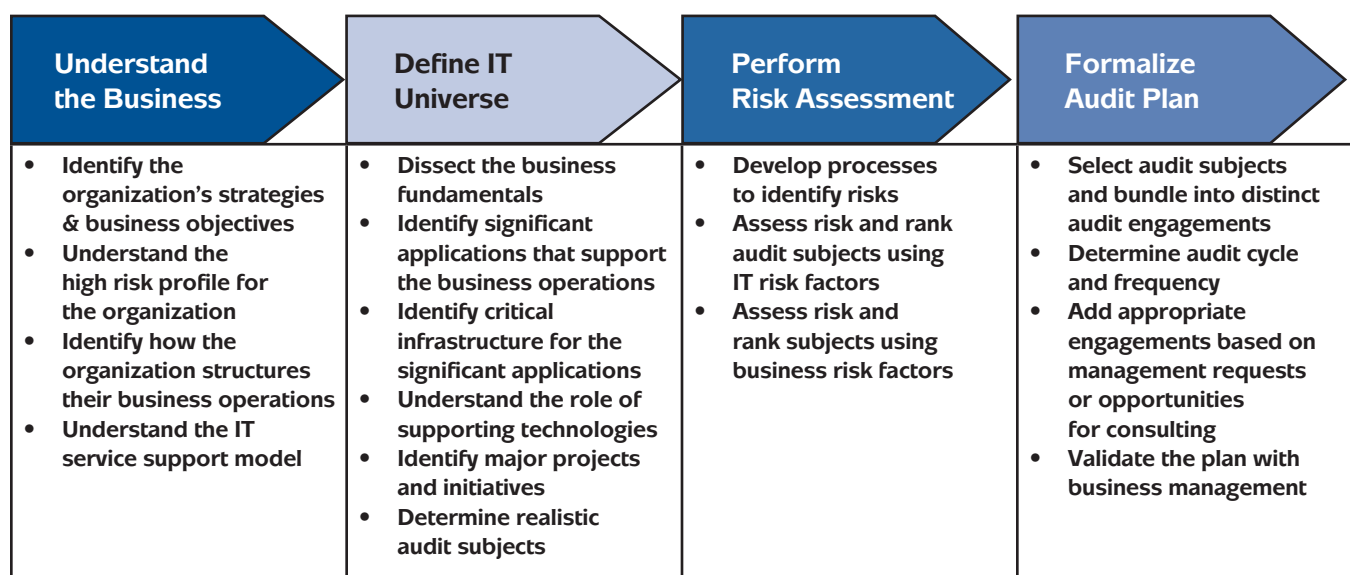


Figure 2. The IT audit plan process

### 3. Understanding the Business

Getting started with the right perspective is paramount to defining an effective IT audit plan. An appropriate perspective to keep in mind is that technology only exists to support and further the organization's objectives and is a risk to the organization if its failure results in the inability to achieve a business objective. Hence, it is important to first understand the organization's objectives, strategies, business model, and the role that technology has in supporting the business. This can be done by identifying the risks found in the technologies used and how each risk might prevent the organization from achieving a business objective. Doing so will result in more meaningful and useful assessments for management.

Furthermore, auditors need to become familiar with the organization's business model. Because each organization has a distinct mission and set of business goals and objectives, business models help auditors to identify the products or services the organization provides, as well as its market base, supply channels, manufacturing and product generation processes, and delivery mechanisms. Having a fundamental knowledge of this information will help auditors understand unique business risks and how technology supports existing business models and mitigates the organization's overall risk profile.

#### 3.1 Organizational Uniqueness

Every organization is different. Even companies operating in the same industry will have different business models, objectives, organizational structures, IT environments, and delivery models. Therefore, audit plans should be defined uniquely for each organization. In addition, the importance of technology might differ within industry segments. Consider the companies that assemble and sell personal computers. Besides using a variety of business models, these companies rely on technology differently to meet business objectives. For instance, the traditional sale distribution model of channeling products through physical stores and resellers require the use of technology to manage operation and accounting activities, while technology reliance is much greater for companies that sell products over the Internet. As a result, the online marketer's revenue stream depends more on the availability of critical IT functionality, which also increases the level of IT risks. As this example illustrates, the way an organization deploys its technology resources and systems creates a unique set of business risks.

#### 3.2 Operating Environment

To become familiar with the organization, auditors first need to understand its objectives and how business processes are structured to achieve objectives (refer to figure 3).

Auditors can use different internal resources to identify and understand the organization's goals and objectives, including:

- Mission, vision, and value statements.
- Strategic plans.
- Annual business plans.
- Management performance scorecards.
- Stockholder annual reports and supplements.
- Regulatory filings, such as those submitted to the U.S. Securities and Exchange Commission (SEC).

After becoming familiar with the organization's entity-level strategic objectives, the next step is to identify the key processes that are critical to the objectives' success. When doing so, auditors need to understand how each business process differs within operating units, support functions, and major organizationwide projects, as well as how the process relates and links to entity objectives.

Project processes are unique, but equally important, in ensuring initiatives that add value to the organization are managed and commercialized appropriately. A process is considered key if its failure prevents the organization from fully achieving the strategic objective to which it is tied. Operating units include core processes through which the organization achieves primary objectives, such as manufacturing, sales, and distribution activities. Support functions include management processes that oversee and support core operational functions, such as governance and compliance activities, finance, human resources, treasury, cash management, and procurement activities.

Once processes are identified, auditors need to outline the significant applications and critical IT infrastructure (e.g., databases, operating systems, networks, and physical environments) supporting these applications. Underlying these applications and IT infrastructure are supporting IT processes, such as systems development life cycles, change management, operations, and security activities. Auditors should note that applications require periodic assessments based on their significance to financial reporting activities, regulatory compliance, or operational requirements.

Examining the operating environment this way (i.e., starting from the top of the organization) will help auditors understand and inventory each critical component. To fully understand the operating environment and its risks also requires a comprehensive understanding of different technology factors that influence and help categorize organizational risks.

#### 3.3 IT Environment Factors

Different factors and analysis techniques should be considered to understand the operational environment and its unique risks. This is because an organization's control environment complexity will have a direct effect on its overall



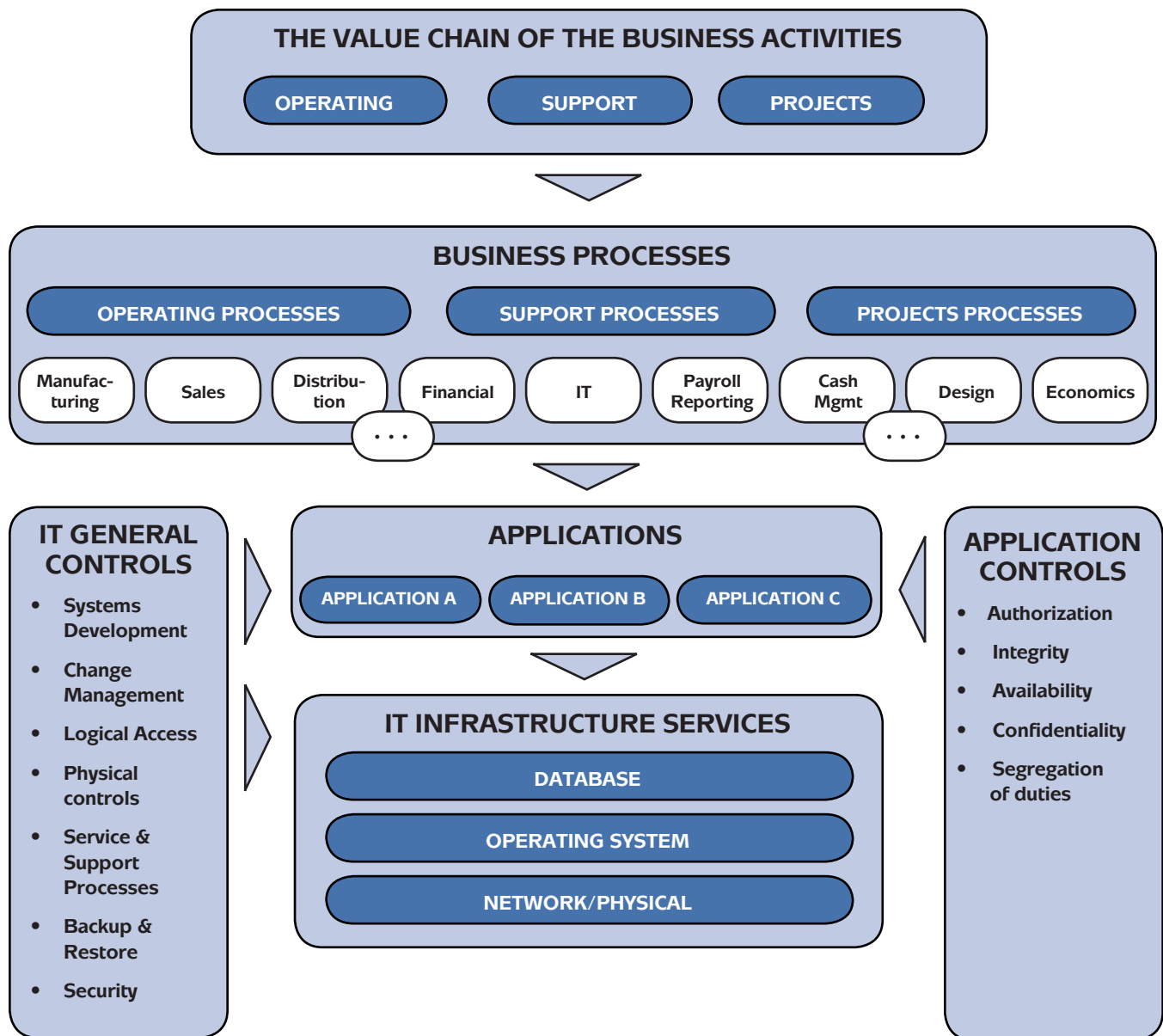


Figure 3. Understanding the IT environment in a business context

Figure adapted and revised from: *IT Control Objectives for Sarbanes-Oxley*, 2nd Ed., used by permission of the IT Governance Institute (ITGI). ©2006 ITGI. All rights reserved.

risk profile and system of internal control. Important factors to consider include:

1. **The degree of system and geographic centralization (i.e., distribution of IT resources).** The organization's business model may determine the IT function's structure and delivery model. For instance, companies operating with decentralized business units that have the autonomy to make operating decisions may have decentralized IT operations, more diversity of applications, and a larger variety of deployed products. On the other hand, in more centralized companies auditors might find enterprise-based applications and centralized IT infrastructure support. Because risks vary as companies approach either end of the centralization continuum, audit responses should vary accordingly.

When establishing the IT audit universe, consideration should be given to aligning individual audits with the management function that has accountability for that area. A centralized IT delivery model may allow for fewer, but possibly larger, individual audits that are concentrated on core technologies and enterprise applications. Conversely, a decentralized delivery model *could* require more audit engagements to achieve a proper alignment with management accountability.

2. **The technologies deployed.** The organization's system architecture diversity will determine the breadth of technical knowledge required within the internal audit function and the number of areas that need to be reviewed. Diversity could be in any and all levels of the *IT stack* — the key components of an application's technical infrastructure, including its program code, database, operating system, and network infrastructure.

For instance, *application program code* includes the sets of computer programs, control files, tables, and user interfaces that provide functionality for specific business operations such as accounting, payroll, and procurement. Other applications could manage critical business information, such as engineering and design project data, legal, and personal medical information. The organization also may have applications that control manufacturing processes commonly called process control systems.

On the other hand, *database systems* enable the storage, modification, and extraction of data (e.g., Oracle, Microsoft SQL Server, and DB2), while *operating systems* perform a computer's basic tasks, such as handling operator input; managing internal computer memory; and providing disk drive, display, and peripheral device functions. Examples of operating systems include variations of Windows and UNIX installed in computers and servers. Handheld devices such as personal digital assistants and cell phones also require operating systems.

Finally, *networks* link computers and enable them to communicate with each other. They consist of physical components, such as switches, routers, firewalls, wiring, and programs that control the routing of data packets. Networks also can be deployed using radio frequency technology, commonly called wireless networks.

All four layers of the stack are essential to enabling automated business functionality and introduce availability, integrity, and confidentiality risks. The degree of risk is based on the criticality of the business activity the technology supports and enables, and on the technology's configuration and deployment. Therefore, the more variety in each of these layers, the higher the organization's risk profile. For instance, it is simpler for IT departments to manage a homogeneous environment of Windows 2003 servers running a SQL Server database for a single enterprise resource planning (ERP) application than a variety of operating systems and database platforms underlying different applications. While ideal, the first scenario might not be practical for a large organization with diverse operations or a decentralized business model. In creating the audit universe, critical IT elements should be identified and assessed as part of the top-down analysis techniques described in this guide.

3. **The degree of customization.** Generally, customized implementations add complexity to the management of IT assets. Off-the-shelf software relies primarily on the support of vendors who have a high degree of knowledge and expertise on their products. When vendor software — whether applications, operating systems, or other supporting software — is modified to fit an organization's business need or process, a large amount of ownership is assumed and more risk is introduced into the equation. Generally, organizations should perform a cost-benefit analysis when making the decision to customize third-party software. However, control aspects might not be considered fully in this analysis. In addition, audits of customized implementations also require greater technical knowledge on the part of the auditors.
4. **The degree of formalized company policies and standards (i.e., IT governance).** The purpose of an IT governance program is to enable the organization to better manage its day-to-day IT activities and risks through the use of policies and standards. For example, organizations with formalized policies and standards that guide management oversight and help to establish the IT control environment have a better chance of implementing an effective IT governance program. These programs, in turn, are effective when policies and standards are communicated, understood, monitored, enforced, and updated by management.

*Policies* are general, long-term statements of principle that address management's operational goals; are intended to have a long-term effect in guiding the development of business rules for specific situations; and can be interpreted and supported by standards, controls, and guidelines. In terms of IT, policies can provide high-level management directives in areas such as intellectual property rights, data protection, retention, and privacy to ensure compliance with laws and regulations and the effective safeguard of data assets.

On the other hand, *standards* describe a mandatory business process or procedure and provide further direction on how to comply with the policy statement to which they are linked. IT standards are generally technology-neutral and can be further defined by technology-specific controls and guidelines (i.e., configuration settings or procedures) that define how the standard should be implemented.

As a general rule, organizations should establish an ongoing maintenance process for all policies and standards that addresses the latest regulatory mandates. For example, recent changes to the U.S. Federal Rules of Civil Procedure governing the production of evidence in court cases address the discovery and production of electronically stored information. Because of these changes, an organization's level of risk partly depends on its adherence to updated record retention policies and standards that consider the management of electronically stored information.

Different IT governance frameworks and methodologies are available, including COBIT, ISO's 27002 Standard on information security management, the Canadian Institute of Chartered Accountants' IT Control Guidelines, and the Information Security Forum's Standard of Good Practice for Information Security. These frameworks provide a structured way of categorizing control objectives and control areas across the entire control environment. (For additional information on these and other compliance frameworks, auditors can refer to The IIA's *Information Technology Controls* GTAG.<sup>5</sup>) Organizations can adopt one of these frameworks or use them as a reference when developing their own. Section 5.3 provides information on leading IT governance best practices to help organizations assess the content and effectiveness of these frameworks.

5. **The degree of regulation and compliance.** Organizations in highly regulated industries generally will have a high-risk profile due to the potential consequences of noncompliance with regulatory mandates. However, successful organizations in highly regulated industries also have disciplined control environments and effective

management oversight to ensure ongoing compliance, which results in a lower residual risk profile. The organization's regulatory requirements, therefore, should be appropriately considered in the risk profile and IT audit universe. For example, all organizations registered with the SEC are required by the U.S. Sarbanes-Oxley Act of 2002 to report on the effectiveness of their internal controls over financial reporting. The legislation also created the U.S. Public Company Accounting Oversight Board (PCAOB) to guide public accounting firms on how to conduct an audit of internal controls over financial reporting. Other regulations include the Basel II Accord in the finance sector and a growing number of privacy and data protection laws and regulations, such as the European Union's Directive on Data Protection, U.S. Gramm-Leach-Bliley (GLBA) Act, the U.S. Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS).

6. **The degree and method of outsourcing.** IT outsourcing is becoming more prevalent in many organizations due to the high cost and expertise required to deliver noncore services. (The IIA's *Information Technology Outsourcing* GTAG provides a detailed discussion on the types of IT outsourcing arrangements and their degree of risk.<sup>6</sup>) In terms of outsourcing, it is important for auditors to consider the different risks stemming from the outsourcing arrangement when drafting the IT audit plan. Key factors include how management views its oversight and monitoring role, the maturity of the arrangement (e.g., transitioning versus an established working process), country-specific risks, and the completeness of the vendor's and organization's business continuity plans.
7. **The degree of operational standardization.** Operational processes and procedures include the entire system development life cycle as well as configuration, change, incident, operations, and security management activities. Similar to the degree of centralization and the diversity of deployed technologies, the level of operational standardization can impact the reliability and integrity of the IT infrastructure and its assets. Consequently, organizations that adopt standardized processes throughout their service delivery functions increase their ability to operate as a high-performing organization.

An example of a standardized practice is ITIL, a set of concepts and techniques for managing IT infrastructures, as well as the development and installation of new computer systems and IT operations. Its books on service support and service delivery are the most widely used and understood ITIL publications. One of the primary

<sup>5</sup> GTAG: *Information Technology Controls*, p. 18.

<sup>6</sup> GTAG: *Information Technology Outsourcing*.

benefits of ITIL is that it establishes a common vocabulary of defined and widely used terms. Organizations that implement ITIL concepts have claimed a higher degree of reliability and lower delivery costs.

8. **The level of reliance on technology.** Some organizations are intensive technology users or use technology to differentiate themselves from their peers and competitors. While technology can improve overall internal controls with the use of automated application controls, strong governance and internal operational processes become more important as reliance on IT increases. In addition, as organizations depend more on the availability and integrity of IT functionality to enable business operations and meet their objectives, the significance of IT risks in the organization's overall risk profile increases. Hence, the nature and extent to which the organization relies on technology should be evident in the risk assessment used to develop the IT audit plan.

These eight IT environment factors, along with the top-down approach used to understand the organization's operations and IT infrastructure, provide auditors with the information needed to move to the next step of the audit planning process — defining the IT audit universe and performing a risk assessment.

### 4. Defining the IT Audit Universe

Determining what to audit is one of the most important internal audit activities, as performing the annual IT audit plan will have a profound impact on the overall success of the internal audit department. Consequently, the ultimate goal of the IT audit plan is to provide adequate coverage on the areas that have the greatest risk and where internal auditors can add the most value to the organization.

One of the first steps to an effective IT audit plan is to define the *IT universe*, a finite and all-encompassing collection of audit areas, organizational entities, and locations identifying business functions that could be audited to provide adequate assurance on the organization's risk management level. At this initial phase, identifying potential audit areas within the IT universe is done independently from the risk assessment process. Auditors need to be aware of what audits could be performed before they can assess and rank risks to create the annual audit plan. Defining the IT audit universe requires in-depth knowledge of the organization's objectives, business model, and the IT service support model.

#### 4.1 Examining the Business Model

Organizations can have different operational units and support functions to accomplish its objectives, which, in turn, have business processes that link activities to achieve their goals. Referring back to the example of companies that assemble and sell personal computers, a traditional company in this industry sector consists of several assembly plants located in different countries, sales, and marketing units, as well as different corporate management and support functions. The sales and marketing units, for instance, have established processes for accepting, fulfilling, and invoicing customer orders, while other operating units and support functions have their own processes. Underlying these processes will be critical IT applications and supporting infrastructure. Therefore, it is important for auditors to understand the company's IT environment when defining the IT universe and identifying the processes critical to the success of each unit.

Using a top-down approach to understand the organization's structure and activities can help auditors identify critical IT functionality processes that sustain the organization's operating units and support functions. However, variation in how similar business units perform their processes can add complexity to this analysis. For instance, manufacturing plants in different locations might use different procurement processes. In decentralized organizations, business units might use different applications for similar business processes, or a common application might be configured differently to the extent it functions like an entirely different application. For example, one business unit uses SAP R/3 on a UNIX and Oracle platform, while another business unit uses SAP R/3 on a Windows and SQL Server platform. Although similar,

the IT support structure for these business processes is different and may require separate assurance reviews.

#### 4.2 Role of Supporting Technologies

Identifying supporting IT infrastructure technologies can be a simple process when detecting business activities that rely on key applications. However, it is much harder to associate the use of supporting technologies, such as the company's network, e-mail application, and encryption software, to business objectives and risk. Yet, these supporting technologies exist because the business requires them, and a failure in these services and products can hinder the organization's ability to accomplish its mission. Therefore, key supporting technologies, while not directly associated with an application or business process, must be identified and represented in the universe of auditable areas.

#### 4.3 Annual Business Plans

Another important element is to take into consideration the organization's annual business plans and strategies. Operating plans can provide auditors with information on important changes and projects that may be pursued in the upcoming year, which might require audit involvement and become subjects in the IT audit universe. Projects might be directly IT-related, such as the implementation of a new ERP system, or business projects that manage major engineering or construction initiatives. For example, energy companies form major capital projects when developing new facilities to bring oil and gas discoveries into production. These business projects can benefit from the use of critical IT components that merit IT audit attention, such as access controls over document management systems and external network connections for partners and contractors. Because companies can be partners on one project and competitors on another, it is important to limit their access to required IT resources only.

#### 4.4 Centralized and Decentralized IT Functions

Auditors need to identify centrally managed IT functions that support the entire or a large portion of the organization. Centralized functions are good candidates for individual audits in the IT audit universe and include network design and security administration, server administration, database management, service or help desk activities, and mainframe operations. For example, the organization may have a server administration group that is responsible for all Windows servers. Because this group might use common configurations and administrative processes across the entire server population, it represents an ideal candidate for an individual IT audit that is part of the IT audit universe. The homogeneous nature of the environment also lends itself to sampling for the audit's execution.



There are several benefits to identifying centralized audit subjects. The main benefit is the effective use of limited IT audit resources, which can enable the audit team to focus on one area, use sampling techniques, and gain a large amount of coverage in a single audit. Another benefit is the transfer of internal audit efficiencies to other audits because centralized areas have already been covered and may be excluded from the scope of other audits. The benefit of referencing centralized audit coverage is particularly applicable to application auditing. For example, there could be hundreds of applications residing within a Windows server administration group environment. Since the general controls for the infrastructure are reviewed in a more centralized audit, the IT audit should be limited to application-specific technical areas rather than the entire infrastructure platform hosting the application. The organization also benefits as it is audited thoroughly only once and is not impacted when applications are reviewed individually during each business process audit.

Furthermore, organizations may centralize their IT functions differently. A common practice of many organizations is to create a single network support function that manages its network design and security administration. This network support function could be divided into firewall, router, and switch configuration activities, as well as Internet connectivity, wireless, digital voice, and external network connection management. As a result, each of these areas may be an independent audit subject in the IT universe. Furthermore, because centralized IT functions can change over time, they should be reviewed and refreshed in the audit universe at least annually.

A similar approach can be taken for decentralized IT functions, where each physical location might represent a separate audit subject. Depending on the location's size, the site's audit may review general and technical controls for each infrastructure stack layer. The review should only include the IT controls for which the local site is responsible, while controls handled by centralized IT functions should be excluded. If the site is large and supports a wide number of technologies, auditors might need to perform multiple reviews for that location as part of the IT audit universe.

### 4.5 IT Support Processes

Even if the organization has a decentralized IT function, it may have standardized support processes. Organizations that are striving to be high-performing organizations understand the importance of having standardized support processes across their operating units regardless of the business model. Examples of standardized support processes include service desk activities as well as change, configuration, release, incident, and problem management procedures. The service desk is generally the first point of contact for customers to register an IT service or issue resolution request, thus initiating the request's life cycle management process and triggering a

chain of events including incident, problem, change, and release management activities.

Again, one of the leading sources for IT service best practices is ITIL. Many organizations are implementing ITIL practices or other standardized processes to attain better efficiency and higher performance in managing their IT functions. Internal audit groups should become involved in efforts to implement standardized support processes where appropriate and consider new ways to provide assurance on their effectiveness. One approach could be to review the deployment and governance of standardized processes at the enterprise level within the audit plan. These top-level reviews could assess the effectiveness of the processes themselves, the effectiveness of deployed processes, and the effectiveness of the governance model to ensure standardized support processes are used as intended. Once standardized processes are audited, site audits should concentrate on how they are followed rather than on their effectiveness.

### 4.6 Regulatory Compliance

Different laws and regulations around the world are mandating the use of internal controls and risk management practices and the privacy of personally identifiable information, including the Sarbanes-Oxley Act and Basel II Accord. As discussed earlier, some of these regulations mandate the protection of customer information in the credit card industry (e.g., GLBA and the PCI DSS) and the safeguarding of personal medical information (e.g., HIPAA). Although most of these regulations do not address IT controls directly, they imply the need for an adequately controlled IT environment. Therefore, these regulatory areas are potential subjects in the IT audit universe, as auditors need to determine whether the organization has rigorous processes in place and whether they are operating effectively to ensure compliance.

### 4.7 Define Audit Subject Areas

The way the IT environment is divided into individual audit subjects could be somewhat influenced by personal preference or staffing considerations. However, the ultimate goal is to figure out how to divide the environment in a manner that provides the most efficient and effective audits. The preceding discussions on centralized IT functions and standardized support processes stated how audit subjects can be grouped in the audit universe to define an audit approach that is more efficient. Although auditors should not be assessing business risks at this phase of the audit planning process, the goal is to have an audit plan that focuses on the highest-risk areas where auditors can add the most value.

Although there is no single right way to define IT audit subjects, there are incorrect or inappropriate ways to do this.<sup>7</sup>

---

<sup>7</sup> GTAG: *Management of IT Auditing*, p. 10.



Pitfalls include improper sizing of subjects, basing a plan solely on staffing capabilities, and creating a focus imbalance.

In addition, audit subjects should be divided into appropriately sized areas to define a reasonable allocation of audit resources. When doing so, auditors should keep in mind that defining small or large audit subject areas might hinder audit efforts. This is because a certain amount of overhead is required for each audit engagement, including administrative efforts for audit planning, management reviews, sign-offs of completed work, and reporting and communicating results. If the audit universe and plan contains numerous small audits, for example, internal auditors could spend as much time administrating the audits as performing them. Conversely, if the audit subject area is defined broadly, audits could run for an extended period of time, be disruptive to the client, or be reviewed insufficiently. Depending on the organization's culture, overly broad definitions might even result in an unplanned increase in scope (i.e., scope creep).<sup>8</sup>

Finding the right audit size depends on the organization's audit practices and culture. As a general rule for most organizations, defining audit subjects that require two to three technical auditors for a three- to four-week duration is a reasonable target, as this provides different auditor perspectives and experiences. In addition, the three- to four-week duration is a reasonable request for most organizations.

The audit size also should be consistent with company-accepted historical audit practices. However, the IT audit universe should not be defined solely on audit staffing capability, as this might result in a focus imbalance. For instance, some IT audit functions do not have any technicians or IT professionals, but consist of business auditors who have knowledge of currently used business applications. Because these auditors tend to focus on the application layer and might ignore the underpinning infrastructure layers, it's important to have a well-balanced coverage of all layers as part of the audit.

Ideally, the internal audit function should consist of highly technical personnel and general auditors who have a good understanding of application controls. The technical auditors, for example, would help ensure the IT infrastructure has proper security controls in place and review general application controls. The proper balance of audit subjects covering all environment layers should be the cornerstone of the IT audit plan even if the IT audit constraint is an issue. If that is the case, alternative resource staffing for these audits would be required to supplement the expertise of the internal audit staff.

Auditors should consider that the audit technique used during the security review could be ineffective when used in a nonhomogeneous server environment consisting of multiple server platforms. This is because the general server administration subject area might be too large or unmanageable.

For this reason, many organizations review security based on their platform type, thus enabling a more detailed review. Unfortunately, this activity could result in redundancy as audit steps are duplicated. Hence, auditors could establish separate audit areas for each platform type and a general controls subject audit that is performed across all platforms.

A key consideration in identifying IT environment components and in grouping distinct audit subjects is management accountability. A worst-case scenario would be to define audit subjects crossing reporting lines and involving management from different reporting units, as this might create a conflict over who eventually owns the resolution of issues presented in the audit. As a result, it should be clear who will receive the audit report and who is responsible for the remediation of identified control deficiencies. Finally, the scope of each audit subject should be described clearly so that organizational accountability is determined properly.

### 4.8 Business Applications

CAEs need to determine which audit group will be responsible for the planning and oversight of business application audits. Depending on how the audit function operates, business applications can be included as part of the IT audit universe, business audit universe, or both. There is a growing consensus among internal audit functions that business applications should be audited with the business processes they support. This provides assurance over the entire suite of controls — automated and manual — for the processes under review, helps to minimize gaps and overlaps of audit efforts, and minimizes confusion over what was included in the scope of the engagement.

Because of their expertise, the business audit function is probably best suited to determine when applications should be reviewed. If business applications are maintained as part of the IT audit universe, the business audit universe should be linked to the IT audit universe to work together during the audit. Even if business applications are maintained separately from the IT audit universe, individual audit subjects can be created within the IT audit universe for large-scale applications that are used by multiple functions for multiple processes, such as ERP systems. This is because it might make sense to review the application's general controls in a stand-alone audit rather than arbitrarily including this area in one of the many business audits.

### 4.9 Assessing Risk

After the IT universe is defined, a systematic and uniform assessment of risk across all subjects should be the next step in determining the annual audit plan. The next section presents risk and risk assessment fundamentals that can help CAEs and internal auditors create an effective IT audit plan.

<sup>8</sup> GTAG: *Management of IT Auditing*, p. 10.

### 5. Performing a Risk Assessment

The IIA defines *risk* as the possibility that an event will occur that could affect the achievement of objectives, which is measured in terms of impact and likelihood.<sup>9</sup> Therefore, it is vitally important for organizations to determine the contents of their risk portfolio periodically and perform activities to manage risks to an acceptable level. As discussed earlier, the risk assessment process should not be conducted until the CAE and internal audit team understand the contents of the IT universe and how they link back to or support the organization. It is paramount — no matter the risk assessment model or approach used — for the risk assessment to determine IT environment areas that can significantly hinder the organization's achievement of objectives. In other words, the risk assessment needs to examine the infrastructure, applications, and computer operations or components that pose the greatest threat to the organization's ability to ensure system and data availability, reliability, integrity, and confidentiality.

In addition, auditors need to identify the effectiveness and usefulness of risk assessment results, which should be directly predicated on the methodology employed and its proper execution. That is, if the risk assessment's methodology input (i.e., the IT universe and its link to the business audit universe) is deficient or is applied incorrectly, it is likely that the output (i.e., risk assessment results) will be incomplete in some capacity.

#### 5.1 Risk Assessment Process

After the CAE and internal audit team understand the organization and its use of technology, they can conduct the risk assessment. Performing this task correctly is paramount to ensuring relevant IT risks (i.e., those with the greatest likelihood of occurrence and impact to the organization) are identified and evaluated effectively and adequate mitigation measures take place. The culmination of the risk assessment process is then used by the CAE and audit team to develop the IT audit plan.

##### 5.1.1 Identify and Understand Business Objectives

One of the foundational elements of any risk assessment methodology is gaining an understanding of the organization's business objectives and determining how IT is used to assist or support the achievement of these objectives. If business objectives are not identified, auditors need to perform this activity before performing the IT risk assessment. Business objectives may be broad and strategic in nature (e.g., become the industry leader) or more linear and tactical

in nature (e.g., replace legacy IT applications with an ERP solution).

Furthermore, according to IIA Practice Advisory 2110-1: Assessing the Adequacy of Risk Management Processes, risk management processes should have five key objectives:

- Risks arising from business strategies and activities need to be identified and prioritized.
- Management and the board need to determine the level of risk acceptable to the organization, including the acceptance of risks designed to accomplish the organization's strategic plans.
- Risk mitigation activities need to be designed and implemented to reduce or otherwise manage risk at levels that are acceptable to management and the board.
- Ongoing monitoring activities need to be conducted to reassess risk periodically and the effectiveness of controls to manage risk.
- The board and management need to receive periodic risk management process reports. The organization's corporate governance processes also should provide periodic communication of risks, risk strategies, and controls to stakeholders.

Additional guidance from IIA Practice Advisory 2010-2, Linking the Audit Plan to Risk and Exposures, defines how organizational risk, strategic planning, and changes in management direction should be reflected in the audit plan.

##### 5.1.2 Identify and Understand IT Strategy

Once CAEs and internal auditors become familiar with the organization's objectives, they need to identify the company's overall IT strategy to understand how it aligns with the objectives identified in the prior step. Because the organization could have different forms of documentation showing the relationship between its business objectives and the IT strategic plan, CAEs and internal auditors need to obtain, read, and understand these documents. Generally speaking, the IT strategic plan should link back to organizational objectives and provide clear direction as to how it links back to these objectives. In other words, the IT plan should identify tactical actions to be performed by the IT department within a defined period of time, which are designed to support the achievement of the organization's objectives.

##### 5.1.3 IT Universe

As discussed earlier, auditors first need to inventory the key computing environment components to determine which IT areas need to be reviewed from a risk and controls perspective. While there isn't a single-best approach to perform the inventory, many organizations divide their IT universe

<sup>9</sup> *International Standards for the Professional Practice of Internal Auditing*, p. 17.

into three major sub-categories: infrastructure, computer operations, and applications.

The infrastructure area consists of all computing components that support the flow and processing of information, such as servers, routers, bridges, mainframes, communication lines, printers, datacenters, networking equipment, antivirus software, and desktops. Computer operations, on the other hand, consist of the processes and controls that manage the computing environment. Examples include physical and logical security administration, backup and recovery, business continuity and disaster recovery planning, service-level agreements (SLAs), program change controls, and compliance with laws and regulations. Finally, applications consist of the software used by the organization to process, store, and report business transactions. Examples include ERP systems and stand-alone applications, such as Microsoft Excel or Access.

## 5.2 Ranking Risk

Once an inventory of the IT universe is completed, the next step is to assign a risk rating to all sub-categories — infrastructure, computer operations, and applications. These sub-categories need to be ranked based on the impact their risks will have on the organization and their likelihood of occurrence. In other words, auditors need to determine what could go wrong in each area and how the organization will be affected if controls to manage or mitigate risk are not designed and operating effectively.

In addition, auditors need to keep in mind that each risk might not be equally significant or weighed the same way across the IT audit universe. (Weight differentiates the relative importance of a risk over the others). For example, if an area has a direct tie to the accuracy of financial reporting, it would carry a higher weight relative to an area that does not directly affect the accuracy of financial reporting. According to The Research Foundation's *Assessing Risk*, there are three approaches to measuring risk and impact:<sup>10</sup>

1. **Direct probability estimates and expected loss functions or the application of probabilities to asset values to determine exposure for loss.** This process is the oldest and not considered a best practice. The insurance industry still uses this method, but internal auditing does not.
2. **Risk factors or the use of observable or measurable factors to measure a specific risk or class of risks.** This process is favored for macro-risk assessments, but is not efficient or particularly effective for micro-risk assessments, except when auditable units are homogeneous throughout the audit universe as in branch, location, or plant audits.

3. **Weighted or sorted matrices or the use of threats versus component matrices to evaluate consequences and controls.** This method is superior for most micro-risk assessments.

This GTAG will focus exclusively on the weighted or sorted matrices approach to measure risk and impact. As shown in table 1, this approach uses a simplistic method to rate risk that is based on the risk's high (i.e., three), medium (i.e., two), or low (i.e., one) likelihood of occurrence.

Likelihood Scale		
H	3	High probability that the risk will occur.
M	2	Medium probability that the risk will occur.
L	1	Low probability that the risk will occur.

Table 1. Risk likelihood scale

While the likelihood of risk occurrence is relatively simple to determine, determining the impact of risk occurrence is another matter entirely. This is because there can be several different qualitative and quantitative aspects of risk impact. Furthermore, not every qualitative and quantitative aspect is treated equally (i.e., some risks are more important than others). According to *Assessing Risk*, three types of risk factors are commonly in use — subjective risk factors, objective or historical risk factors, and calculated risk factors.

1. **Subjective risk factors.** Measuring risk and its impact requires a combination of expertise, skills, imagination, and creativity. This emphasis on subjective measurements is borne out in practice — many auditable units change so much between audits that prior audit history is of little use. Therefore, an experienced practitioner's sound subjective judgment is just as valid as any other method.
2. **Objective or historical risk factors.** Measuring risk factor trends can be useful in organizations with stable operations. In all cases, current objective information is helpful in measuring risk.
3. **Calculated risk factors.** A subset of objective risk factor data is the class of factors calculated from historical or objective information. These are often the weakest of all factors to use because they are derivative factors of risk that is further upstream.<sup>10</sup>

<sup>10</sup> The IIA Research Foundation's *Assessing Risk*, 2<sup>nd</sup> Edition, 2004.

Due to these risk factors, CAEs and internal auditors must design and use a risk impact model that fits their organization. The model should be similar to the one used for the enterprisewide risk assessment. However, the model's scale and rank methodology needs to be changed for each IT risk. As shown in table 2, and for the purposes of this GTAG, a simplistic ranking method that uses high, medium, and low categories is used for the impact of each component that is based on the same likelihood concepts presented in table 1.

Impact Scale (Financial)		
H	3	The potential for material impact on the organization's earnings, assets, reputation, or stakeholders is high.
M	2	The potential for material impact on the organization's earnings, assets, reputation, or stakeholders may be significant to the audit unit, but moderate in terms of the total organization.
L	1	The potential impact on the organization is minor in size or limited in scope.

**Table 2.** Risk impact model scale

Table 3 on page 15 shows an example of a completed risk assessment that is based on the scales used for likelihood and impact across the risk categories of financial impact, quality of internal controls, changes in the audit unit, availability, integrity, and confidentiality. The score for each area is calculated by multiplying risk's likelihood and impact values across each category. For example, on the risk category for ERP application and general controls, the sum of the likelihood and impact values is 42. The same logic is used across the other risk categories for each possible audit area.

Based on this scoring approach, the lowest possible score is six and the highest possible score is 54. Table 4 shows the scoring ranges and their corresponding audit or review frequencies based on the organization's resource availability.

Level	Composite Risk Score Range	Recommended Annual Cycle
H	35–54	Every 1 to 2 years
M	20–34	Every 2 to 3 years
L	6–19	Every 3 to 5 years

**Table 4.** Scoring ranges and corresponding audit or review frequencies

### 5.3 Leading IT Governance Frameworks

Up to this point, the guide has focused on the steps necessary to define the IT audit universe and to perform a risk assessment that determines what should be audited and how often. This discussion is not based on any particular IT governance framework, such as COBIT, the ISO 27002 Standard, or ITIL. As a result, it is the CAE's responsibility to determine the components of these and other frameworks that best serve the organization.

It is important to keep in mind that none of these frameworks is a "one-size-fits-all." Rather, they are frameworks organizations can use to manage and improve their IT functions. While it is not within the scope of this GTAG to provide guidance on the pros and cons of these and other IT governance models, an overview of COBIT will be provided.

Since its release in 1996, COBIT has been a leading IT governance framework. Its mission is "to research, develop, publicize, and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors."<sup>11</sup> As a framework and supporting tool set, COBIT allows organizations to bridge the gap with respect to control requirements, technical issues, and business risks, and communicate that level of control to stakeholders. COBIT also enables the development of clear IT control policies and practices.<sup>12</sup>

In addition, COBIT provides a set of tools CAEs and internal auditors can use to help guide the IT risk assessment process. Some of its tools are a set of clearly stated control objectives, ideas on how to test controls, and a scale for ranking the maturity of the IT control environment. The COBIT framework consists of four domains with a total of 34 IT processes: plan and organize (PO), acquire and implement (AI), deliver and support (DS), and monitor and evaluate (ME).

As with any best practice control framework, auditors should proceed with caution when using this framework. CAEs and internal auditors must understand and apply the framework's concepts and guidance in their proper context. In other words, COBIT has been developed and refined over the last decade with the assistance of practitioners, academia, and different industries from around the globe. As a result, COBIT tends to have the look and feel of a framework that might work beautifully in a large organization with a sizable IT function, but may be equally challenging to work with in mid-size and small organizations.

Furthermore, the CAE and internal audit team must realize that simply because the IT function does not follow or adhere to the COBIT framework, this does not mean the IT function, its processes, or data is not controlled or managed

<sup>11</sup> COBIT 3<sup>rd</sup> Edition, p. 1.

<sup>12</sup> COBIT 4.1, p. 8.

## GTAG — Performing a Risk Assessment

properly. At a minimum, CAEs and internal auditors can use COBIT as a helpful guide during the IT risk assessment and audit process. In a best case scenario, the CAE and internal audit team should integrate the use of COBIT under the umbrella of risk and control-related frameworks and guidance, as well as to help the IT function with implementing part or all of the framework.

Area	Financial Impact		IT Risks										Score and Level	
			Quality of Internal Controls		Changes in Audit Unit		Availability		Integrity		Confiden-tiality			
	L	I	L	I	L	I	L	I	L	I	L	I		
ERP Application & General Controls	3	3	2	3	3	3	2	3	2	3	2	3	42	H
Treasury EFT Systems	3	3	3	3	3	3	2	2	3	2	2	2	41	H
HR/Payroll Application	3	3	3	2	3	3	2	2	2	3	2	3	40	H
Employee Benefits Apps (Outsourced)	2	3	2	2	3	3	3	2	2	3	3	3	40	H
IT Infrastructure	2	2	3	2	3	3	3	3	3	2	2	2	38	H
Process Control Systems	1	1	2	2	2	2	2	2	1	1	1	1	15	L
Database Administration and Security	2	2	2	2	2	2	3	3	2	2	2	1	27	M
UNIX Administration and Security	2	2	2	3	2	2	3	1	1	1	3	2	24	M
Corp. Privacy Compliance	2	2	3	2	3	3	2	1	2	2	3	3	34	M
Windows Server Admin and Security	2	2	1	2	2	2	2	3	3	2	2	2	26	M
Environment Reporting Systems	2	2	3	2	2	2	2	3	1	1	3	1	24	M
SOX Sustainability Review	2	2	2	2	2	2	1	1	2	2	1	2	19	L
Network Administration and Security	2	2	1	1	1	2	2	1	2	2	2	2	17	L
ITIL Deployment Practices	1	1	1	3	2	1	3	1	1	3	3	3	21	M
IT Governance Practices	1	1	2	2	1	1	3	1	1	1	1	2	12	L
Remote Connectivity	1	1	1	2	2	1	1	1	1	2	2	2	12	L
Application Program Change Control	2	3	1	3	1	1	1	1	1	3	1	2	16	L
Lowest possible score			6											
Highest possible score			54											
Mid point			30											
L = Likelihood I = Impact														

Table 3. Example of an IT risk-ranking score model



## 6. Formalizing the IT Audit Plan

Defining the IT audit universe and performing a risk assessment are precursor steps to selecting what to include in the IT audit plan. While everything in the IT audit universe could be reviewed on a recurring basis if the availability of resources is unlimited, this is not the reality for most internal audit functions. Consequently, CAEs must create an IT audit plan within the constraints of the audit function's operating budget and available resources.

### 6.1 Audit Plan Context

Figure 4 depicts the differences and challenges of moving from the risk assessment step to identifying the audits that will be included as part of the audit plan. In theory, each of these steps should be a separate and distinct effort because the objectives and focus are different. In the risk assessment, the objective is to understand risks in a relative context. Therefore, the major focus or driver of this effort is risk, while a major influencer may be resources. In defining the audit plan, the objective is to review high-risk areas through the allocation of available resources. As such, the driver is the resources and the influencer is the risks.

For most companies, these two steps are merged to some extent, as depicted in the overlap area of the two spheres representing each process in figure 4. For example, certain risks or auditable areas may be excluded from the risk assessment based on the level of resources that may be required to execute the audit. However, it is important to perform these steps in an objective manner considering each step's stated objective and driver forces.

In addition, the IT audit plan should be created as part of the internal audit function's strategic planning process. This planning process should be cyclical and can be understood under the classical management cycle of "plan, do, check, and act." Thus, while the plan is the key enabler to implement the process, it delineates how to reach audit objectives and goals. As a result, it should include a list of audit activities as well as the timing, dependencies, and resource allocation needed to reach audit goals.

Certain IIA standards describe the nature of internal audit services and provide quality criteria against which the performance of these services can be measured. More specifically, the 2000 series, Performance Standards for Managing the Internal Audit Activity, are relevant to the audit planning process:

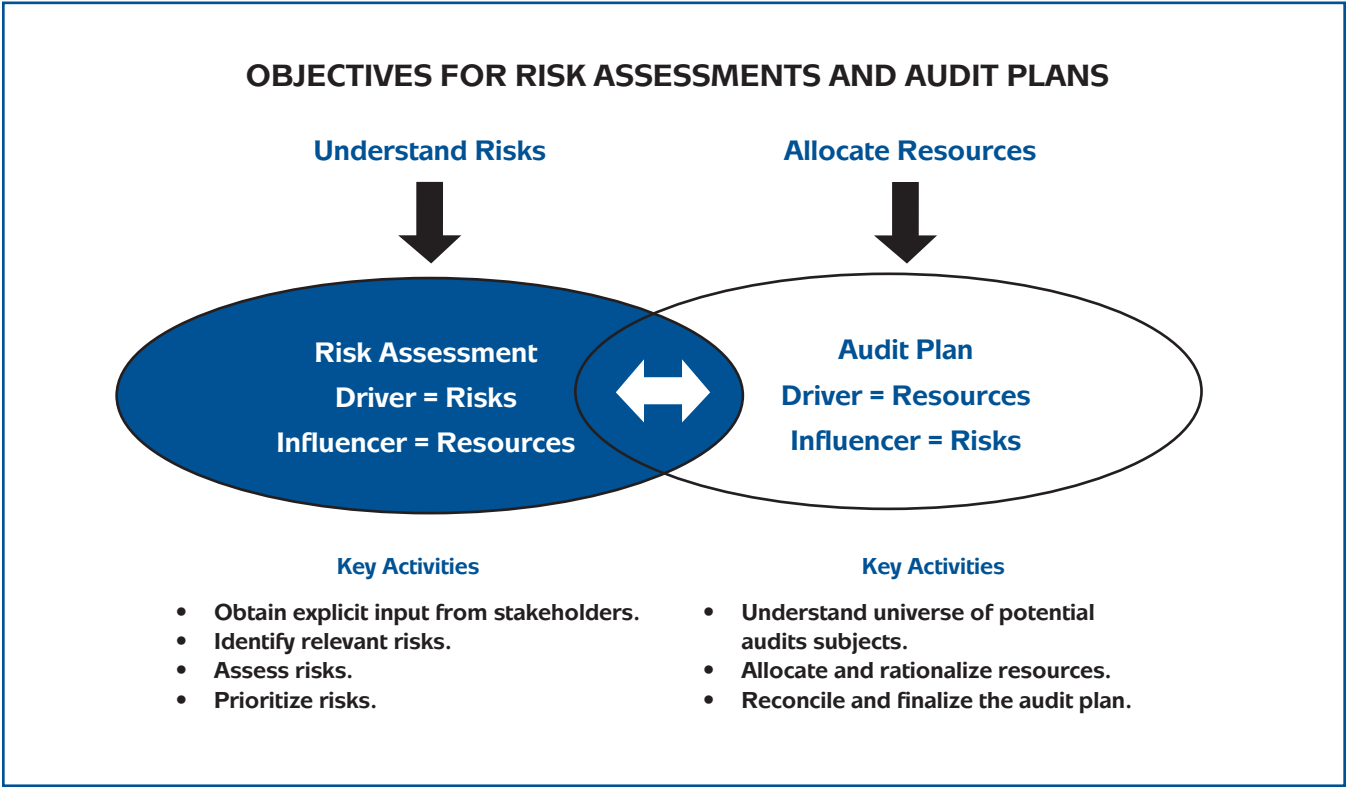


Figure 4. Objectives for risk assessment and audit plan (Source: Ernst & Young 2007)



- **IIA Standard 2010: Planning.** The CAE should establish risk-based plans to determine the priorities of internal audit activities consistent with the organization's goals.
- **IIA Standard 2020: Communication and Approval.** The CAE should communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and board for review and approval. The CAE also should communicate the impact of resource limitations.
- **IIA Standard 2030: Resource Management.** The CAE should ensure that internal audit resources are appropriate, sufficient, and deployed effectively to achieve the approved plan.

## 6.2 Stakeholder Requests

Internal auditors should have ongoing discussions throughout the IT audit plan's development with key stakeholders to better understand the business and risks the organization faces. Through these discussions, insights on the business will be gathered along with concerns key stakeholders might have. This is also an opportunity to learn about special audit assurance and consulting services requests, referred to in this document as stakeholder requests.

Stakeholder requests may come from the board of directors, audit committee, senior managers, and operating managers. They should be considered during the audit planning phase based on the engagement's potential to improve the overall management of risks and the organization's control environment. These requests may be specific enough to determine the required resource allocation, or the allocation may be based on previous audit work. These engagements also can include fraud investigations that come up throughout the year and requests to review service providers. (The IIA Standard 2010.C1 provides information on consulting engagements.) CAEs, therefore, should consider accepting proposed consulting engagements based on their potential to improve risk management activities and add value to and improve the organization's operations. Accepted engagements should be included in the IT audit plan.

## 6.3 Audit Frequency

Depending on the risk assessment's results, not all audit areas can nor should be reviewed in every audit cycle. As presented in section 5, audit frequency is based on an evaluation of the likelihood and impact of risk occurrence in relationship to the organization's objectives. Since audits occur on a cyclical basis, multiyear audit plans are developed and presented to management and the audit committee for review and approval. The multiyear plan, usually three to five years in terms of its timeframe, is created to document

what audits will be performed and when, ensure adequate audit coverage is provided over this period of time, and identify audits that may require specialized external resources or additional internal resources. In addition, most organizations create a one-year plan, as a derivative of the multiyear plan that outlines planned audit activities for the upcoming year.

Auditors can use one of two strategies to arrive at the ideal frequency of planned audit activities:<sup>13</sup>

- The audit frequency is established in an initial risk assessment to take place every three to five years and is proportional to the risk level.
- The audit plan is based on a continuous risk assessment without a predefined audit frequency. Some organizations use this approach, which is especially appropriate within the context of the IT audit plan, given the higher rate of IT change as compared to changes in non-IT activities.

Table 5 shows criteria that can be used to determine frequency and resource allocation based on the results of the risk assessment. This process should be understood as a cyclical, repetitive, and iterative sequence of activities, integrating a top-down approach through at least three layers:

- Layer 1: The audit universe where all the inputs are integrated.
- Layer 2: The individual business processes where engagements should be identified and preliminarily planned.
- Layer 3: The audit engagements where fine-tuning and plan optimization can be conducted.

	Priority	Frequency	Resource Allocation
H	Immediate action, usually within the first year	Annual reviews or multiple actions within the cycle	High allocation
M	Mid-term action within the audit cycle	One or several audit engagements within the cycle; could be postponed	Base allocation
L	Audit engagements usually not planned within the cycle	At most one audit engagement planned within the cycle	Limited allocation

**Table 5.** Frequency and resource allocation of audit activities

<sup>13</sup> Brink's *Modern Internal Auditing*, 6th Ed, 2005, p. 292.

# GTAG — Formalizing the IT Audit Plan

In addition to frequency, other factors should be considered when defining the audit plan:

- **Internal audit sourcing strategies.** Different sourcing or staff augmentation strategies are common practices in the industry, including hiring internal staff, outsourcing, and co-sourcing, which should be considered during the annual planning process.
- **Estimated available IT audit resources.** This consists of a technical skills inventory of current staff that is mapped to IT audit plan needs. The availability of resources usually is established on an annual basis and is based on the number of full-time equivalent auditors and skills required. Available audit days are the net of possible audit days minus nonaudit activities and exception time, such as training, vacation, and holidays.
- **Board and management requests included in the plan and related to control assurance or consulting services.**
- **The organization's regulatory and compliance requirements.** These should be included in the audit universe and risk assessment.
- **External audits that should be synchronized with the audit plan.** The IIA Performance Standard 2050 establishes that the CAE should share information and coordinate activities with other internal and external providers of relevant assurance and consulting services to ensure proper coverage and minimize duplication of efforts.
- **Internal initiatives and efforts to improve the audit function.** Any effort beyond audit engagements that represents an investment of effort should be planned, budgeted, and reflected in the audit plan. Examples include quality assurance reviews, integrated risk assessments, audit committee reporting tasks, and audit recommendation follow-ups.
- **A contingency IT audit budget and plan for reasonable coverage of unplanned situations.**

## 6.4 Audit Plan Principles

Internal auditors should consider The IIA's Practice Advisory 2010-1: Planning for the IT Audit Plan when identifying audit plan principles:

1. Planning should be consistent with the charter of the internal audit function and involve establishing goals, schedules, staffing, budgeting, and reporting.
2. Internal audit activities should be capable of accomplishing the goals within a specific time and budget and be measured in terms of, at least, targeted dates and levels of accomplishment.
3. The plan should include the work schedule with activities to be performed and their key planned dates, as

well as estimated efforts in terms of their timeframe for completion and resources.

4. The plan should be prioritized based on:
  - a. Dates and results of the last audit engagement.
  - b. Updated assessments of risks and effectiveness of risk management and control processes.
  - c. Requests by the board and senior management.
  - d. Current issues relating to organizational governance.
  - e. Major changes in the business, operations, programs, systems, and controls.
  - f. Opportunities to achieve operating benefits.
  - g. Changes to and capabilities of the audit staff. (Work schedules should be sufficiently flexible to cover unanticipated demands on the internal audit activity.)

## 6.5 The IT Audit Plan Content

The content of the IT audit plan should be a direct reflection of the risk assessment described in previous sections. The plan also should have different types of IT audits, for example:

- Integrated business process audits.
- Audits of IT processes (e.g., IT governance and strategy audits, as well as audits of the organization's project management efforts, software development activities, policies and procedures, COBIT/ISO/ITIL processes, and information security, incident management, change management, patch management, and help desk activities).
- Business projects and IT initiative audits, including software development life cycle (SDLC) reviews.
- Application control reviews.
- Technical infrastructure audits (e.g., demand management reviews, performance reviews, database assessments, operating systems audits, and operation analyses).
- Network reviews (e.g., network architecture reviews, penetration testing, vulnerabilities assessments, and performance reviews).

To verify each audit provides appropriate coverage, auditors can incorporate the following elements as part of the audit:

- IT general controls, application controls, and infrastructure controls.
- Contributions to operational reviews, financial reviews, and compliance reviews.
- Main control objectives (i.e., segregation of duties, concentration of duties, and security, among others).
- New IT trends and their threats, innovations, and impact.
- All IT layers of the stack.

## 6.6 Integration of the IT Audit Plan

One key aspect of the planning process is to determine the integration level of the IT audit plan with non-IT audit activities in the audit department. As explained in section 4.7, auditors need to determine which audit group will be responsible for the planning and oversight of business application audits. This discussion could be extended to include all IT components. For instance, will the IT audit plan be presented and executed on a stand-alone basis or will IT audit subjects be integrated with business areas? Answers to these questions should be based on the internal audit department's function as well as its staff, size, geographical distribution, and management approach. A range of integration scenarios could be considered from a low integration scenario where the IT audit function is well-defined and established within the internal audit department (i.e., with their own IT audit universe and scope) to a fully integrated audit approach where all IT components are understood under each business segment.

Table 6 illustrates scenarios based on different options to integrate the IT audit plan. These scenarios are:

- **A low-integrated plan.** This is a stand-alone IT audit plan under the responsibility of the IT audit team. A low-integrated plan is organized by IT subject areas, is generally isolated from non-IT audit activities, and includes the review of applications. Non-IT audit activities generally do not include any of the IT components within their scope.
- **A partially integrated audit plan, which outlines IT audit engagements that are established by a core IT audit team.** These plans provide an additional set of planned engagements, generally referred to as application reviews, which are distributed across other non-IT audit teams and coordinated with other business process reviews.

- **A highly integrated audit plan, where IT audit activities are incorporated as part of business process engagements.** Often, IT audit activities are planned under the responsibility of a multidisciplinary team that has a balanced skill set, including IT audit expertise.

Given that a system of internal control typically includes manual and automated controls, with more reliance on application controls, the ability to scope an audit that covers all controls is essential in providing a holistic assessment of the control environment. A complete business audit, including a review of all IT components, provides the opportunity to evaluate whether there is an appropriate combination of controls to mitigate business risks.

## 6.7 Validating the Audit Plan

Unfortunately, there is no direct test that can be performed to validate whether the right and most effective audit plan exists. Therefore, auditors need to establish criteria to evaluate the plan's effectiveness in meeting its objectives. As discussed earlier, the plan should consist of risk-based audits, mandated audit areas, and management requests for assurance and consulting services. Because one of the objectives of the planning phase is to allocate resources to areas where the department can add the most value to the organization and highest risk IT areas, auditors should determine how the plan reflects this objective.

The chart in figure 5 depicts the plan's target. According to this chart, if all audit subjects and engagements are plotted based on their risk likelihood and impact, audits should be reflected in all chart quadrants. The bolded box represents the ideal selection of audits and engagements, so

Audit Universe	Low-integrated Audit Plan	Partially Integrated Audit Plan	Highly Integrated Audit Plan
Business Processes <ul style="list-style-type: none"> <li>Operational</li> <li>Financial</li> <li>Compliance</li> </ul>	Non-IT audit	Non-IT audit	Integrated approach
Applications Systems <ul style="list-style-type: none"> <li>Application controls</li> <li>IT general controls</li> </ul>	IT audit	Integrated approach	Integrated approach
IT Infrastructure Controls <ul style="list-style-type: none"> <li>Databases</li> <li>Operating systems</li> <li>Network</li> </ul>	IT audit	IT audit	Integrated approach

Table 6. IT auditing and integrated auditing

# GTAG — Formalizing the IT Audit Plan

that the largest majority of the plan consists of audits from the highest-risk quadrant with the balance proportionally selected from medium- and low-risk quadrants. Furthermore, some of the audits in the plan should deal with compliance and mandated areas. Consequently, auditors should note that while there are valid reasons for including low-risk audits in the plan, alternative audit approaches such as control self-assessments should be considered to limit the resources required to complete the review.

## 6.8 The Dynamic Nature of the IT Audit Plan

As technology continues to change, so does the arrival of new and potential risks, vulnerabilities, and threats to the company. In addition, technological changes may prompt a new set of IT goals and objectives, which in turn leads to the creation of new IT initiatives, acquisitions, or changes to meet the organization's needs. An important point to consider when drafting the audit plan, therefore, is the organization's dynamic nature and its ongoing changes. More specifically, auditors need to consider the higher rate of IT change compared to changes in non-IT activities, the appropriate timing of a system's SDLC phases, and the results of SDLC audits.

In addition, auditors need to consider the specific source of the change. For instance, frequent changes in the IT audit plan could be the result of:

- Changes in strategic, organizational, or human resources.
- New business process initiatives involving the use of high-risk technology, such as e-commerce.
- Major changes in applications, such as the use of a new Web application version.
- Critical administration and support software packages.
- Network and infrastructure threats and vulnerabilities that lead to a reassessment of information security management activities.

As a consequence, periodic reassessments of IT audit plan priorities should be conducted and, if needed, reported to the board and senior management on a more frequent basis as compared with other more traditional and static audit topics. The IT audit function also must analyze changes in the IT audit universe and have the flexibility to adjust the plan to the new conditions. Furthermore, the plan should be reassessed periodically, and greater flexibility is needed to react to changes in the business and IT environments by adjusting the ranking and prioritization of planned audits. Finally, it is

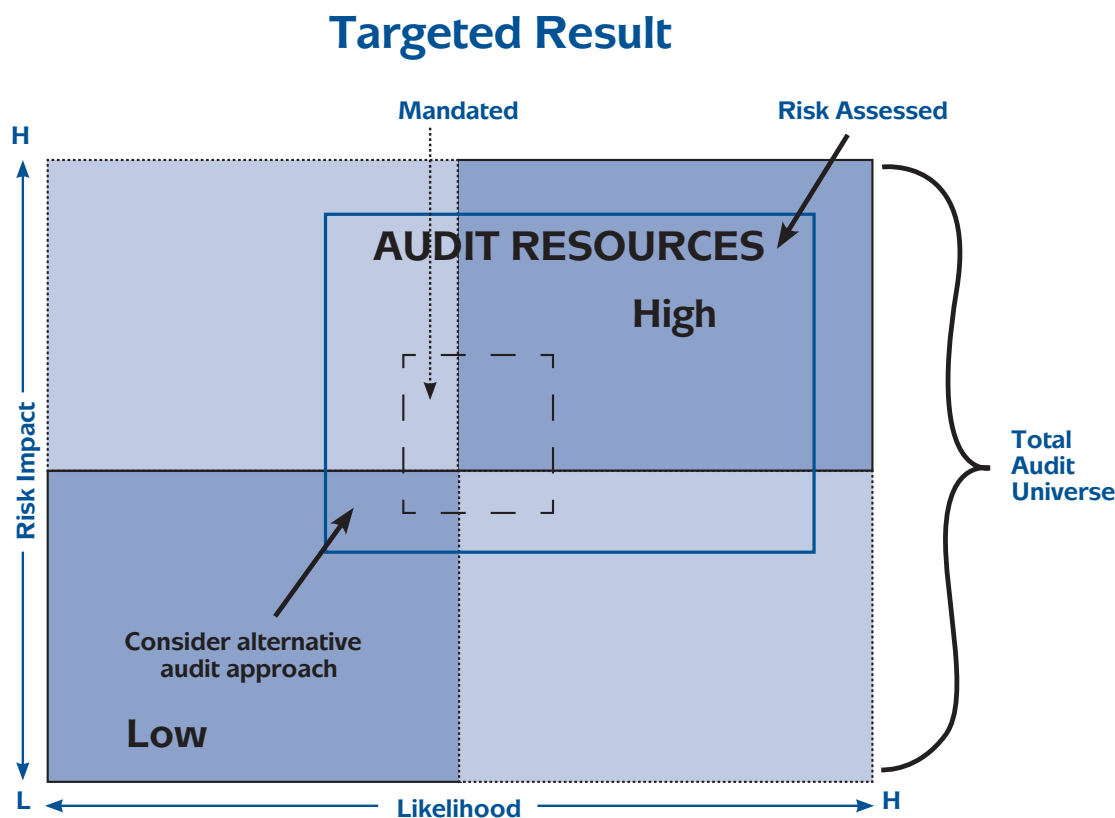


Figure 5. Chart of targeted audit results

important for the plan to link each element of the IT audit universe to one of the following SDLC phases: feasibility study, analysis, design, implementation, testing, evaluation, and maintenance and production.

The value added provided by an internal audit function depends highly on the quality of its recommendations and the benefit that the company obtains from their implementation. Often there are direct benefits from addressing monetary compliance issues. However, there may be an indirect benefit to help enhance the organization's reputation, competitive advantage, maturity of business processes, and innovation.

One of the main attributes of audit recommendations that affect their value added is timing. This attribute is especially relevant during the entire life cycle of IT applications. In general, the earlier in the software's life cycle a weakness or risk is identified, the higher the added value of audit recommendations. For example, the cost of implementing a structural change to address a critical application weakness is substantially greater once the system is in production compared to addressing the same weakness at the design phase.

Besides the added value stemming from audit recommendations, the internal auditor's reputation is improved in terms of his or her professionalism. The challenge for the IT audit function then becomes how to plan activities to deliver the appropriate type of audit recommendations within the optimal life cycle timeframe. As a rule, the planning strategy must be performed prior to the beginning of the entire cycle, so that appropriate activities are planned in terms of time and resources.

It is critical for the IT audit plan to balance audit activities throughout the entire life cycle, such as avoiding a concentration of audit efforts on the maintenance and production phase and having adequate coverage during the early stages. By following these recommendations, organizations will be able to move from a traditional and post-mortem planning strategy (i.e., one that is based mostly from an operational, compliance, and financial approach) to one that is more innovative, adds value, and is more consultative in nature.

### **6.9 Communicating, Gaining Executive Support, and Obtaining Plan Approval**

As part of their goals, the internal audit department should present the audit plan to senior management and audit committee board members. In particular, resource requirements, significant interim changes, and the potential implications of resource limitations should be communicated to senior management and the board, according to IIA Standard 2020.<sup>14</sup>

It is also important for the IT component of the internal audit plan or the IT audit plan to be discussed with senior management and the board as well as key IT stakeholders, such as the chief information officer, the chief technology officer, IT managers, business applications owners, and other employees with similar roles. The input received from these stakeholders is paramount to the success of the audit planning exercise and will enable CAEs and internal auditors to better understand the business environment, identify risks and concerns, and select audit areas. Furthermore, dialogue on the final plan will help to validate the stakeholders' input throughout the process and provide a preview of upcoming activities.

When discussing the IT audit plan, internal auditors should do so in a manner that is supported by key IT executives, managers, and staff. Gaining the IT team's understanding, coordination, and support will make the audit process more effective and efficient. In addition, understanding the plan facilitates an open and continuing dialogue where evolving risks and changes to the operating environment can be discussed throughout the plan's life cycle and adjustments are made on an ongoing basis. Interaction with the clients when conducting the risk assessment and prior to the final plan's approval is critical to ensure the plan's overall quality.

---

<sup>14</sup> *Internal Auditing: Assurance & Consulting Services* (2007) by Kurt F. Reding, et al, ISBN 978-0-89413-610-8, pp. 8–11.



### 7. Appendix: Hypothetical Company Example

The example in this chapter illustrates how to incorporate the IT audit planning elements discussed in earlier sections. Although the steps can be universally followed, the example's audit subjects and risk assessment results are generic in nature.

#### 7.1 The Company

The hypothetical company is a publicly traded manufacturer and supplier of commodity products used as feeder stock by consumer product manufacturers in different markets around the world. The company's profile is as follow:

- US \$7 billion in total assets.
- Based in the United States.
- Thirty production facilities in seven countries, including Belgium, China, Qatar, Saudi Arabia, Singapore, South Korea, and the United States.
- Six research, technology, and quality control centers located in each production facility.
- Five thousand employees worldwide.
- Five major competitors.
- Holds nearly 3,000 domestic and international patents and patent applications.
- Three major business units for manufacturing operations along product lines, centralized headquarters, and support-service organizations.
- Three major capital projects to build and expand manufacturing capacity.

In addition, the company's centralized IT organization consists of four basic divisions:

- Global infrastructure:
  - Telecommunications.
  - Voice communications.
  - Networks.
  - Remote connectivity.
  - Desktop and Internet.
  - Information life cycle management.
  - Servers.
- Enterprise applications:
  - One major ERP application used throughout the company for supply chain management, financial accounting, human resources (based in the United States), sales, and distribution.
  - Also supplies SAP technical support and Advanced Business Application Programming (ABAP).

- Manufacturing Systems:
  - Responsible for systems operating at manufacturing facilities.
  - Local applications include payroll for non-U.S. sites, research and quality control databases, environmental reporting, and manufacturing process control systems.
  - Financial analysis and controls.
- Strategy and risk management:
  - Contracts, purchasing, and licensing.
  - Strategy, architecture, and standards.
  - Security services.
  - IT change and governance.
  - Project management office.

The manufacturing facilities are the organization's life-blood. Because they are located throughout the world and have different capacity sizes, they introduce risks that may impact business fundamentals and financials. Furthermore, although the manufacturing facilities create a somewhat decentralized business model, the organization's centralized corporate and service elements offer the opportunity for process-based audits that cross business functions.

In the area of compliance, the organization is subject to U.S. and European requirements, including Sarbanes-Oxley, the European Union's Directive on Data Protection (Privacy), the U.S. Foreign Corrupt Practices Act, and other similar regulations in the locations in which it operates. According to the annual business plan, several major capital investment projects are under way that will have a great impact on the organization's future competitiveness.

Finally, the company's IT function aligns closely with its business model. The company uses a fairly homogeneous group of applications, including a standard ERP application, a global network and server infrastructure, and standard support processes for IT service delivery functions, governance, and security.

#### 7.2 The IT Audit Plan

Based on this description, an IT audit universe can be identified that defines a holistic inventory of conceivable audit subject areas and provides management with information on the effectiveness of their control environment and operations.

As mentioned in the previous paragraphs, the centralized corporate and services elements offer the opportunity for global, process-type audit subjects. The company's centralized ERP application, global infrastructure support areas, and standard IT service delivery processes are good candidates for independent audit subjects covering large areas of IT risk.

Manufacturing facilities also are represented in the IT audit universe with subjects from locally supported applications



## GTAG — Appendix: Hypothetical Company Example

and an underlying infrastructure (shown as facility 1–30 for simplicity in table 7). These audit subjects are likely to be aligned with business process audits in each facility.

Table 7 shows what a sample universe of potential IT audit subjects might look like for the company. Each of the 30 manufacturing facilities has these and other audit subject areas.

Business Unit	Audit Subject
Corporate	Network administration and security
Corporate	Remote connectivity
Corporate	Windows Server administration and security
Corporate	UNIX administration and security
Corporate	ERP application and general controls
Corporate	Sarbanes-Oxley sustainability review
Corporate	Corporate privacy compliance
Corporate	Database administration and security
Corporate	IT governance practices
Corporate	ITIL deployment practices
Corporate	Application program change control
Business Segment 1–3	Major capital investment projects (e.g., information protection and corporate compliance)
Facility 1–30	IT infrastructure
Facility 1–30	Human resources and payroll application
Facility 1–30	Process control systems

**Table 7.** IT audit universe

After the IT audit universe is defined at a high level, the next step is to assess the business and IT risks on each area. Risk categories are assessed based on their likelihood of occurrence and the impact they would have on the organization if the risk was not adequately managed. This risk approach uses relative ranking as shown in table 8. For example, a three-point scale to assess likelihood and impact is used as outlined in the following description:

Likelihood Scale		
H	3	High probability that the risk will occur.
M	2	Medium probability that the risk will occur.
L	1	Low probability that the risk will occur.

Impact Scale (Financial)		
H	3	There is a potential for material impact on the organization's earnings, assets, reputation, or stakeholders.
M	2	The potential impact may be significant to the audit unit, but moderate in terms of the total organization.
L	1	The potential impact on the organization is minor in size or limited in scope.

**Table 8.** Three-point likelihood and impact scale

To aid in the analysis, a range is selected that indicates a relative risk ranking of high, medium, and low, as follows:

Level	Composite Risk Score Range	Recommended Annual Cycle
H	35–54	Every 1 to 2 years
M	20–34	Every 2 to 3 years
L	6–19	Every 3 to 5 years

**Table 9.** Range of relative risk ranking

As part of the risk assessment step, auditors need to define a recommended annual cycle for audit subjects in the universe based on composite risk score ranges, where high-risk audit subjects are reviewed every one to two years, medium-risk subjects every two to three years, and low-risk subjects every three to five years. This will ensure that high-risk areas are reviewed frequently and low-risk areas are covered adequately over a five-year span. Table 10 on page 24 shows an example of a completed risk assessment.

## GTAG — Appendix: Hypothetical Company Example

Area	Financial Impact		IT Risks										Score and Level	
			Quality of Internal Controls		Changes in Audit Unit		Availability		Integrity		Confidentiality			
	L	I	L	I	L	I	L	I	L	I	L	I		
ERP Application & General Controls	3	3	2	3	3	3	2	3	2	3	2	3	42	H
Treasury EFT Systems	3	3	3	3	3	3	3	2	3	2	2	1	41	H
Facility 3 – HR/Payroll Application	3	3	3	2	3	3	2	2	2	3	2	3	40	H
Employee Benefits Apps (Outsourced)	2	3	2	2	3	3	3	2	2	3	3	3	40	H
Facility 3 – IT Infrastructure	2	2	3	2	3	3	3	3	3	2	2	2	38	H
Facility 3 – Process Control Systems	3	3	3	2	3	3	3	3	2	2	2	1	39	H
UNIX Administration and Security	2	2	3	2	3	3	2	3	3	2	2	2	35	M/H
Corp. Privacy Compliance	3	1	3	3	3	3	2	1	2	1	3	3	34	M/H
Database Administration and Security	2	2	2	2	2	2	3	3	2	2	2	1	27	M
Windows Server Admin and Security	2	2	1	2	2	2	2	3	3	2	2	2	26	M
Facility 1 – IT Infrastructure	2	2	3	2	1	3	3	2	3	1	1	1	23	M
Facility 1 – Process Control Systems	2	3	3	2	2	2	3	3	1	1	1	1	27	M
Environment Reporting Systems	2	2	3	2	2	2	2	3	1	1	3	1	24	M
Facility 2 – IT Infrastructure	2	2	3	2	1	3	3	2	3	1	1	1	23	M
Major Capital Investment Projects	2	2	3	3	1	1	2	2	1	1	2	3	25	M
Application Program Change Control	2	3	2	3	1	2	2	2	1	3	1	2	23	M
SOX Sustainability Review	2	2	2	3	2	2	1	2	2	2	1	2	22	M
Network Administration and Security	2	2	2	1	2	2	2	2	2	2	2	2	22	M
Facility 2 – Process Control Systems	2	2	2	2	1	2	2	2	2	2	1	1	19	M/L
ITIL Deployment Practices	1	2	2	3	3	1	3	1	1	3	2	1	19	M/L
Facility 2 – HR/Payroll Application	1	2	1	2	2	3	2	2	3	1	1	2	19	M/L
Facility 30 – HR/Payroll Application	1	1	1	2	2	2	2	2	2	2	1	2	17	L
Facility 1 – HR/Payroll Application	1	1	1	2	2	2	2	2	2	2	1	2	17	L
Facility 30 – IT Infrastructure	1	1	3	1	1	1	2	2	2	1	1	1	12	L
Facility 30 – Process Control Systems	1	1	2	2	2	2	2	2	1	1	1	1	15	L
IT Governance Practices	1	1	2	2	1	1	3	1	1	1	1	2	12	L
Remote Connectivity	1	1	1	2	2	1	1	1	1	2	2	2	12	L
L = Likelihood I = Impact														

Table 10. Risk assessment

## GTAG — Appendix: Hypothetical Company Example

Once risk assessment results are available, the next step is to formalize the audit plan. As discussed in section 6, the audit plan consists of risk-driven audit projects, mandatory compliance reviews, stakeholder requests, and follow-up audits of previously identified significant issues. Because these tasks need to be completed using available internal audit resources, some risk-driven audit projects might not be incorporated in the plan.

Continuing with the hypothetical company example, the board has asked the IT department to be involved in the coordination of an external infrastructure penetration test, and operating management has requested assurance that Sarbanes-Oxley management testing is sustained throughout the organization. In addition, the IT function asked the internal audit department to be involved with an ITIL deployment project to identify whether service delivery processes are effective and cover all risks.

These stakeholder requests are accepted because they fit with the mission of the internal audit department and will

be added automatically to the audit plan. Furthermore, there was a significant segregation of duties issue identified in the previous year's procurement process audit, so a follow-up review will be added to the plan to ensure agreed upon remediation efforts are progressing as planned. In the compliance area, compliance with the new corporate policy on protecting personal data for privacy will be included because there are plans to transmit personal data between non-U.S. facilities and the U.S. corporate headquarters.

The company has an IT audit staff of five auditors or approximately 1,000 available days for engagements after considering exception time and training. Based on the risk assessment of available audit subjects, mandatory activities, and stakeholder requests, the most effective audit plan is shown in table 11. Several high-risk subjects were not included in the plan (e.g., treasury electronic funds transfer (EFT) systems, process control systems, and database administration and security) because they were reviewed in the last 12 months.

Engagement	Risk Level	Cycle	Audit Days Allocated
Penetration Test Coordination	*	0	40
Procurement Application Follow-up	*	0	20
ERP Application & General Controls	H	1	100
Facility 3: HR/Payroll Application	H	2	30
Employee Benefits Apps (Outsource)	H	3	100
Facility 3: IT Infrastructure	H	2	90
UNIX Administration and Security	M/H	1	90
Corp. Privacy Compliance	M/H	3	40
Windows Server Administration and Security	M	3	90
Facility 1: IT Infrastructure	M	3	90
Facility 1: Process Control Systems	M	3	90
Environment Reporting Systems	M	3	30
Major Capital Investment Projects	M	3	30
Sarbanes-Oxley Sustainability	M/*	3	120
ITIL Deployment Practices	L/*	4	40
Total			1000
* Management Request			

Table 11. The audit plan

## GTAG — Appendix: Hypothetical Company Example

The audit plan in table 11 represents the ideal audit plan based on the company's internal audit department and its understanding of the company's strategies and objectives, historical knowledge of the control environment, and anticipated changes in operations during the next audit period. The plan should be reviewed with senior and operations management as a follow-up discussion to the risk assessment and audit planning phases. Doing so will validate management input was considered accurately in the process and give managers a preview of the upcoming year's IT audit plan.

The review also is an appropriate time to discuss potential audit engagement dates as the company might experience blackout periods due to the audit's possible disruption of company operations. For example, planned dates for application or infrastructure upgrades should be discussed, as well as schedules of significant operational activities, such as plant shutdowns and turnarounds, that could affect the audit process.

Following the plan's completion is the scheduling of audits and audit resources. In general, audits have to be staffed with appropriately skilled auditors to ensure the engagement's success. However, the audit schedule is also a good opportunity to address staff development needs through the exposure of audits that will expand and develop specific skill areas.

Finally, there will be changes that might impact the audit plan and schedule due to the organization's dynamic nature. As a result, it is important to have an effective plan in place, manage the plan throughout its life cycle, and be flexible to company changes so that resources stay focused on evolving risk areas and the organization's concerns.

## 8. Glossary of Terms

**Application program code:** Sets of computer programs, control files, tables, and user interfaces that provide functionality for specific business operations, such as accounting, payroll, and procurement.

**Business process:** A set of connected business activities that are linked with each other for the purpose of achieving a business objective.

**Chief audit executive (CAE):** The top position within the organization responsible for internal audit activities.

**Compliance:** Conformity and adherence to applicable laws and regulations, which also includes conformity and adherence to policies, plans, procedures, contracts, or other requirements.

**Consulting services:** Advisory and related services that are agreed to with the client to improve an organization's governance, risk management, and control environment.

**Control environment:** Board and management attitudes and actions regarding the significance of organizationwide controls. The control environment provides the structure for the achievement of the internal control system's primary objectives.

**Database systems:** A system of programs that enable data storage, modification, and extraction.

**Enterprise resource planning (ERP):** ERP systems are major software applications that manage whole business processes. They also integrate procurement, inventories, sales, distribution, human resources, and customer service activities, as well as financial management and other organizational aspects.

**Framework:** Guiding principles that form a template organizations can use to evaluate business practices.

**IT infrastructure:** Key components of an application's technical infrastructure, including its program logic code, database, operating system, network, and physical environments housing each component.

**Internal audit function:** A department, division, team of consultants, or other practitioners that provide independent, objective assurance and consulting services designed to add value and improve an organization's operations.

**Networks:** Physical devices, such as switches, routers, firewalls, wiring, and programs, which control the routing of data packets to link computers and enable them to communicate with each other.

**Operating systems:** Software that performs a computer's basic tasks, such as handling operator input, managing internal computer memory, and providing disk drive, display and peripheral device functions.

**Outsourcing:** The use of a third-party to perform noncore company services. Outsourcing is becoming more prevalent due to the high cost and expertise required to deliver noncore services.

**Policy:** A written statement that communicates management's intent, objectives, requirements, and responsibilities.

**Risk:** The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

**Risk assessment:** A methodology for determining the likelihood of an event that could hinder the organization from attaining its business goals and objectives in an effective, efficient, and controlled manner.

**Risk management:** The management process used to understand and deal with uncertainties that could affect the organization's ability to achieve its objectives.

**Service support processes:** Within an IT context, the processes used to manage an organization's IT infrastructure and the development and installation of new computer systems and IT operations. Service support processes include service desk activities and configuration, change, release, incident, and problem management procedures.

**Standards:** A mandatory business process or procedure that provides direction on how to comply with the policy to which it is linked. IT standards are generally technology neutral and can be further divided into IT-specific controls and guidelines.

**System of internal controls:** A system comprising the five components of internal control — the control environment, risk assessment, control activities, information and communication, and monitoring — to ensure risk is managed.

**System implementation projects:** Larger scale efforts in the IT delivery function to deploy new systems of applications or infrastructure components. These efforts involve project management activities, business processing reengineering, and behavioral change management techniques.

**Third party:** An entity that is not affiliated with the organization.

### 9. Glossary of Acronyms

**CAE:** Chief audit executive

**CBOK:** The IIA Research Foundation's Common Body of Knowledge

**COBIT:** Control Objectives for Information and Related Technology

**COSO:** The Committee of Sponsoring Organizations of the Treadway Commission

**EFT:** Electronic funds transfer

**ERM:** Enterprise risk management

**ERP:** Enterprise resource planning

**EU:** European Union

**GLBA:** U.S. Gramm-Leach Bliley Act

**GTAG:** Global Technology Audit Guide

**HIPAA:** U.S. Health Insurance Portability and Accountability Act

**IIA:** The Institute of Internal Auditors

**ISO:** International Organization for Standardization

**IT:** Information technology

**ITGI:** IT Governance Institute

**ITIL:** The UK Office of Government Commerce's IT Infrastructure Library

**PCAOB:** U.S. Public Company Accounting Oversight Board

**PCI DSS:** Payment Card Industry Data Security Standard

**QAR:** The IIA's external quality assurance review

**SDLC:** System development life cycle

**SOX:** U.S. Sarbanes-Oxley Act of 2002



## 10. About the Authors



### Kirk Rehage

Kirk Rehage is the group manager of IT auditing for Chevron Corp., a member of The IIA's Advanced Technology Committee and ISACA, and term governor for the North California East Bay IIA Chapter. As IT audit group manager, Rehage is responsible for the Internal Audit Department's IT assurance and controls consulting activities in more than 180 countries.

Rehage has more than 30 years of energy industry experience and has held a variety of roles delivering IT services, such as building computing infrastructure and network environments, managing application delivery organizations, and technical programming of engineering and earth science analytical software and database solutions.



### Steve Hunt, CIA, CISA, CBM

Steve Hunt is a senior manager in the risk consulting group of Crowe Chizek and Company LLC, vice chair of The IIA's Advanced Technology Committee, and a member of ISACA and the Association of Professionals in Business Management. At Crowe Chizek, Hunt works with *Fortune* 1000 mid-sized, and small-market companies in different industries, directing the delivery of financial, operational, and IT risk management engagements.

Hunt has more than 20 years of experience working in different industries, including accounting, internal auditing, and management consulting. More specifically, he has performed in-depth Sarbanes-Oxley compliance audits and other internal and external audits, and participated in business process reengineering projects and business development initiatives. He also has several years of experience configuring SAP R/3 applications and application security and business process controls and has been a featured speaker at several universities and organizations in the United States.



### Fernando D. Nikitin, CIA, CISA, CGEIT, CISM, CISSP

Fernando Nikitin has more than 16 years of experience in internal auditing, IT governance, and information security and has worked for banking, government, and multilateral organizations. He is an internal auditor at the Office of the Auditor General of the Inter-American Development Bank. Previously, Nikitin was the IT audit manager at Banco de la Republica Oriental del Uruguay.

Nikitin is a member of The IIA's Advanced Technology Committee, a board member of ISACA's Government and Regulatory Agencies Board, and a contributor of the National Institute of Technology of India. He is also a former president of ISACA Montevideo's Uruguay Chapter, co-founder of the Project Management Institute's Uruguay Chapter, and a member of the International Information Systems Security Certification Consortium. Nikitin earned his MBA degree from EOI Business School in Madrid, Spain.

## Reviewers

The IIA thanks the following individuals and organizations that provided valuable comments and added great value to this guide:

- Professional Practices Committee:
  - Advanced Technology Committee
  - Board of Regents
  - Committee on Quality
  - Internal Auditing Standards Board
  - Professional Issues Committee
  - Ethics Committee
- Urton Anderson, McCombs School of Business, The University of Texas at Austin, USA
- Lily Bi, The IIA, USA
- Larry Brown, The Options Clearing Corp., USA
- Faisal R. Danko, London, UK
- Christopher Fox, ASA, eDelta, New York, USA
- Nelson Gibbs, Deloitte & Touche LLP, USA
- Frank Hallinan, Chevron Phillips Chemical Co. LP, USA
- Greg Kent, SecureIT, USA
- Lemuel Longwe, Ernst & Young Chartered Accountants, Zimbabwe
- Steve Mar, Resources Global, USA
- Tom Margosian, Ford Motor Company, USA
- James Reinhard, Simon Property Group Inc., USA

# The Unique Alternative to the Big Four



Crowe is a top 10 public accounting and consulting firm. We provide innovative solutions in the areas of assurance, financial advisory, performance, risk consulting, and tax. Differentiating ourselves from many others, Crowe has a specific focus on serving a broad array of organizations' risk consulting needs. Service areas include:

- Governance, risk, and compliance;
- Internal audit teaming, cosourcing, and outsourcing;
- Sarbanes-Oxley Section 404 consulting;
- IT audit cosourcing;
- Vulnerability and threat management;
- Technology risk assessment;
- Business continuity and disaster recovery.
- Regulatory consulting;
- Application integrity;
- Identity and access management;
- Privacy and data protection;
- SAS 70 audits;
- Payment card industry reviews.

With clients throughout the United States and internationally, Crowe's practice brings together independent, objective, and cost-effective experts in internal auditing from Big Four and large corporate internal audit backgrounds to provide innovative solutions to their clients. Learn why companies are turning to Crowe Chizek and Company LLC as The Unique Alternative to the Big Four.

For more information, contact **Vicky Ludema** at **800.599.2304** or [vludema@crowechizek.com](mailto:vludema@crowechizek.com).



# Crowe provides a consultative and practical approach to IT audit.



Do you need an IT audit department or are you looking to augment your existing IT audit department with some specialized skills? Whatever your IT audit needs are, Crowe Chizek and Company LLC can tailor a solution for you.

Crowe's IT audit outsourcing/cosourcing comes with a comprehensive portfolio of IT audit services to help you:

- Assess the technology components that are critical to your business processes;
- Determine technology risks that your organization may be exposed to;
- Develop custom IT audit plans based on the results of our technology risk analysis;
- Evaluate the adequacy of existing controls to manage your specific risks;
- Design and implement control solutions and improvements;
- Comply with regulatory requirements such as SOX 404, GLBA, and HIPAA.

Crowe's services are delivered by highly trained specialists with practical technology solutions and innovative processes to help meet your IT audit needs. Our risk assessment and audit methodologies and tools provide a structured and optimized approach to help evaluate and address technology risks.

Our audit professionals have a strong mix of industry and internal audit experience in various technologies such as SAP, PeopleSoft®, Oracle®, JD Edwards, VMWare, UNIX®, Microsoft® Windows, mainframe, and AS/400. Our professional certifications include CISA, CCP, CIA, CISSP, MCSE, and CCSE.

Crowe has served more than 100 clients in the internal audit outsourcing or cosourcing capacity across the United States. Whether you need full-time or on-demand IT audit experts, count on Crowe.

The Unique Alternative to the Big Four®



Oracle and PeopleSoft are registered trademarks of Oracle Corp.  
Microsoft is a registered trademark of Microsoft Corp.  
UNIX is a registered trademark of the SCO Group.



Crowe Chizek and Company LLC is a member of Horwath International Association, a Swiss association (Horwath). Each member firm of Horwath is a separate and independent legal entity. Accountancy services in the state of California are rendered by Crowe Chizek and Company LLP, which is not a member of Horwath. © 2008 Crowe Chizek and Company LLC

RISK8068



## *Developing the IT Audit Plan*

Due to the high degree of organizational reliance on IT, it is crucial that chief audit executives (CAEs) understand how to create an IT audit plan as well as determine the frequency of audits and the breadth and depth of each audit. However, results from several Institute of Internal Auditors (IIA) external quality assessment reviews reveal that developing an appropriate IT audit plan is one of the weakest links in internal audit activities. Many times, internal auditors simply review what they know or outsource to other companies, letting them decide what to audit.

To this end, *Developing the IT Audit Plan* can help CAEs and internal auditors:

- Understand the organization and how IT supports it.
- Define and understand the IT environment.
- Identify the role of risk assessments in determining the IT audit universe.
- Formalize the annual IT audit plan.

This GTAG also provides an example of a hypothetical organization to show CAEs and internal auditors how to execute the steps necessary to define the IT audit universe.

Visit [www.theiia.org/guidance/technology/gtag/gtag11](http://www.theiia.org/guidance/technology/gtag/gtag11) to rate this GTAG or submit your comments.

Order Number: 1046

IIA Member US \$25

Nonmember US \$30

IIA Event US \$22.50

