

**GTAG**

GLOBAL TECHNOLOGY AUDIT GUIDE

# Management of IT Auditing



The Institute of  
Internal Auditors

## GTAG Partners



AICPA – American Institute of  
Certified Public Accountants  
[www.aicpa.org](http://www.aicpa.org)



CIS – Center for Internet Security  
[www.cisecurity.org](http://www.cisecurity.org)



CMU/SEI – Carnegie-Mellon University  
Software Engineering Institute  
[www.cmu.edu](http://www.cmu.edu)



ISSA – Information Systems Security Association  
[www.issa.org](http://www.issa.org)



ITPI – IT Process Institute  
[www.itpi.org](http://www.itpi.org)



NACD – National Association of  
Corporate Directors  
[www.nacd.org](http://www.nacd.org)



SANS Institute  
[www.sans.org](http://www.sans.org)

# **Global Technology Audit Guide**

## **Management of IT Auditing**

Author

Michael Juergens, Principal, Deloitte & Touche LLP

Contributing Author

David Maberry, Senior Manager, Deloitte & Touche LLP

Contributing Editors

Eric Ringle, Senior Manager, Deloitte & Touche LLP

Jeffrey Fisher, Senior Manager, Deloitte & Touche LLP

March 2006

This guide has been produced and distributed through  
the sponsorship by Deloitte & Touche LLP.

Copyright © 2006 by The Institute of Internal Auditors, 247 Maitland Avenue, Altamonte Springs, Florida 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 of 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.

# GTAG – Table of Contents

---

1. Summary for the Chief Audit Executive	1
2. Introduction	2
3. Defining IT	3
3.1 IT Management	4
3.2 Technical Infrastructure	4
3.3 Applications	4
3.4 External Connections	5
4. IT-related Risks	6
4.1 The Snowflake Theory	6
4.2 Risk Evolution	6
4.3 IT-related Risk Proliferation	7
4.4 Types of IT-related Risks	7
4.5 IT Risk Assessment	7
5. Defining the IT Audit Universe	10
5.1 Tips for the CAE	10
5.2 Budgeting for IT Audit	10
6. Executing IT Audits	12
6.1 Frameworks and Standards	12
6.2 IT Audit Resource Management	14
7. IT Audit Accelerators	17
7.1 Audit Facilitators	17
7.2 Testing Accelerators	17
8. Questions for the CAE	19
A. Appendix A - Emerging Issues	20
A.1 Wireless Networks	20
A.2 Mobile Devices	20
A.3 Interfaces	21
A.4 Data Management	21
A.5 Privacy	22
A.6 Segregation of Duties	22
A.7 Administrator Access	23
A.8 Configurable Controls	24
A.9 Piracy	24
Other Resources	25
About the Authors	26

Information technology (IT) is changing the nature of the internal audit function. As new risks emerge, new audit procedures are required to manage these risks adequately. This guide, which was created to help the chief audit executive (CAE) plan and manage the IT audit function more effectively and efficiently, covers how to:

**Define IT** – What areas should be considered for inclusion in an IT audit plan? The CAE should be able to measure his or her planned IT audit scope against the guidelines presented here to help ensure that the scope of IT audit procedures is adequate.

**Evaluate IT-related Risk** – It is clear that the evolution of IT introduces new risks into an organization. This guide will help the CAE understand how to best identify and quantify these IT-related risks. Doing so will help ensure that IT audit procedures and resources are focused on the areas that represent the most risk to the organization.

**Define the IT Audit Universe** – IT audit resources are typically scarce, and IT audit demands are substantial. A section on defining the IT audit universe will help the CAE understand how to build an IT audit plan that effectively balances IT audit needs with resource constraints.

**Execute IT Audits** – The proliferation and complexity of IT dictates the need for new IT audit procedures.

Auditing by checklist or by inquiry is likely to be insufficient. This book offers specific guidance for the CAE on how to execute IT audit procedures and how to understand what standards and frameworks exist in the marketplace that can support required procedures.

**Manage the IT Audit Function** – Managing the IT audit function may require new management techniques and procedures. This guide provides helpful hints and techniques for maximizing the effectiveness of the IT audit function and managing IT audit resources.

**Address Emerging Issues** – IT evolves rapidly. This evolution can introduce significant new risks into an organization. The world class CAE focuses IT audit attention on not just the basic building blocks of IT, but also new and emerging technologies. A section on emerging issues will provide specific information on a number of emerging technologies, evaluate the risks that these technologies pose to an organization, and provide recommendations for how the CAE should respond to these risks.

The focus of this guide is on providing pragmatic information in plain English, with specific recommendations that a CAE can implement immediately. Further consideration is given to providing questions that a CAE can ask to help understand whether his or her IT audit function is a high performer.

## GTAG — Introduction — 2

There is no question that IT is changing the nature of the internal audit function. The risks companies face, the types of audits that should be performed, how to prioritize the audit universe, and how to deliver insightful findings are all issues with which CAEs must grapple. Without a deep technical background, however, it may be challenging to find answers to these and other questions.

This GTAG is designed for CAEs and internal audit management personnel who are responsible for overseeing IT audits. The purpose of the guide is to help sort through the strategic issues regarding planning, performing, and reporting on IT audits. Consideration will be given to the fundamentals as well as emerging issues.

IT auditing is increasing in importance, primarily because organizations are becoming increasingly dependent on IT. Key processes are automated, or enabled by technology. It is possible for a sales order to come in through a Web site, be transmitted to the warehouse floor, and be shipped to the customer without anyone other than the warehouse worker seeing or touching the order.

As organizations increase their reliance on IT, two primary issues emerge:

- **A large percentage of the key internal controls on which the organization relies are likely to be technology driven.** Example: Corporate policy states that before any payment is made to a vendor, a three-way match is performed. Historically, that match was likely performed by a clerk, who physically matched pieces of paper, stapled them, and filed them. Now, all matches may be performed by the organization's enterprise resource planning (ERP) system. The system automatically performs the match based on pre-configured rules and tolerance levels and automatically posts variances to defined variance accounts.

To audit that control effectively, an auditor must go into the configuration settings of that ERP system and evaluate the rules and settings. This requires a far different skill set and audit program than the historical process did. To perform an effective audit, the historical audit approach needs to be re-engineered to address the new risks. This requires a focus on — and understanding of — audit technology.

- **Systems that lack integrity or have control deficiencies will have a larger impact on the organization's operations and competitive readiness, thereby increasing the need for effective IT controls.** Example: Consider the automated process described above, where a sales order comes in via a Web site and is directly transmitted through the ERP system to the warehouse floor. Now consider what happens when a customer accidentally orders 100 pallets instead of 100 units. If the organization has fully optimized its processes with an ERP system, it is possible that the system will check inventory, note that 100 pallets are not available, update the production schedule to

produce 100 pallets, and automatically send off purchase orders for raw materials via Electronic Data Interchange (EDI). Potentially, this error may not get caught until the customer receives the goods — far too late.

Clearly, to mitigate these types of risks, organizations need to execute well-designed IT plans that consider these issues. Unfortunately, most organizations have only migrated to highly automated environments in the last 10 years or fewer. Thus, traditionally, there may not have been a deep focus on audit technology, nor deep sources of thought leadership regarding how to audit technology. Part of that is due to the rapid rate of technological advances. There have not been any radical developments in the three-way match process in many years; however, the applications used to support these processes evolve annually.

One additional issue that often comes up when planning the IT audit universe is truly understanding how the IT controls relate to financial reporting, fraud, and other key issues. This is relatively easy to grasp when you are evaluating controls within an application system (e.g. the three-way match settings discussed above). However, it is much more difficult when evaluating supporting technologies. Assume the organization maintains an Internet connection, but does not have a firewall to protect the internal network. Are the financials misstated? Are operations impacted? It becomes harder to draw the direct correlation as the technology is further removed from the business operations.

Given this, many CAEs often provide less audit attention to these supporting technologies, which can represent a rather myopic view of IT risk. The fact of the matter is that control deficiencies in supporting technologies can have a far greater impact on the organization than IT controls specific to a single process.

For example, let's assume that an organization creates electronic payments that it sends to its vendors. These payments are routed electronically to bank accounts based on automated clearing house (ACH) routing numbers for each vendor account. All those ACH numbers are stored somewhere in a table in the organization's database system. A database administrator, or anyone with the right access to the database, could merely change every entry in that table to his or her own bank account ACH route. The next time the organization did an electronic check run, the entire run would be deposited into the perpetrator's bank account. This would completely circumvent all security, control, and audit trail mechanisms that exist within the business process and the business application — including positive pay.

In the above scenarios, it is easy to see how a control deficiency at the database level could have a far greater impact than a deficiency with the three-way match settings. It is for this reason that CAEs must carefully consider all layers of the IT environment when planning the IT audit universe for the year.

One of the initial challenges a CAE faces when developing the IT audit plan for the year is defining the IT boundaries. Are the phone and voice mail systems part of IT? Should facilities badging and physical security systems be included? What if those are outsourced to the property management company? These are some of the issues that CAEs grapple with when trying to determine how to allocate IT audit resources.

The reality is that IT means different things to different organizations. Even two companies in the same industry may have radically different IT environments. Unfortunately, what IT is, or should be, is not clearly or universally defined.

This section will help CAEs address how to think about IT within an organization. Recognizing that there is a high amount of heterogeneity in IT environments, one way a CAE can approach the definition of IT is by thinking about it in layers, like a parfait. Each layer is different and important. Risks exist at each layer of the environment, and the risks vary greatly. Hacking the corporate Web site, for example, is a very different risk to the organization than stealing the aforementioned electronic check run.

**Consider Each Layer**

For an IT audit function to be effective, the risks of each layer need to be considered and prioritized, and audit resources should be allocated to each layer. If the IT audit plan does not include audits for each layer of the environment, odds are that the audit plan taken as a whole is not going to address the organization’s IT risk adequately.

It should be noted that, in some cases, it may be appropriate to consider all the layers over a period of time (i.e.

over multiple years on a rotational basis) rather than covering all layers within a single year. Private companies or organizations that do not need to comply with the U.S. Sarbanes-Oxley Act of 2002 or other controls regulations or legislation, such as the Federal Deposit Insurance Corporation Improvement Act, may wish to establish a plan that covers the IT universe over a period of two to three years. Rotational plans that extend beyond three years are probably inadequate due to the high rate of change in the IT environment.

How many resources should be allocated to each layer? Where within the layer should they be allocated? Answers to these challenging questions should be the natural outcome of the risk assessment processes, combined with the auditor’s judgment and strategic thinking. Regardless of the specific resource allocation, all layers should be considered.

**What Are the Layers?**

Figure 1 below, is a simple depiction of an IT environment. Obviously, each organization is different, but this graphic should cover the majority of critical systems for most organizations. The key layers to consider are:

- IT management.
- Technical infrastructure.
- Applications.
- External connections.

Note that this graphic doesn’t define the categories of the IT audit plan. When specific IT audits are planned, they may be organized into categories based on the organization’s processes, or by standardized frameworks, etc. This graphic is

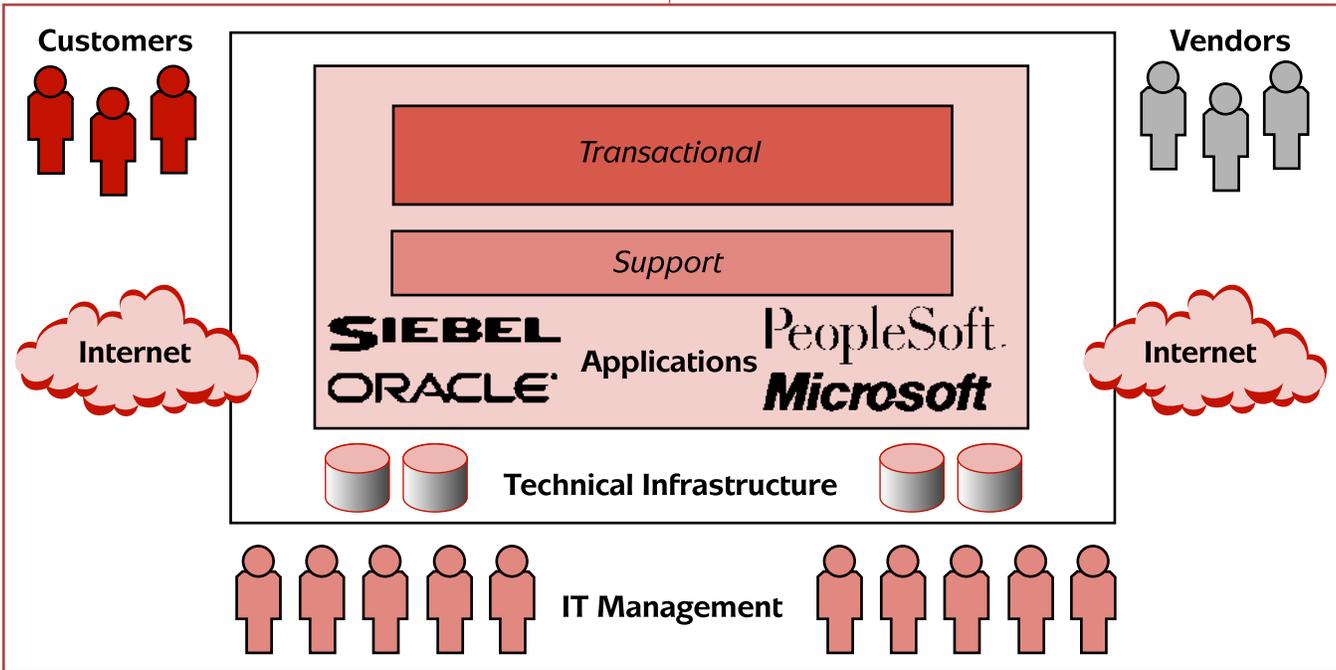


Figure 1 – IT Environment

## GTAG – Defining IT – 3

designed to get the CAE thinking about the IT environment and making sure that audit resources are allocated to each layer. Organizing the specific audits is left to the judgment of the CAE.

### 3.1 IT Management

This layer comprises the set of people, policies, procedures, and processes that manage the IT environment. Technologies can be deployed — for example, an organization can implement SAP ERP in a Unix environment — but the integrity of the systems and data are highly contingent on specific tasks that administrative personnel perform on a regular basis. Therefore, this layer includes:

**System Monitoring** – Monitoring involves identifying transactions that failed to post due to a processing error, or identifying when a database becomes corrupted.

**Programming** – Many organizations perform internal programming for various systems. Programming needs to be managed and overseen so that programs with errors do not impact the integrity of key systems.

**Planning** – The IT department should be developing both long-term and short-term IT strategic plans. These should align with the organization’s long- and short-term plans. The absence of good IT strategic planning all but guarantees that IT will not support the organization’s objectives, taken as a whole.

**Management of Outsourced Vendors** – Many organizations outsource various components, or all, of the IT environment to an external vendor. In these situations, managing the outsourced relationship effectively is a critical piece of ensuring the integrity of the computing environment.

**IT Governance** – Setting a strong tone at the top for designing, building, and operating IT systems with integrity; communicating that culture throughout the IT function; overseeing the development and deployment of policies and procedures; and assessing performance are key components of running an IT function.

Note that audits of these functions will be similar to process audits. The IT auditor is looking at people and tasks as opposed to a technical system setting. Tests of controls will be quite different and will require a certain amount of judgment.

### 3.2 Technical Infrastructure

This layer is referred to by many different names, such as general computer controls, pervasive controls, or supporting technologies. It essentially refers to the systems that underlie, support, and enable the primary business applications. In general, this includes:

**Operating Systems** – The set of programs that instruct the computer systems on how to function. Examples include Unix, Windows 2003, and OS/400. All programs and

files eventually reside somewhere on the operating system. Actions performed at the operating system level generally circumvent most security and controls that exist at the process level. For example, consider an executive’s laptop. If the executive wants to delete an e-mail, he or she would log in to the e-mail application and delete that e-mail. The program would probably ask, “Are you sure?” Then, the deleted e-mail would be stored in a special folder for a period of time so that it could be recovered. However, the same executive could also open Windows Explorer and delete all directories in the C: drive. The effect would be the same; the e-mail would be gone. In the latter example, though, there are clearly fewer controls.

**Databases** – All business data, critical or otherwise, ends up residing in some sort of database somewhere in the environment. Databases are comprised of tables containing data, which, among other things, form the basis for all business reports. Examples include Oracle, MS SQL Server, and DB2. Actions performed at the database level also tend to circumvent most controls that exist at the process level — vis-à-vis the earlier accounts payable fraud example.

**Networks** – For data to flow through an organization, it must have a method of traveling, whether across a wire, a fiber optic cable, or wireless system. The network consists of physical components such as cables; devices that manage the movement of network traffic such as switches, routers, or firewalls; and programs that control the movement of data. The integrity of the network plays a large role in ensuring the completeness and accuracy of the organization’s business data. For example, if a warehouse worker preparing to ship a product scans it with a barcode scanner, how does that transaction get recorded back on the general ledger (G/L)? Answer: It travels across the network and is processed. But what if it doesn’t travel across the network? What if it is changed along the way, or disappears altogether? How would the organization know?

Technical infrastructure audits tend to focus more on review of technical configuration settings than processes.

### 3.3 Applications

Business applications are programs that perform specific tasks related to business operations. These generally can be classified into two categories: transactional applications and support applications.

#### Transactional Applications

Transactional applications consist primarily of software that processes and records business transactions. Examples include sales order processing, general ledger recording, and warehouse management. Transactional applications

typically fall into one of the following categories:

**Buy Side** – enables procurement and supply chain processes.

**Sell Side** – enables sales and distribution processes.

**Back Office** – enables financial accounting, payables, receivables, and human resources processes.

**ERP** – integrated software that does one or more of the above.

### Support Applications

Support applications are specialized software programs that facilitate business activities but generally do not process transactions. Examples include e-mail programs, fax software, document imaging software, and design software.

The bulk of the IT audit attention should be oriented toward transactional applications. However, depending on certain industries, some support applications may be high risk as well. Example: Company XYZ makes a consumer product and has a highly recognizable brand. It continuously loses money due to product knock-offs being sold by corporate pirates. Its creative team designs new products on an integrated computer design software package. In this case, the company should evaluate the controls around this support application, as it could represent a bottom-line risk to the company if new designs are stolen prior to new products hitting the street.

### 3.4 External Connections

The corporate network does not operate in isolation. It is most certainly connected to many other external networks. The Internet, of course, is the one that most readily comes to mind, but many times CAEs make the mistake of stopping there. In fact, it is highly likely that the corporate network is connected to many other networks. For example: Does the organization do business via EDI? If so, the corporate network is probably connected to an EDI provider network, or perhaps directly connected to the network of a trading partner. Does the organization use any third-party warehouse providers? If so, the two networks are probably linked together.

Furthermore, as organizations continue to automate key processes, more access to the corporate network is granted to outsiders, often via the Internet. Consider, for example, the ability to look up the account status of a credit card or the shipping status of a FedEx package. Customers who perform those activities are likely entering those companies' internal networks via the Internet.

The issue here is that external networks are not under the control of the organization and therefore should not be trusted. All communication to and from external networks should be tightly controlled and monitored. It can be challenging to define IT audit procedures to address this risk, because the organization can only audit what it can control. Thus, it is critical to audit the entry and exit points, at a minimum.

### 4.1 The Snowflake Theory

Every IT environment is unique and, accordingly, represents a unique set of risks, says the snowflake theory. The differences in IT environments make it increasingly difficult to take a generic or checklist approach to IT auditing. To be effective, each organization should define an IT audit approach and create IT audit work plans that are specific to the needs of that particular environment.

This is very different from the financial or operational audit areas, where certain risks are endemic to a given industry or size of company. Consider the following: Company ABC and Company XYZ are both media and entertainment companies. Both companies face risk in calculating ultimate accounting entries for movies that have been released. This process would be something that the internal audit function would definitely audit.

On the IT side, however, Company ABC is using Oracle Applications as the primary business system, running on Windows 2000 and using an Oracle database. There is one centralized Oracle system. Company XYZ has a decentralized IT function, with each business unit using its own system on a variety of platforms. Each business unit reports into a consolidation system, which the company has outsourced to a third-party provider. Clearly, the IT audits that would be planned and executed for Company ABC would vary greatly from those for Company XYZ.

#### The Configuration Factor

Another primary factor in the snowflake theory is configuration. When a company deploys a given technology, it configures the technology to support its particular objectives. There can be a high degree of variability from environment to environment. One company using Windows 2003 as the primary operating system may have set up multiple domains, with trusted relationships among all the domains. Another may have only a single domain, using Windows Active Directory to manage all user access. Although both companies are using the same technology, the risks are very different; consequently, the performance of IT audits is also very different.

Configuration also impacts the business applications. Company ABC and Company XYZ both implemented SAP as the primary business system and enabled the payables process with SAP. Company ABC has configured SAP to perform a three-way match, matching price, quantity, and date. It has set over and under tolerance levels of \$50 or 5 percent, whichever is lower. Company XYZ has configured SAP to perform “evaluated receipt settlement,” where the payment is automatically generated based on whatever was received, regardless of what was ordered or billed. No three-way match is performed, and no tolerance limits are established. Once again, although both companies are using SAP, the risks of each of those configurations are quite different, and the IT audits that should be performed at each company are also different.

#### An Array of Variables

Other variables that impact the snowflake theory are:

- Degree of system centralization.
- Degree of geographic centralization.
- Number of servers.
- Choice of infrastructure technologies.
- Degree of customization.
- IT department organizational structure.
- Versions of specific technology used (e.g. Windows 2000 versus Windows 2003).
- Degree and method of outsourcing.
- Corporate policies (e.g. saving all e-mails forever versus saving no e-mails).

The net result of all these variables is the snowflake theory: No two IT environments are alike. Therefore, it is very difficult — if not impossible — to take a checklist approach to planning and executing IT audits. Each company should have an entirely unique IT audit plan based on its specific IT risks.

The challenge, of course, is adequately identifying the business and IT risks specific to the organization’s particular IT environment. This is why the IT risk assessment process is critical, perhaps even more so than the overall risk assessment. Additionally, the risk assessment should be performed by knowledgeable resources — such as those who understand how the company’s usage of Active Directory will impact the IT audits that need to be performed.

### 4.2 Risk Evolution

The snowflake theory dictates that each company will have a risk profile that is unique to that organization only. However, there is another dimension of risk that is important to consider as well, and that is risk evolution. Risk evolution is based on Moore’s Law. Moore’s Law, which was initially proposed in 1965, states that every 18 months, the data density on an integrated circuit doubles. What this means pragmatically is that technology is increasing rapidly, which should come as no surprise to anyone.

Consequently, IT-related risk is not static. Given the high growth and expansion of technology, IT-related risks will change — sometimes dramatically — from year to year. It is even possible to have a situation where the IT audit schedule was based on an effective IT risk assessment process, but by the time the actual audits are to be performed, that risk profile had evolved, and the planned IT audits are no longer sufficient.

To combat this issue of IT-related risk evolution, the CAE should:

- Recognize the dynamic nature of IT-related risk and perform independent IT risk assessments every year.
- Develop an understanding of the IT department’s short-term plans for a given year and analyze how those initiatives may impact the IT risk assessment.
- Begin each actual IT audit by refreshing the risk assessment component of that particular audit.

- Be flexible with respect to the IT audit universe; monitor the organization's IT-related risk profile and be willing to adapt audit procedures as it evolves.

### 4.3 IT-related Risk Proliferation

A third dimension to consider when evaluating IT-related risk is the concept of proliferation, which refers to the additive nature of IT-related risks. Assume that the organization has identified IT risk A and IT risk B. Independently, each risk may be low, but when the two risk-related processes work together, they create IT risk C which is far greater than the sum of the individual risks.

Example: Company XYZ is running Oracle Applications. There is no process in place for monitoring system activity. Also, the system administrators all have full access to the system. Independently, each of these items represents risk, but together they represent a situation where a number of people can do whatever they want on the system (approve invoices, cut checks, set up new payroll accounts) with no detective checks and balances. In this case, understanding the IT management and monitoring processes, along with the specific security of the system, is important to understanding the true risk.

For this reason, it is important to consider IT-related risk holistically, rather than discretely. The CAE should consider IT-related risk at the enterprise level, assessing not just each individual risk, but also how the individual risks impact each other. Remember that the IT environment has layers. Imagine that one is trying to sift sand through a number of screens piled on top of each other. Although each screen has holes in it, the layers of screens will prevent any sand from getting all the way through. Now imagine that each screen has a small hole in it, directly aligned with a small hole in the layer beneath it. In this case, sand can fall all the way through the screens without impediment.

The world class CAE is always considering all the layers of the IT environment when planning or executing IT audits. Evaluating the impact of risks at one layer against risks at other layers is very important when performing the IT risk assessment.

### 4.4 Types of IT-related Risks

The first step in understanding the risks associated with IT is to identify what can go wrong, including:

- Availability – when the system is unavailable for use.
- Security – when unauthorized access to systems occurs.
- Integrity – when the data is incomplete or inaccurate.
- Confidentiality – when information is not kept secret.
- Effectiveness – when the system does not deliver an intended or expected function.
- Efficiency – when the systems cause a sub-optimal use of resources.

The various IT-related risks generally can be grouped into two main categories: pervasive risk and specific risk.

#### Pervasive Risk

Certain IT-related risks are not limited to one specific system or process. These risks impact the enterprise as a whole, and therefore are referred to as pervasive risks. Example: Company XYZ is connected to the Internet and does not maintain a firewall. What account balance does that impact? Potentially all account balances or potentially no account balances. Another example might be the presence of water sprinklers in the data center. If those accidentally go off and douse all the servers with water, which operational processes would be impacted? It could be all processes, no processes, or anything in between.

#### Specific Risk

Specific risk, on the other hand, can be attributed directly to a specific process or account balance. Consider the three-way match configuration settings mentioned in the introduction of this guide. If those settings are set incorrectly, the risk will specifically relate to payables and cash.

CAEs often struggle with the fact that pervasive risks represent far greater risks to the enterprise than specific risks. However, it is very difficult to quantify a pervasive risk. Moreover, when reporting a control deficiency related to a pervasive risk, it is far more difficult to link it to the business impact due to the deficiency.

The importance here is balance. The CAE should remember that both pervasive and specific risks are important and focus audit attention on both types of risk. If a review of the planned IT audit universe doesn't reveal audits that cover both kinds of risk, it is likely that the IT audit universe will not cover the organization's risks adequately.

### 4.5 IT Risk Assessment

The auditor should use an appropriate risk assessment technique or approach in developing the overall plan for the effective allocation of IT audit resources. Risk assessment is a technique used to examine auditable units in the audit universe and select areas for review that have the greatest risk exposure. The risks associated with each IT layer cannot be determined by reviewing the IT-related risks in isolation, but must be considered in conjunction with the organization's processes and objectives.

#### Impact Versus Likelihood

The assessment of IT-related risk must also consider the impact and likelihood of occurrence. The impact of IT-related risk events is often high, particularly for pervasive risks. Likelihood may be harder to determine because it is a prediction value (e.g. What is the likelihood that a hacker will break into the organization's Web site?). Past experience and general best practices may be used to support these estimates. The product of impact and likelihood helps to define the severity of the risk, which provides a basis for comparing and prioritizing IT-related risks.

Consider Company XYZ, which has implemented Windows 2003. Should this be audited as part of this year's IT audits? The answer, like many other answers regarding IT, is "It depends." In this case, there are multiple factors impacting the decision. The key consideration is the risk to the business and the impact the technology has on the operations of the organization. If the only application running on Windows 2003 is the application that updates zip codes when the post office changes them, then clearly the technology has very little impact on the overall integrity of the organization's operations. Consequently, it would be a waste of IT audit resources to bother auditing this system. Conversely, if the organization's primary supply chain systems run on Windows 2003, then the technology definitely impacts the achievement of the organization's objectives and should be included in the IT audit plan.

Many times, though, the answers are not quite so self evident. It is for this reason that an effective IT audit function is highly dependent on the performance of a robust IT risk assessment. The IT risk assessment helps address the issues posed by the snowflake theory and allows organizations to determine which areas warrant audit attention.

### Traditional Risk Assessments Aside

It is important to note that traditional risk assessment processes and activities may not support an effective IT risk assessment. These processes and tasks should be re-engineered to address the needs of an IT risk assessment adequately. Specifically, most legacy risk assessment processes are highly interview-based. Interviews alone are likely insufficient to assess IT risk, because a good deal of the IT risk is based on how technology is configured specifically at the organization. Moreover, a good part of risk in the IT arena is dictated by emerging issues. For example, assume a hacker discovers a new flaw in Windows 2003 and builds a tool that exploits this flaw. Microsoft identifies the issue and releases a patch that removes the flaw. An IT auditor would likely need to understand information about what patches have been installed before they could adequately assess the true risk around that technology.

### Static Versus Dynamic Risk

In Section 4.4, consideration was given to the concept of pervasive versus specific risk. Understanding those dynamics is important. However, when performing an IT risk assessment, it's also important to consider static versus dynamic risk.

**Static Risk** – Static risk does not change from year to year and is typically driven by the industry within which the organization operates. For example, Company XYZ is an online retailer of books and has risk associated with its Web servers that run the online ordering system. If those servers go down, the company's revenue stream is shut down until the servers come back up again.

When assessing static risk, inquiry and interview techniques are, in many cases, adequate. Also, these assessments tend to need a little updating each year, based on new conditions, but generally hold true year after year. Unless Company XYZ decides to get out of the online book business and open up a brick-and-mortar solution, the Web servers will continue to be an area of high risk.

**Dynamic Risk** – Dynamic risk is risk that is constantly changing. It tends to be less driven by the industry and more driven by the evolution of technology (remember Moore's Law). The discovery of a new flaw in Windows 2003 is a great example of a dynamic risk. Last year's risk assessment would not have identified that risk; it didn't exist at that time. Dynamic risk also impacts how the IT risk assessment process should be conducted. In this case, the IT risk assessment process should be focused on the process that IT management has in place to monitor patches and measure their timely implementation.

Legal and regulatory issues are also large dynamic risks. These issues impact all areas of the business, but given the evolution of technology, there are far greater new legal and regulatory issues relating to technology that arise each year. Consider, for example, all of the new rules and regulations relating to the privacy of consumer information that have been promulgated in the recent past.

### Assessing Dynamic IT Risk

When performing an assessment of dynamic IT risk, inquiry procedures alone are probably insufficient. There are two key steps that must be taken: discovery and analysis.

**Discovery** – Discovery is the process of determining which technologies have been deployed, how they have been configured, and what business processes they support and align with. In many cases, tools are used to support the discovery process. For example, an organization with a decentralized IT function may not know how many servers and versions of operating systems are in use enterprise-wide. A network discovery and mapping tool could help gather this data quickly and accurately.

**Analysis** – Analysis is based on the evaluation of the data once it has been collected. Once again, this would likely not be driven via inquiry procedures, but would be more based on the IT auditor analyzing the collected data against emerging issues and new technology risks.

One other concept that emerges in the analysis phase is the concept of risk dependency. This concept was touched on earlier using an analogy of sifting sand through a pile of screens (Section 4.3 IT-related Risk Proliferation). If there is a hole in each screen, then sand could fall all the way

through them. This is the essence of risk dependency. The impact of a given risk may depend on the presence of other risks. For example, Company XYZ has not segregated the corporate network and is using a number of wireless networks. The engineering team electronically collaborates on design documents for new products. In this case, the business risk is that a competitor could sit outside with an antenna and gather information on new product designs. This risk is created by the combination of network design, process design, and new technology, and each risk is dependent on the existence of the other two risks. The total risk is greater than the sum of each individual risk.

It is for this reason that many organizations utilize a “layers of defense” strategy, which provides multiple layers of security and control. It is important that during the analysis process, the CAE evaluates the design and effectiveness of all the layers of defense before concluding on the impact of an IT risk or weakness.

#### **Robust IT Risk Assessment**

Given these issues, the CAE should plan accordingly and ensure that the IT risk assessment process:

- Is performed in depth every year and isn't just an update of the prior year.
- Considers all the layers of the IT environment.
- Considers both static and dynamic risks.
- Is not strictly based on interviews, but uses other discovery techniques.
- Is supplemented with the appropriate level of analysis after discovery.
- Is performed by the appropriate personnel.

This last bullet is one that may pose one of the larger challenges to CAEs, because IT is a very broad term and comprises many layers. The skills required to understand each layer are dramatically different. A networking specialist with deep technical skills has a very different skill set than an SAP application specialist with deep technical skills. To perform an effective IT risk assessment, specialists who understand all layers of the IT environment need to be involved. These are rarely, if ever, evident in a single person. What is far more likely is that a team of IT audit specialists with skills across all layers will need to be involved. This team will also have to work together closely through the process, primarily because of the issue of risk dependency.

Once the IT risk assessment has been performed with the appropriate level of accuracy, the next step is to determine which IT audits should be performed. If the IT risk assessment was performed effectively, the organization should have a reasonable idea of what IT risks exist. However, this also poses a number of challenges, not the least of which is defining IT audits.

In the previous example (page 8), the company had identified a business risk of transmitting important product design information outside of the organization. What audit should be performed to address this risk? Should an audit of wireless networks be performed; an audit of network architecture and design; or an application review of the electronic design application? And if the audits are broken up in that fashion, the odds are that the reporting of audit findings will be related to technical settings for each individual technology. That's fine, but the audit committee likely does not care about detailed technical settings and probably wants IT audit findings to be tied to the business issues.

Consequently, the way in which IT audits are defined plays a large role in the overall effectiveness of the IT audit function. This is exacerbated by the need for the IT audit function to integrate with the process/operational/financial auditors and the procedures they are performing, particularly in environments with large integrated ERP applications, where a high number of key process controls are contained with the systems.

Although there is no right way to define IT audits, there are certainly degrees of wrong. For example, many CAEs make the mistake of scoping an "IT general controls" audit. This is so broad that it's almost meaningless, especially in a large organization. Are telephone switches included? How about desktop configuration? Environmental controls in the data center? All of the above? If so, the audit will require a substantial amount of time to complete.

### 5.1 Tips for the CAE

The challenge is to provide the right level of granularity in the definition of the IT audit universe so as to make it effective and efficient. This will be different for every IT audit function (an extension of the snowflake theory), but some considerations for the CAE when defining IT audits are:

- **Using overly broad definitions for IT audits (e.g. IT general controls) will almost ensure that there will be scope creep in audit procedures.** Furthermore, there may also be a gap between what management thinks is being audited and the true audit procedures being performed. For example, Company XYZ implements SAP for financial accounting processes. The IT audit function performs a post implementation review of accounts payable configurable controls, but calls it an "SAP post implementation review." After the audit, the company has a major issue with the SAP user security setup. The audit committee is likely to ask why that wasn't caught in the SAP post implemen-

tation review. This answer is that wasn't evaluated. But the nomenclature of the audit was deceiving. With that in mind, CAEs should make sure that the definition of each IT audit is a fair and accurate description of what is being reviewed.

- **The audit universe for the year should touch on all the layers in the IT environment.** Although each IT environment is different, the layers tend to be the same. If the IT audit plan does not include some review for each of the layers, odds are that the plan, as a whole, is deficient.
- **IT audits should be structured in such a way as to provide for effective and logical reporting.** Application reviews, for example, are rarely optimally effective when they are broken out independently (e.g. an Oracle accounts payable review). Applications should be integrated from an execution and reporting process with process/operational/financial audits. IT audits of pervasive technologies (e.g. networks, processes, etc.) tend to be more effective when audited at the enterprise level. In other words, don't perform a network audit at the Pittsburgh facility and another network audit at the Phoenix facility. Perform one enterprise network audit. Geography matters less than process.
- **IT audits should cover the appropriate risks.** In many cases, IT audit budgets are determined before the IT risk assessment is performed. This inevitably leads to one of two situations:
  1. An inadequate number of audit hours is spread over too many audits, which results in consistently poor quality IT audits because there is not enough time to do any of them correctly.
  2. Audits that should be performed are not performed because the budget does not allow for them to be performed.

IT audit planning and budgeting should be an outcome of the IT risk assessment process, not done before the IT risk assessment. Also, the IT risk assessment should be considered in the context of the risk assessment for the company as a whole. It may well be that in a particular organization, the IT environment presents so much risk to the company that all internal audit procedures performed for the year should be IT audit procedures — a hyperbolic situation to be sure, but not unfeasible.

### 5.2 Budgeting for IT Audit

One of the common mistakes a CAE makes when defining the IT audit universe is underestimating the amount of time required to do an IT audit. The issue, in many cases, is the snowflake theory. Example: Company ABC is running a financials application on an AS/400. The IT auditor wants to assess the security around the AS/400, and he or she spends 100 hours performing the review. Company XYZ is also running a similar application on an AS/400. Should the review take the same amount of time?

The answer, of course, is that it depends. If Company ABC has 100 users and Company XYZ has 1000 users, it may be more appropriate to assume that it would take 10 times longer for Company XYZ, if the audit must evaluate all users. If the audit approach is to merely evaluate the access rights of a sample of 10 users, then the audits might take the same amount of time, but would offer different levels of assurance.

That example illustrates the danger of estimating IT audit budgets. It is easily possible to misjudge the effort required by orders of magnitude, which is not usually seen on the operational or financial side of the audit house. Those estimates may be wrong, but not by orders of magnitude.

Another example might be the audit of an SAP system. A security review of an SAP system with two production clients will take twice as long as a security review of an SAP system with one production client. Woe betides the CAE who estimated the budget without fully understanding the IT environment (refer to the IT risk assessment section). If estimates had been generated without knowing how many production clients there were, the budget estimates could be significantly incorrect.

How should a CAE address this issue? Certainly one crucial element is understanding the IT environment, which should naturally evolve from performing an adequate IT risk assessment. Another critical component is accurately estimating the time required to perform IT audit tasks. Certain IT audit tasks, such as reviewing a configuration setting, may be done quickly and efficiently. Other tasks, such as auditing a complicated user security architecture, may take a substantial amount of time. Tactically, a CAE should challenge the budget estimates on planned audits, ensure that enough front-end planning has been done to justify an estimate, and ensure that IT audit staff and management concur with the estimate. Be aware that under very few circumstances can an IT audit of fewer than 80 hours be effective for any technology.

## GTAG – Executing IT Audits – 6

The process for executing an IT audit is, in theory, no different than the process for executing an operational audit. The auditor plans the audit, identifies and documents controls, tests the design and operating effectiveness of the controls, concludes, and reports. Because most CAEs are familiar with this overall process, it will not be covered in detail in this GTAG. However, there are certain elements of an IT audit that do vary somewhat from more traditional audits. Therefore, this section will identify some of those areas and provide CAEs with some perspective and ideas on how to manage them. See Figure 2, Audit Process Overview, below.

### 6.1 Frameworks and Standards

One challenge auditors face when executing an IT audit is knowing what to audit against. Many organizations have not fully developed IT control baselines for all applications and technologies. The rapid evolution of technology would likely render any baselines useless after a short period of time.

The snowflake theory dictates that each IT environment is different. However, this does not detract from the concept of control objectives. Control objectives, by definition, should remain more or less constant from environment to environment. Consider the objective that all critical business data and programs should be backed up and recoverable. Now, each environment may do that very differently; backups could be manual, or automated, or a tool can be used. They could be incremental only, or there may be complete backups of everything. Backups could be done daily, weekly, monthly, etc. Storage of backups could be onsite in a fireproof safe, offsite at another company facility, or outsourced to a third party. The method used by the organization to manage backups would certainly impact the audit procedures and the budget for the audit, but the control objective would not change. Given this, a CAE should be able to start with a set of IT control objectives, and although it would not provide 100 percent specificity to that particular environment, select an appropriate framework.

### COSO and COBIT

Where can a CAE find a comprehensive set of IT control objectives? The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) *Internal Control–Integrated Framework* and *Enterprise Risk Management – Integrated Framework* are excellent sources of information, but are not focused on IT. Moreover, IT has greatly evolved since 1992, when the initial COSO framework was published, which makes the COSO IT control objectives less effective in managing today's technologies. A COSO-based control environment should be augmented with more detailed IT control objectives to assess the IT control environment effectively. A number of options are available for this.

One IT control framework is *Control Objectives for Information and related Technology* (COBIT), which was originally published by the Information Technology Governance Institute in 1994, with the support of the Information Systems Audit and Control Association (ISACA). Version 4.0 of COBIT was released in November 2005. COBIT is not intended to compete with the COSO frameworks, but it can be used to compliment them by augmenting them with more robust IT-specific control objectives. COBIT 4.0 contains 214 detailed IT control objectives organized around 34 IT processes. Clearly, COBIT provides a more detailed approach than COSO's internal control or ERM frameworks, which provide a good starting point for identifying control objectives relevant to the environment being audited.

### Policies, Standards, and Procedures

A framework such as COBIT offers a generally accepted set of IT control objectives that helps management to conceptualize an approach for measuring and managing IT risk. Management would generally use such a framework to guide the development of a comprehensive set of IT policies, standards, and procedures.

For example, a functional IT control framework would typically include a control objective on securing information systems from unauthorized access. An organization could accomplish this objective by defining a policy that specifies

### Audit Process Overview



Figure 2 – Audit Process Overview

that all production systems must be accessed by a unique user ID and password. This policy would then be augmented by an organizational standard that defines the ID and password requirements (e.g. IDs are the first letter of the user's first name, followed by their last name; passwords must be at least eight characters long and contain a mix of letters and other characters; etc.). Such a standard would then be augmented by procedures that would define how the standards are implemented on a platform-by-platform basis and would specify the “evidence of control” created and retained via successful performance of the procedure. This cascading approach from control framework to policy, standard, and procedures is the essence of ensuring that IT controls correspond effectively to the business and the enterprise control environment.

Assume that in the example above, the organization has not defined a standard that provides specifics around password length, etc. In that case, the CAE will face some challenges in determining what to audit against, and will often end up engaged in a debate with IT management over what constitutes a sufficient control. Which is more secure: a password with a minimum length of six characters that expires every 30 days, or a password with a minimum length of eight characters that expires every 90 days? There are often references made to “best practices” but a specific link is not always drawn.

In the absence of organization-specific IT control standards, there are various public marketplace and industry IT control standards. These can help support IT audit procedures by offering a set of “best practice” recommendations where specific details are laid out (e.g. password must be at least eight characters and must be set to expire every 60 days). An IT auditor can use these standards as a baseline to audit against. This is also useful when reporting deficiencies, as it takes the subjectiveness out of the deficiency. Compare “Password security can be enhanced” with “Passwords do not conform with ISO27001 information security standards.” Obviously, the second wording will invite less debate.

The challenge with using public standards to audit against is that there are a lot of different standards, and they do not always recommend the same thing. The purpose of this GTAG is not to debate the merits of various standards, but simply to encourage the CAE to consider supporting IT audits by using a standard — whichever standard makes the most sense for the organization and is acceptable to IT management. In most cases, a standard relates to a very specific element of the IT environment, such as security or custom program development. In most cases, the CAE is not in a position to dictate the specific standard used by the organization. This decision should be made by IT or executive management. If a standard already has been agreed upon and deployed, the CAE should identify that standard and audit against it. The CAE also has an obligation to assess the overall sufficiency of the standards chosen by IT management to ensure they are responsive to the organization's risk profile, business requirements, and regulatory requirements.

### Six Sources for Standards

Some standards for consideration are:

**ISO27001 / ISO17799** – The International Organization for Standardization published this internationally recognized generic information security standard, which began as a British Standard (BS7799), evolved into an ISO standard (ISO17799), and is now known as ISO27001. It contains generally accepted best practices on information security management and is useful as a baseline for IT auditors to audit against. <http://www.iso.org>

**Capability Maturity Model Integration** – Carnegie Mellon University's Software Engineering Institute (SEI) has published Capability Maturity Models (CMMs) for various processes within an organization, primarily related to the deployment of software. Examples include Systems Engineering CMM and Software Acquisition CMM. These CMMs provide a model for building sustainable controlled processes within an organization and are useful to IT auditors performing audits of system development processes. In 2005, the SEI integrated the existing CMMs into the Capability Maturity Model Integration (CMMI). <http://www.sei.cmu.edu/cmml/general/general.html>

**National Institute of Standards and Technology (NIST)** – The Computer Security Resource Center is a division of NIST that provides a comprehensive series of publications that offer detailed information on information security control topics. Sample publications include *Biometric Data Specification for Personal Identity Verification and Guidance for Securing Microsoft XP for IT Professionals*. These standards, a must-have for any IT auditor working in the public sector or in the aerospace and defense industry, provide best practices that can be used in other industries as well. <http://csrc.nist.gov/publications/nistpubs/index.html>

**SysAdmin, Audit, Network, Security (SANS) Institute** – One of the most trusted sources for information security education and training in the world (and by far the largest), the SANS Institute publishes numerous documents on various aspects of security for various technologies. SANS publications provide a number of specific requirements that an IT auditor can audit against. <http://www.sans.org/aboutsans.php>

**The IT Infrastructure Library (ITIL)** – Supported by the British Standards Institute, ITIL provides best practices for supporting IT services. ITIL publications are focused on supporting the management of IT services. As such, they are a valuable support tool for an internal auditor performing any audits of the IT management layer. <http://www.itil.co.uk/>

**Vendor-specific Standards** – Many technology vendors issue security and control guidelines for the technology they produce. SAP, for example, issues a three-volume

security guide that provides detailed recommendations for securing and controlling the SAP ERP application. These vendor-released standards often do not take security and control considerations to the same level that perhaps a NIST publication might, but they provide a good start. They may also help limit debate around findings (e.g. “SAP password restrictions are not set in accordance with vendor-documented security requirements”). CAEs should check with the vendors of mission-critical systems to see if specific standards are available. In many cases, the vendor may not have released anything, but the user group associated with that technology has (e.g. Americas’ SAP Users’ Group).

### 6.2 IT Audit Resource Management

The resources assigned to execute planned audits play a critical role in the efficiency and effectiveness of the audits. IT encompasses a wide range of technology — the skill set needed to audit a firewall configuration is vastly different from the skill set needed to audit accounts payable three-way match configuration tables in Oracle Applications. It is critical to match the skills needed to perform a particular IT audit with the appropriate IT auditor.

One of the challenges today’s CAEs face is identifying, hiring, and retaining competent IT audit professionals. Inevitably, any discussion on this topic will coalesce around the issue of hiring an IT person and teaching that person how to audit versus hiring an auditor and teaching him or her IT. There is no perfect solution, and there will always be exceptions, but directionally, the CAE should consider that no IT auditor will be able to do all IT audits. Thus, any IT audit function will need to have some IT auditors more aligned with applications and some IT auditors more aligned with infrastructure technologies. In terms of sourcing IT auditors who will be more aligned with applications, generally it is more effective to find financial, process, or audit people and teach them a particular application. In terms of sourcing IT auditors who will be more aligned with auditing infrastructure technologies, generally it is more effective to hire IT people and teach them how to audit. Consequently, a CAE who has a strong understanding of the current IT audit universe and the current IT audit skill sets on staff should be able to focus his or her recruiting efforts accordingly.

#### IT Auditor Retention Strategy

Once IT auditors have been hired, the next key challenge is retention. IT auditors tend to be more mobile than traditional auditors due to the current lack of skilled IT auditors in the marketplace. One way for a CAE to address this issue is to improve compensation. In many cases, budgets do not allow for this; therefore, the CAE may need to be creative when devising a retention strategy.

Many IT auditors are motivated by exposure to technology. They enjoy playing with new and exciting technologies.

Below are some areas in which the CAE can support retention goals by leveraging the IT auditor’s desire for technology exposure:

**Certifications** – There are a number of technology certifications available. These include technical certifications — such as various certifications in Cisco routers and database technologies — and certification in specific modules of SAP. ISACA offers a Certified Information Systems Auditor (CISA) certification. ITIL Foundation Certification provides a basic understanding of the various ITIL processes for service management and service delivery. This is a must for IT auditors reviewing IT departments using ITIL processes.

The CAE may want to consider bonuses that are tied to specific “hot skills” certifications — i.e. an IT auditor receives a bonus for becoming a Cisco Certified Network Associate (CCNA). This allows the organization to provide additional compensation without raising base salaries. Moreover, many certifications take a fair bit of time to accomplish, which ensures that an IT auditor will stay at least the length of time required to get certified. A word to the wise, however, sometimes IT auditors will be collecting IT certifications to move out of the audit function. It is necessary to carefully examine whatever certifications the IT auditor wishes to pursue and make sure that those fit within the scheduled IT audit universe.

**Rotation** – Consider a rotation program between the IT department and the IT audit function. This can help increase IT audit capacity, as well as strengthen auditing’s relationships with the IT department. Be aware of potential independence concerns when deploying this type of strategy. Also, be sure that the IT audit function can provide some audit expertise to the deployed IT “rotatees.”

**Continuing Education** – IT auditors will need more training than process or operational auditors. There have been relatively few quantum leaps in three-way matching processes in the last 10 years, but there certainly have been great strides in IT. For IT auditors to stay abreast, they need to be trained early and often. The CAE should recognize this and build a training strategy for the department that considers the needs of the IT auditors. Consideration should be given to developing expertise in a broad range of important topics. This can be accomplished by assigning certain IT auditors to become subject matter experts in a given technology (e.g. one IT auditor is the Microsoft specialist, another is the database specialist, and a third is the SAP specialist). This will provide for better audits than if all IT auditors are trained in all subjects. However, it requires more diligence and planning when constructing an IT audit training plan for the year.

**User Groups** – Most technology vendors maintain a user group, which consists of customers who use the

technology and get together to share ideas, concerns, and hopefully influence future developments of the technology. Although traditionally user groups have been the domain of IT professionals and business users, in many cases, these groups can be valuable to the IT auditor as well. The Americas' SAP Users' Group, for example, maintains a subgroup that is focused on security and controls. IT auditors should seek out the user groups for the critical technologies used by the organization and join them. In many cases, there may be no incremental cost to the organization. Most user groups are managed by company; all employees of the company are welcome to join.

### Adequate Staffing

Many IT audit functions have budgetary constraints that prevent them from maintaining a staff with the range of IT audit skills needed to audit the IT audit universe effectively. The organization would not expect the IT department to operate without on-staff expertise in operating systems, databases, networks, and application systems. Yet, it sometimes expects the IT audit function to operate without sufficient resources. Inevitably, this leads to auditing by checklist and using inquiry techniques as the primary source of audit evidence. As indicated throughout this document, for an IT audit function to be effective, a specific audit plan must be driven by a robust risk assessment and backed up with audit procedures that are designed specifically to the nuances of that particular environment. The CAE should justify the budgetary need to support a range of IT audit skill sets to senior management and the audit committee.

One primary reason for the CAE to advocate sufficient resources stems from Paragraph 140 of the U.S. Public Company Accounting Oversight Board's Auditing Standard No. 2, An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements, which states:

"... the following [circumstance] should be regarded as at least a significant deficiency and as a strong indicator that a material weakness in internal control over financial reporting exists ... The internal audit function or the risk assessment function is ineffective at a company for which such a function needs to be effective for the company to have an effective monitoring or risk assessment component, such as for very large or highly complex companies."

The absence or limited presence of an IT internal audit function in an organization with a large or complex IT environment could present a situation in which the organization's external auditor could conclude that Paragraph 140 may apply.

In some circumstances, the CAE may want to explore the possibility of co-sourcing some or all of the IT audit function. Most CAEs understand the pros and cons of co-sourcing; this

guide is not meant to be a primer on it. However, CAEs generally struggle with how much to co-source and what IT audits to co-source. The optimal mix varies from organization to organization (the snowflake theory applies again), but CAEs may find it useful to benchmark their organization against the following data from The Institute of Internal Auditors' (IIA's) 2004 Global Audit Information Network (GAIN) report:

- 39 percent of all purchased internal audit services are IT audit related.
- Percentage of IT audit work outsourced:
  - 8.1 percent of organizations outsource 100 percent of their IT audit work.
  - 7.1 percent of organizations outsource most of their IT audit work.
  - 8.3 percent of organizations outsource between 25 percent and 50 percent of their IT audit work.
  - 33.1 percent of organizations outsource "some" of their IT audit work.
  - 41.6 percent of organizations do not outsource any of their IT audit work.
- Strategy for the next three years:
  - 18.9 percent of organizations plan to increase their IT audit outsourcing.
  - 64.9 percent of organizations plan no changes to their amount of IT audit outsourcing.
  - 13.3 percent of organizations plan to decrease their IT audit outsourcing.

Additional suggestions with respect to co-sourcing include:

**Co-source the Technical Audits** – In this case, "technical audits" refers to audits that are performed in the technical infrastructure and application layers of the IT environment. Generally, these audits require a much higher level of specific technical expertise, which is more likely to be found in the marketplace than internally. IT audits of the management layer are much more focused on IT processes (e.g. systems development) and therefore require less in-depth technical skills.

**Consider Using Two Providers** – It may be useful to maintain contracts with a primary provider of co-sourced services as well as a secondary provider. In certain cases, one firm may have conflict of interest in a potential audit for some reason; it may be useful to have a backup provider waiting and ready to step in. A word of caution: the primary provider should perform at least 80 percent of the co-sourced activities. Anything less than that and the drop in efficiency (e.g. twice as many meetings and increased administrative overhead) will outweigh the benefits. To ensure that the providers learn the organization's business well and treat the organization as an important client, no more than two firms should be used. If Firm ABC

## GTAG – Executing IT Audits – 6

---

provides most or all of the IT audit services to an organization, it will have a different relationship with the organization than if Firm ABC is one of two or three firms providing 30 percent of the IT audit services to the organization.

**Co-source Globally Distributed Audits** – Most firms maintain employees in all major global regions, and many firms operate on different pricing structures for local resources. Thus, if an organization wanted to audit its operations in Kuala Lumpur, it may be able to use a firm with local Malaysian resources at a reduced cost, as opposed to sending resources to Malaysia. The one exception to this recommendation is when the internal audit charter dictates that the internal audit function provide a certain amount of consultative services to the business units around controls. In such a case, it may be more useful to have one team audit around the globe so that internal best practices can be observed by the team and shared among business units.

As noted above, IT audit budgets can be difficult to estimate and manage. CAEs should look for opportunities to use accelerators — tools and/or techniques that help support the procedures IT auditors will be performing — to increase the efficiency and effectiveness of the audit. CAEs can use an accelerator to do the same audit in less time or do more detailed audit procedures in the same amount of time.

Many audit accelerators require an investment, so the CAE should carefully consider the cost/benefits of any solution prior to investing in an accelerator. Audit accelerators can be divided into two general categories: audit facilitators, which help support the overall management of the audit (e.g. an electronic workpaper management tool), and testing accelerators, tools that automate the performance of audit tests (e.g. data analysis tools).

## 7.1 Audit Facilitators

### Electronic Workpapers

Although not specific to just IT audits, electronic workpaper management can be very useful. These solutions provide centralized management and retention of workpapers, audit workflow, version tracking, electronic sign off, etc. There are a number of vendors in the marketplace that offer these tools. It's important to consider the functionality of the tool. For example, can it support multiple simultaneous audits? Prior to implementing any tool, the audit functional requirements should be defined. Perhaps more important, however, is the content that is provided with the tool. Does it contain suggested audit procedures or control activities? CAEs will certainly need to customize whatever knowledge base is included with the tool, but it can provide a significant head start.

### Project Management Software

Not specific to auditing necessarily, project management software schedules work plans, assigns responsibility for tasks, tracks project milestones and deliverables, and can be used by the IT audit function to provide additional consistency and reporting in IT audits. Project management software is currently used by 35 percent of 2004 GAIN survey respondents.

### Flowcharting Software

Software that can graphically document transaction flows, control points, and key process steps is very useful — almost necessary — when documenting process walkthroughs, particularly for Sarbanes-Oxley compliance purposes. Storing graphical process documentation electronically supports the ease of updating flowcharts as processes change and provides for easy storage and sharing. Flowcharting software is currently used by 59 percent of 2004 GAIN survey respondents.

### Open Issue Tracking Software

This software allows for tracking of outstanding audit issues or deficiencies and is often integrated with document management software, especially those designed for Sarbanes-

Oxley compliance purposes. Functionality typically includes the ability to assign responsibility for remediation procedures, assign due dates and deliverables, and track and report on progress. Open issue tracking software is currently used by 47 percent of 2004 GAIN survey respondents.

### Audit Department Web Site

A number of audit departments have established departmental Web sites. These are generally intranet-based, but can be Internet-based. Internet-based solutions offer global sharing of information across organizations, but raise confidentiality concerns. Either type of solution provides an internal audit function with the ability to have central information sharing and communication. These solutions can be custom-developed or purchased from vendors. Audit department Web sites are currently used by 42 percent of 2004 GAIN survey respondents.

## 7.2 Testing Accelerators

Testing accelerators can automate time-consuming audit tasks, such as reviewing large populations of data. Also, using a tool to perform audit procedures helps establish consistency. For example, if a tool is used to assess server security configuration, all servers tested with that tool will be assessed along the same baselines. Performing these procedures manually allows for a degree of interpretation on the part of the IT auditor. Lastly, the use of tools enables IT auditors to test an entire population of data, rather than just a sample of transactions. This provides for a much higher degree of audit assurance.

CAEs should be aware of the following considerations with respect to IT audit accelerators:

- Tools cost money. The CAE should be sure that the benefits outweigh the costs before embarking on any tool implementation.
- The IT auditors will need to be trained on the new tool. It is not uncommon that a tool sits unused in an internal audit department because no one knows how to use it. This clearly reduces the return on investment of any tool.
- The tool will also need support, patch management, and upgrades. Depending on the tool, it may require a standalone server as well. For this reason, any tool selection should be managed with the IT department's assistance.
- In some cases, IT management or third-party service providers may not allow the tools to access the production environment directly. Any use of tools and/or scripts should be thoroughly discussed with, and approved by, IT management and be tested fully before deploying.

### Data Analysis Software

These tools allow an IT auditor to perform robust statistical analysis of large data sets. They can also be used to support

process or operational audits (e.g. accounts payable fraud reviews), and they can support many types of testing, such as Benford's analysis, cumulative sampling, etc. One consideration when using a data analysis tool is that it may be difficult to extract the data from the original source. It is critical that audit procedures be performed to ensure the completeness and accuracy of the source data. Some of the key vendors in this arena are:

- ACL: <http://www.acl.com/Default.aspx?bhcp=1>
- Idea: [http://www.audimation.com/product\\_feat\\_benefits.cfm](http://www.audimation.com/product_feat_benefits.cfm)
- Monarch: <http://monarch.datawatch.com/>
- SAS: <http://www.sas.com/>

### Security Analysis Tools

These are a broad set of tools that can review a large population of devices and/or users and identify security exposures. There are many different types of security analysis tools, but generally they can be categorized as follows:

**Network Analysis Tools** – These tools consist of software programs that can be run on a network and gather information about the network. Hackers would typically use one of these tools on the front end of an attack to determine what the network looked like. IT auditors can use these tools for a variety of audit procedures, including:

- Verifying the accuracy of network diagrams by mapping the corporate network.
- Identifying key network devices that may warrant additional audit attention.
- Gathering information about what traffic is permitted across a network (which would directly support the IT risk assessment process).

A list of the top 75 tools can be obtained at [www.insecure.com](http://www.insecure.com).

**Hacking Tools** – Most technologies have a number of standard vulnerabilities, such as the existence of default IDs and passwords or default settings when the technology is installed out-of-the-box. Hacking tools provide for an automated method of checking for these standard vulnerabilities. Such tools can be targeted against firewalls, servers, networks, and operating systems. Many provide for plug-and-go usage; the IT auditor plugs in a range of what it wants the tool to search for, leaves, and comes back in a few hours, or the next day. By then, the tool has developed a report of all vulnerabilities identified in that range.

These tools are important for an IT auditor to run for several reasons, not the least of which is that these are the tools that a hacker would use to mount an attack against the organization. The organization should at least have the same information that a hacker would have. It's important to note that some of these tools are potentially dangerous to run, because they can impact the integrity of the systems they are scanning. The IT auditor should

review the planned usage of any of these tools with the security officer and coordinate the testing with IT management to ensure the timing of testing will not impact production processing. In some cases, the security officer or systems administrators may already be running some of these tools on a regular basis as part of the systems management processes. If so, the results may be able to be leveraged to support IT audits, if properly designed and executed. A list of the top 75 tools can be obtained at [www.insecure.com](http://www.insecure.com).

**Application Security Analysis Tools** – If an organization is using any large integrated business application (like an ERP system such as SAP or Oracle), many of the key internal controls are highly security dependent. For example, perhaps Company XYZ has a corporate policy that all checks over \$10,000 require management approval before issuing. That's certainly a good control. Now, assume that Company XYZ has configured its Oracle system so that any check created over \$10,000 automatically is placed in a holding queue for someone to approve and release. This example is another solid use of IT controls to support corporate policies. Now, assume that all users on the Oracle system have full access to the system. Obviously, any user could go into the holding queue and approve and release the check. It is for this reason that application level security must be well designed and built in conjunction with the application's processes and controls. Also, this is an example of why any type of audit (financial, process, operational, or IT) in a large integrated application environment needs to include a user security component to be effective.

Unfortunately, building functionality to support application user security audits is not necessarily a priority for many vendors, who tend to be more operationally focused. Consequently, it is often extremely cumbersome and time-consuming to perform application user security audits. These audits may be accelerated by using an application security analysis tool, many of which tend to be specialized for various application systems (PeopleSoft, SAP, or Oracle) and analyze user security against preconfigured rules. These tools may also evaluate segregation of duties within the application. The CAE should be aware that most of these tools come with a set of preconfigured rules or vendor-touted "best practices." Due to the snowflake theory, any implementation of one of these tools will need to be accompanied by a substantive project to create a rule set that is relevant for that particular organization. Failure to do so will result in audit reports that contain a number of either false-positives or false-negatives.

Some key vendors in this arena are:

- Approva: <http://www.approva.net/>
- LogicalApps: <http://www.logicalapps.com/>
- Virsa: <http://www.virsa.com/>
- Q Software: <http://www.qsoftware.com/index.htm>
- Control Solutions International:  
<http://www.csi4sap.com/en/home/>

IT auditing has been around for many years. However, it is constantly evolving and changing. Consequently, the CAE must continually adapt and evolve the IT audit approach and the IT audit universe to perform IT audit procedures that are needed to meet compliance requirements adequately and help manage the overall business risk of the organization.

Although this guide does not have all the solutions and, in some cases, may raise more questions than it answers, hopefully the CAE can use it as a tool to assist with this evolution. The following questions are provided to help CAEs as they consider these issues in the context of their organization:

- Has the organization clearly defined what IT means in their particular organization? Are the chief information officer's areas of responsibility documented? Does the IT audit approach consider all of those areas when evaluating risk and defining the IT audit universe?
- Does the audit function perform an effective IT risk assessment annually? Are knowledgeable specialists in infrastructure technologies, application systems, and IT processes all involved in that assessment?
- Does the IT risk assessment consider the specific technological architecture and configuration employed by that organization?
- How are IT risks quantified? Are both impact and likelihood of occurrence estimated? What industry benchmarks and best practices are used to support these estimates?
- Does the IT audit universe plan for audits at each layer of the IT environment? If not, why not? Are there special circumstances that apply, or is the IT audit plan sub-optimal?
- How are budgets for IT audits estimated? Was enough information gathered on the front end of the audit to support an accurate estimation? Was the specific configuration of the technology considered?
- How are IT audit procedures defined? Are they developed internally for the organization's specific environment, or are marketplace checklists used?
- Has the organization implemented any IT control frameworks or standards? If so, which ones? If not, have security and control baselines been established internally? If not, has the CAE recommended the implementation of an IT control framework and security and control baselines as part of the audit of IT governance and management?
- Are any tools used to accelerate IT audits (e.g. testing accelerators or facilitators)? If not, why not? If so, have they been tested fully and approved by IT management?
- How are IT audits staffed? Are specialists used for various technologies (e.g. applications versus infrastructure technologies)? If not, why not? How are

IT audit workpapers reviewed for quality and adequacy?

- Has a training strategy been established for IT auditors? Does it consider all the layers of the IT environment?
- Are emerging IT issues and risks evaluated each year to determine the relevance within the organization? How does the organization identify these emerging issues?
- Has the audit function benchmarked the IT audit function against industry best practices? Was the GAIN survey or other data repositories used to facilitate this?
- Do all process audits contain procedures that evaluate application configuration settings for the applications that automate the processes? How are these coordinated between audit resources (process versus IT)?

## GTAG – Appendix A – Emerging Issues

Moore's Law predicts the continued evolution of technology. This appendix covers some emerging technologies of which CAEs should be aware, and the potential impact on the organization and the IT audit function. By no means is this a comprehensive list of all emerging technologies, but it's indicative of some of the more prevalent issues in the marketplace.

These issues will certainly vary from environment to environment (the snowflake theory) and may present greater or lesser risk depending on industry, technology, or business processes. The issues, along with their risks and recommendations, are presented in no particular order, but are designed to get CAEs thinking about their environment and whether currently scheduled IT audit procedures will evaluate these issues.

### A.1 Wireless Networks

Wireless networks are proliferating throughout organizations, because they are useful and can support business objectives directly. However, they are also easy to set up (as any person who has set up a home wireless network can likely attest to) and provide a potential entry point into the corporate network. CAEs should be concerned both with the security of wireless networks that are authorized by the organization as well as rogue wireless networks that users have established without authorization.

#### Wireless Network Risks

**Intrusion** – Wireless networks may allow unauthorized entry into the corporate network.

**Eavesdropping** – Wireless networks may allow unauthorized personnel to access confidential information that is transmitted across wireless networks.

**Hijacking** – An unauthorized user may hijack the session of an authorized user connected to a wireless network and use that session to access the corporate network.

**Radio Frequency (RF) Management** – The wireless network may send transmissions into unwanted areas, which may have other impacts. For example, hospitals may have equipment that reacts poorly to radio wave transmissions and therefore should not be exposed to wireless networks.

#### Recommendations for Wireless Networks

Perform a thorough wireless network audit that includes the following two components:

- The organization most likely has wireless networks that have been approved and implemented for a specific business reason. The IT function should assess these networks and help ensure that they are secured and controlled in accordance with management's objectives.
- The organization may have unapproved wireless networks that users have established. The IT audit function should perform procedures to detect if any of

these networks exist and take appropriate action. This is more difficult than ensuring that networks are secured and controlled and will likely entail an IT auditor physically going through business unit locations with an antenna, trying to detect the presence of wireless devices.

At a minimum, the IT auditor should obtain and review a listing of all wireless networks approved by the organization. Corporate policies and procedures should be established for wireless networks and should provide guidelines for securing and controlling these networks, including the use of data encryption and authentication to the wireless network. The IT auditor should review the configuration of the known wireless networks to ensure compliance with developed policies and procedures. The IT auditor should also detect unapproved wireless networks and take appropriate corrective action.

### A.2 Mobile Devices

Most organizations have recognized the value of wireless devices such as Blackberrys, Personal Digital Assistants (PDAs), smart phones, or TELXON units and have proliferated these devices to support business objectives. However, not all organizations have grasped the risk of using these devices.

#### Mobile Device Risks

Many of these devices store critical business data on the device itself. If the device is not configured in a secure fashion, the confidentiality of this data may be impacted if the device is lost or stolen. Also, the transmission of data to the device itself may not be secure, potentially compromising the confidentiality or integrity of that data. Because these devices are often used by upper management, this could be company. Furthermore, these devices may allow remote access into corporate networks, and in the case of TELXON or similar devices, they may initiate the processing of transactions. Consider, for example, a beverage distribution company that equips route drivers with wireless devices that are used to book inventory transactions as they deliver product to each customer.

#### Recommendations for Mobile Devices

The IT auditor should review mobile device management. At a minimum, consideration should be given to:

**Provisioning** – The process for a user to procure a device.

**Standardization** – Are devices standardized?

**Security Configuration** – What policies and procedures have been established for defining security baselines for devices?

**Data Transmission** – How is data transmission controlled?

**Access Into Corporate Networks** – Do devices provide access into the corporate network? If so, how is that controlled?

**Lost or Stolen Devices** – How would the company identify lost or stolen devices and terminate service to them?

**Interface Software** – If these devices initiate business transactions, how is that information interfaced into the corporate applications?

### A.3 Interfaces

Complex IT environments often require complex interfaces to integrate their critical business applications. Even large integrated ERP environments often require complicated interfaces to other distributed applications, like Internet systems. These interfaces may be enabled with middleware technology, which acts a central point of communication and coordination for interfaces. Although interfaces and middleware play an important role in end-to-end processing of transactions, in many cases they are not included in audit plans. This may be because interfaces are difficult to classify. They are similar in function to an infrastructure, or supporting technology, yet they are software applications that may actually process transactions.

#### Interface Risks

Interfaces, and middleware in particular, are a critical link in the end-to-end processing of transactions. At a minimum, they move data from one system to another. At a maximum, they may be responsible for transforming the data, performing some calculation or modifying the data based on some algorithm. Interfaces may also pose a single point of failure to the organization. Consider Company XYZ, which is running an ERP system for financial consolidation. The distributed business units all maintain interfaces from a variety of disparate systems up to the central corporate system. There are approximately 200 of these interfaces, all running through a single middleware server and application. That middleware server suddenly stops functioning. This would have a substantial impact on the operations of the company.

#### Recommendations for Interfaces

The CAE should ensure the IT risk assessment and audit universe considers interfaces and middleware. Specific items that should be considered are:

**Use of Software to Manage Interfaces** – Does the software transform data or merely move it from place to place?

**Interface IDs** – The interface software will probably need access into the systems to/from which it is moving data. How is this access managed? Are generic IDs used? What access are these IDs granted, and who has access to use these IDs?

**Interface Directories** – Are all data moved through a single interface directory? Who has access to that directory? How is it secured and controlled? For instance, does a clerk in one of the business units have access to the directory to upload a file for transaction

processing? If so, does the directory also contain data used in wire transfers or outbound electronic payments? How is the clerk restricted from these data sets? Is data potentially co-mingled?

**Interface Types** – What types of interfaces are used? Are they real-time or batch-oriented? What transactions do they support? Do they initiate the processing of other transactions (e.g. interfaced sales orders initiating the shipment of goods).

### A.4 Data Management

Organizations are automating more and more business processes and functions. At the same time, the cost of data storage is becoming cheaper and cheaper. Even today's personal computers can have hard drives that store 250GB or more data, much more than even large servers could store five years ago. These issues have led to the proliferation of large corporate data storage solutions. It is not uncommon for a mid-sized organization to store and manage terabytes of business data. As organizations begin to manage these large repositories of data, many issues emerge.

#### Data Management Risks

Failure to manage data repositories, or storage area networks (SANS), may result in the loss of critical business data availability. Organizations must ensure that the integrity of these storage solutions is maintained adequately. However, it may be difficult to back up, or reorganize a data storage network that contains six terabytes of business data. New management and maintenance technologies must be deployed, and new management processes must be defined. Moreover, the growth in data storage also coincides with the promulgation of many new laws, statutes, and regulations regarding the management of data. Therefore, the data management requirements of an organization must also adhere to numerous new legal and industry requirements.

#### Recommendations for Data Management

Perform a thorough data management review. At a minimum, consideration should be given to:

**Data Classification** – Has the organization gone through a data classification exercise? What types of data categories have been established, and what were the criteria for organizing data into those categories?

**Data Ownership** – Has the organization formally assigned ownership of data to specific data owners? Have the responsibilities of these data owners been documented?

**Data Retention** – Has a data retention strategy been developed? Even large data storage solutions can fill up, at which point the organization needs to either delete data or move data to some other storage solution, such as archiving it. What is the current archiving/retention policy? How does this impact or support the organization's objectives? If an audit needs

to be performed, will the data be there to audit? Or will it have been archived or deleted? If it has been archived, can it be recovered easily?

**Archiving and Retention Tools** – If a data retention strategy has been defined, it may require tools to support it, such as archiving software, or archiving media. These tools may need to be audited to evaluate how effectively they are performing required procedures.

**Data Management** – How are data managed? What are the daily/weekly/other tasks that need to be performed to help ensure the integrity of data? Who performs those tasks, and how are they procedurized?

### A.5 Privacy

Data privacy and consumer rights are highly visible topics today. A large number of data privacy laws with which large companies must comply have been promulgated. In some cases, these laws may have substantially different requirements, even to the point of incompatibility with one another. For example, a large organization that does business in Europe and North America is subject to the EU Privacy Directive on Data Protection, Canada's Personal Information Protection and Electronic Documents Act of 2000, any number of U.S. state-level regulations, and perhaps industry-specific requirements such as the U.S. Health Insurance Portability and Accountability Act of 1996 or the Gramm-Leach-Bliley Act of 1999. These are all different. If an organization wants to put up a Web site that provides games or media that children might access, they need to be aware of child-protection data privacy laws as well.

#### Privacy Risks

Failure to comply with certain privacy laws could result in fines and/or criminal prosecution. In addition, there could be a significant impact to brand equity. Consider a cereal manufacturer who puts games promoting its cereal on the corporate Web site. A number of children register on the site and play the games. A hacker then compromises the list of registered users, which contains some personally identifiable information about the children who are registered on the site. *The Wall Street Journal* then publishes a story about how the cereal company let personally identifiable information about children leak on the Internet. What would be the impact of that situation? It is difficult to quantify the impact on the organization, but it is likely that the result would not be a positive impact on shareholder value.

#### Recommendations for Privacy

Perform a privacy audit. At a minimum, the organization should consider:

**What Privacy Laws Apply to the Organization** – Has the organization identified all various laws, regulations, and statutes with which it must comply?

**Responsibility for Privacy** – Has a chief privacy officer role been created? What are the responsibilities of that

role? What is the role of general counsel with respect to privacy?

**Policies and Procedures** – Have policies and procedures been established for creating, storing, and managing business data? How are these implemented, and how does the organization ensure compliance?

**Compliance Tasks** – What specific compliance tasks are performed? Does the organization require data encryption? If so, what methods are used? Are Web development methodologies updated to include items such as opt-in policies?

### A.6 Segregation of Duties

As organizations integrate their environments into larger, more complex applications, segregation of duties is less a function of job role and more a function of what transactions the user can perform in the system. Consequently, appropriate segregation of duties is largely dependent on application level security.

At the same time, however, application level security is becoming increasingly complex and requires a greater level of expertise to administer appropriately. As a result, many organizations are experiencing deficiencies related to segregation of duties. Lastly, the complexity of application level security makes it more difficult to audit segregation of duties effectively and efficiently.

#### Segregation of Duty Risks

Inadequate segregation of duties could expose the organization to theft, fraud, or unauthorized use of information resources. Moreover, deficiencies in segregation of duties could affect compliance with Sarbanes-Oxley adversely. A number of the material weaknesses in internal control reported by publicly traded companies in 2004 were related to segregation of duties.

#### Recommendations for Segregation of Duties

Perform a segregation of duties audit, which should include:

**Understanding How Segregation of Duties is Being Managed and Controlled** – What processes, people, and tools are used to support the management of segregation of duties?

**Defining Conflicts** – Has the organization developed a comprehensive listing of all job functions that are deemed to be incompatible? How has this list been modified for business unit locations that have a significantly smaller staff? Who was involved in developing the list? Were all key stakeholder involved in establishing and approving conflicts?

**Determining Specific Deficiencies** – Has the organization used the list of conflicts to identify either specific security roles, or specific individuals who have been granted access that presents a violation of segregation of duties? Is a tool being used to facilitate this process? If so, how has the tool been configured? Does the tool process and monitor conflicts in real time?

**Assigning Responsibility** – Has the organization formally assigned responsibility for managing and controlling segregation of duties to a specific individual or job role? If so, what tasks does this responsibility entail, and what is the period of performance? Have policies and procedures been established to guide this role?

**Performing a Cross-application Analysis** – Have tools, policies, and procedures been established to manage analyzing segregation of duties across applications? Example: Company XYZ is using SAP for financial accounting and PeopleSoft for human resources. A user has access to both systems, and the combined access creates a segregation of duties conflict. Analysis of either the SAP system or the PeopleSoft system would not reveal the conflict. Only a cross-application analysis of both systems would reveal the conflict.

### A.7 Administrative Access

Systems administration personnel are generally granted high levels of access to IT resources. This is explained away because they are presumed to be administrators who need this access to perform their job.

#### Administrative Access Risks

Users with administrative-level access potentially can perform many functions above and beyond their core job responsibilities. A user with full access to a business application, for example, potentially could create an invoice, receive goods, and cut a check. This same administrative user could also delete all audit trail records. A user with administrative access to the database could misappropriate the entire electronic payment run.

As organizations continue to automate and integrate their IT environments, the administrative accounting risks increase. A systems administrator with unlimited access to a full-scope SAP system has much more power than a systems administrator with unlimited access to a warehouse system. Failure to restrict administrative access adequately is a significant exposure, and for publicly traded companies could impact their external auditor's Sarbanes-Oxley Section 404 opinion. For companies that outsource some or all of the IT environment, this risk is even greater for two reasons:

- In many cases, the outsourced provider may serve multiple organizations with a large team. Typically, this means that instead of a team of five administrators supporting one organization, there may be a team of 25 administrators who collectively support five organizations. If so, all 25 administrators likely will be granted a significant level of access.
- Contractual arrangements notwithstanding, it is always a greater risk when someone who is not an employee of the organization has administrative access to systems.

#### Recommendations for Administrative Access

In every environment, administrative access is required to operate the systems. However, the IT audit function should help ensure that systems administrators only have access to data and functions required to perform job responsibilities. Note that this does not include functional transactions. Systems administrators would never, as part of their job duties, post a transaction to the G/L, cut a check, or maintain a vendor master record. As such, they should not have access to perform these transactions. Another typical argument is that administrators need functional access to troubleshoot. However, most troubleshooting and testing should be done in the test environment, not in production. If the test environment is not an adequate representation of production, that indicates a flaw in the systems development process, not a need for increased production access.

The IT auditor should also consider:

**Splitting Access** – Splitting the access to perform a function so that two people are needed to perform the function.

**Generic IDs** – In certain cases, an administrative team may be sharing an administrative ID. The IT auditor reviewing an access report would only see a single user, but the reality may be that multiple users are using that ID. This increases the risk because now the audit trail is compromised.

**Number of People With Administrator Access** – Access to administrative functions should be limited to a small number of administrators only. Not everyone in the IT department needs administrative access.

**Audit Trail Management** – Given that administrative users have a high level of access to the systems, one of the only mitigating controls available is the periodic independent review of audit trails. This review can be performed by IT audit personnel or by other independent resources (e.g. an IT director in another IT function). It's critical to make sure that, if possible, systems administrative personnel cannot delete audit trail data. This step often can be performed either through security or systems configuration.

**Use of Firecall IDs** – Firecall IDs and passwords also can be used to help mitigate the risk of granting administrative access. A firecall ID is an account set up with administrator-level access. This account is kept locked, and the password is known only to an independent person within the organization. When an emergency situation arises, the IT support personnel retrieves the password for the firecall ID, and this retrieval is logged. The support person uses the ID to perform the required tasks and returns the ID to the independent person, who then locks the account. There are some new tools available on the market today that automate this process.

### A.8 Configurable Controls

As discussed in the introduction to this GTAG, many of today's key controls are technology-based, or configured into business applications. Consider the automated three-way match example explored in the Introduction. The functionality of this matching process is controlled by a number of configurable settings within the application (e.g. tolerance levels, type of match by quantity or value, what to do with transactions that fail the match, what accounts to book variances to, etc.).

In many cases, these configurable controls are the primary controls that manage and control the processing of transactions through a given process. However, these controls are often overlooked when performing a process audit.

#### Configurable Controls Risks

Failure to consider configurable application controls when performing a process audit may result in ineffective audit procedures or inaccurate audit conclusions. In addition, it is often much quicker to review a configured setting online than to perform and review a sample of 60 transactions. Therefore, failure to focus on configurable controls may also result in inefficient audit procedures.

#### Recommendations for Configurable Controls

Evaluating configurable controls should not be performed as a standalone IT audit. Rather, all process-oriented audits should evaluate the configurable settings that control that particular process as part of the overall audit. This may pose a coordination challenge because IT auditors likely will need to work hand-in-glove with process auditors to determine which settings are important and to perform the required technical audit procedures.

The CAE should review the audit plan for all planned process audits. If the plan does not include any tests of configurable controls, it should be challenged to determine why no configurable controls are being reviewed. The fact that they are not being reviewed is not necessarily a weakness; there may be any number of valid reasons why configurable controls are not relevant for that particular audit.

If configurable controls are relevant to a particular process audit, it is important to consider how tests of these controls will be performed. Going into a configuration table and evaluating the settings requires a vastly different skill set than reviewing a sample of 60 transactions. Effective CAEs craft an audit plan that utilizes the right skill sets in the right places. For process audits, this may mean coordinating audit procedures among multiple auditors on a single audit. This type of coordination may create some logistical challenges, but should result in a better audit.

### A.9 Piracy

Computer piracy activities are more prevalent today than ever before. As organizations automate their enterprises, more assets are converted to digital form. Managing digital

assets may, for certain companies, be more critical to the company's success than protecting physical assets. The Internet has created a global distribution network that allows quick and anonymous distribution of pirated digital assets.

#### Piracy Risks

As the value of digital assets increases, the risk associated with piracy also increases.

Certain organizations and industries view piracy as one of the greatest risks they face today. Obviously, the recent battles between the recording industry and the various digital music swapping sites (e.g. Napster) are just one example of this.

The direct monetary impact of piracy is hard to quantify, but many organizations estimate that piracy has a bottom-line impact of tens, if not hundreds, of millions of dollars.

#### Recommendations for Piracy

Perform an audit of digital asset management, which should include:

**Inventory of All Digital Assets Maintained by the Organization** – Does the organization have a current list of all digital assets and their respective physical and logical locations?

**Classification** – Has the organization gone through a digital asset classification exercise? If so, what criteria were used for the exercise? What strata were defined?

**Storage** – Where are digital assets stored? How are they stored? Are appropriate backups kept? If backups are stored somewhere else, how are they secured and controlled?

**Data Encryption** – Are digital assets subject to encryption technologies? If so, which technologies? Do the encryption methods make sense for those types of assets?

**Administrative and Third-party Access** – If digital assets are secured, what other people have access to those? Example: Company XYZ is making its latest summer blockbuster movie. It has spent \$200 million on development and marketing. The film is stored in digital form on large editing servers, as any prudent company would do. This data is backed up and stored offsite. One of the people in the storage chain (e.g. the driver or off-site storage manager) takes a copy of the backup and releases the unfinished movie on the Internet several weeks before its theater release, resulting in a significantly reduced box office gross for that particular movie. Unfortunately, the whole fiasco is the result of the initial desire to have good IT controls (e.g. backups). This paradox forces the IT auditor to consider new ways of securing and controlling bits and bytes.

**Transportation and Transmission** – The same issues that applied above also apply to the transportation and transmission of digital assets. Certainly, any unencrypted

digital file sent via e-mail is exposed and potentially could be exploited. Has the organization developed robust policies and procedures that provide for the transportation and/or transmission of digital assets?

### Other Resources

#### Professional Organizations

- Information Systems Audit and Control Association (ISACA) – [www.isaca.org](http://www.isaca.org)
  - Offers the Certified Information Systems Auditor (CISA) and Certified Information Systems Manager (CISM) designations.
- Institute of Internal Auditors (IIA) – [www.theiia.org](http://www.theiia.org)
  - Offers the Certified Internal Auditor (CIA) designation.
  - Offers *ITAudit*, a free electronic newsletter that includes a Reference Library.
- Information Systems Security Association (ISSA) – [www.issa.org](http://www.issa.org)
  - Supports Certified Information Systems Security Professionals.
  - ISC2 administers the certification process, but it is not a professional organization in itself.
- American Institute of Certified Public Accountants (AICPA) – [www.aicpa.org](http://www.aicpa.org)
  - Sponsors Certified Public Accountant (CPA) designation.

#### Helpful Web Sites

- <http://www.csoonline.com>
  - Offers useful resources, including security articles, for security executives.
- <http://www.whatis.com>
  - Great for quick technology definitions and quick links to other IT sites.
- <http://csrc.nist.gov>
  - Computer Security Research Center, sponsored by the National Institute of Standards and Technology.
- <http://www.cyberpartnership.org>
  - The National Cyber Security Partnership, a public-private partnership established to develop shared strategies and programs to better secure and enhance America's information infrastructure.
- <http://www.infosecuritymag.com/>
  - Information security magazine that covers timely security topics.
- <http://www.itgi.org>
  - Exists to assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals.

#### Software and User Groups

- Freeware tools.
  - Business Software Alliance promotes a safe and legal digital world – <http://www.bsa.org/usa/antipiracy/Free-Software-Audit-Tools.cfm>
  - AuditNet<sup>®</sup> is a network of resources available for auditors – <http://www.auditnet.org>
- User groups.
  - Americas' SAP Users' Group – [www.asug.com](http://www.asug.com)
  - Independent Oracle Users Group – [www.ioug.org](http://www.ioug.org)
  - Quest International User Group (for PeopleSoft/JD Edwards) – <http://www.questdirect.org>
  - SQL Server Worldwide Users Group – <http://www.sswug.org>
  - Yahoo's directory of user groups – [http://dir.yahoo.com/Computers\\_and\\_Internet/Organizations/User\\_Groups](http://dir.yahoo.com/Computers_and_Internet/Organizations/User_Groups)

## GTAG – About the Authors

**Michael Juergens**, primary author, has more than 15 years of professional experience and has been with Deloitte since 1996. He currently serves as the leader of Deloitte's Control Assurance practice for the Pacific Southwest region. Juergens specializes in assessment of information technology controls. He is a nationally recognized speaker on internal controls and has spoken to many audiences, including The IIA, ISACA, Americas' SAP Users' Group, MIS Training Institute, and attendees of numerous national and international conferences. He sits on The IIA's Professional Conferences Committee and oversees all the IT audit training courses offered by The IIA. Juergens currently serves as the lead internal controls principal for a number of large multi-national companies. In that regard, he has overseen the delivery of numerous internal control projects, Sarbanes-Oxley readiness projects, and attestation audits. Juergens has a B.A. in economics from the University of California Irvine, and an M.B.A. from the University of California Irvine.

**David Maberry**, contributing author, is a senior manager in Deloitte's Audit and Enterprise Risk Services Control Assurance practice in Los Angeles. He has extensive experience in risk management, compliance, and internal auditing, with specializations in Sarbanes-Oxley compliance assessments, IT risk assessments, pre- and post- implementation reviews, and technical audits on a variety of systems and platforms. Maberry's significant operational experience provides a unique ability to analyze processes in virtually any environment and provide maximum benefit. Prior to joining Deloitte, he worked for more than 11 years in advanced operational management positions in the health care industry. Maberry currently supports multiple *Fortune* 500 companies in their audit compliance and business assessment strategies.

**Jeff Fisher**, contributing editor, is a senior manager in Deloitte and Touche's Audit and Enterprise Risk Services practice. Fisher has been with the firm for more than eight years and serves as the project manager and in a technical quality assurance role for some of Deloitte's largest clients. He specializes in information systems security audits and assessments, project management, and Sarbanes-Oxley Section 404 assessments. Fisher has assisted many of Deloitte's clients in preparing for, and successfully implementing, Sarbanes-Oxley assessment processes on a global basis. Fisher graduated from Ferris State University with a B.S. in accounting and computer information systems. He is a Certified Information Systems Security Professional (CISSP) and a Certified Information Systems Auditor (CISA).

**Eric Ringle**, contributing editor, is a senior manager in Deloitte and Touche LLP's Audit and Enterprise Risk Services practice. He has more than 11 years of experience

and provides services to clients operating around the globe. Ringle specializes in information systems and business process audits and assessments, project management, and Sarbanes-Oxley Section 404 assessments. He has assisted many clients in preparing for, and successfully implementing, Sarbanes-Oxley assessment processes. Ringle graduated from Michigan State University with a B.A. and M.B.A. in accounting. He is a Certified Public Accountant (CPA), Certified Information Technology Professional (CITP), and Certified Information Systems Auditor (CISA).

### Reviewers

The IIA Advanced Technology Committee, IIA global affiliates, American Institute of Certified Public Accountants, Center for Internet Security, Carnegie-Mellon University Software Engineering Institute, Information System Security Association, IT Process Institute, National Association of Corporate Directors, and SANS Institute joined the review process. The following individuals and organizations provided valuable comments to this guide:

- American Institute of Certified Public Accounts
- The Institute of Internal Auditors in Australia
- The Institute of Internal Auditors in United Kingdom
- Christopher Fox – PricewaterhouseCoopers, USA
- David Bentley – Consultant, United Kingdom
- E.W. Sean Ballington – PricewaterhouseCoopers, USA
- Jay R Taylor – General Motors Corp., USA
- Larry Brown – The Options Clearing Corporation, USA
- Lars Erik Fjortoft – Deloitte, Norway
- Lily Bi – The Institute of Internal Auditors
- Stig J. Sunde – Office of the Auditor General Norway

# Are you on a collision course with IT-related risks?

*Here's how to face them  
with confidence.*

Information technology controls are critical for businesses. As you automate more processes, share more data, and outsource more functions, IT controls are a key line of defense against IT related risks. Having the resources and experience to address these risks is the challenge. Deloitte & Touche LLP can help.

We can help you perform risk and impact assessments, develop IT audit plans and assist with performing the audits. We offer a national team of IT audit and controls professionals with extensive experience, as well as subject matter specialists in a range of technologies and industries.

IT-related challenges and risks will only increase over time. Our Enterprise Risk Services professionals can help you meet them head on. Contact us at [internalaudit@deloitte.com](mailto:internalaudit@deloitte.com), 800-871-2586 or visit us at [www.deloitte.com/us/internalaudit](http://www.deloitte.com/us/internalaudit)

## Deloitte.



Audit. Tax. Consulting. Financial Advisory.

[www.deloitte.com/us](http://www.deloitte.com/us)

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein.

Deloitte & Touche USA LLP is the US member firm of Deloitte Touche Tohmatsu. In the US, services are provided by the subsidiaries of Deloitte & Touche USA LLP (Deloitte & Touche LLP, Deloitte Consulting LLP, Deloitte Financial Advisory Services LLP, Deloitte Tax LLP and their subsidiaries), and not by Deloitte & Touche USA LLP.

Member of Deloitte Touche Tohmatsu  
Copyright © 2006 Deloitte Development LLC. All rights reserved.



### *Management of IT Auditing*

Information technology (IT) is changing the nature of the internal audit function. As new risks emerge, new audit procedures are required to manage these risks adequately. The purpose of the guide is to help chief audit executives and internal audit managers responsible for overseeing IT audits sort through the strategic issues involved during the planning, performance, and reporting of IT audits. Consideration is given to IT audit fundamentals and emerging issues.

### *What is GTAG?*

Prepared by The Institute of Internal Auditors, each Global Technology Audit Guide (GTAG) is written in straightforward business language to address a timely issue related to information technology management, control, and security. The GTAG series serves as a ready resource for chief audit executives on different technology-associated risks and recommended practices. The following guides were published in 2005.

Guide 1: Information Technology Controls

Guide 2: Change and Patch Management Controls: Critical for Organizational Success

Guide 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment

Check The IIA technology Web site at [www.theiia.org/technology](http://www.theiia.org/technology)



**The Institute of  
Internal Auditors**

Order Number: 1012  
IIA Member US \$25  
Nonmember US \$30  
IIA Event US \$22.50

ISBN 0-89413-590-2

