GTAG

GLOBAL TECHNOLOGY AUDIT GUIDE

INFORMATION TECHNOLOGY CONTROLS

The Institute of Internal Auditors

The IIA and Technology

The Institute of Internal Auditors (IIA)

Established in 1941, The IIA is an international professional association headquartered in Altamonte Springs, Fla. With more than 100,000 members and representation from more than 100 countries, The Institute is the recognized authority, principal educator, and acknowledged leader in certification, education, research, and technological guidance for the profession worldwide.

The IIA helps you keep up with the latest IT advances by offering specialized training and targeted resources. The IT Audit Curriculum, from The IIA and Deloitte & Touche LLP, helps you stay up to speed with evolving IT systems and adapt to compliance requirements such as the Sarbanes-Oxley Act. Our Global Technology Audit Guides (GTAG), written for CAEs and audit supervisors, address timely issues related to information technology management, control, or security. Our ITAudit is your online resource for free guidance on IT trends and audit tools. Plan ahead for The IIA's IT Conference to be held February 2006 in Orlando, Fla.

For more details and to join, visit www.theiia.org

AICPA – American Institute of Certified Public Accountants
www.aicpa.org

CIS – Center for Internet Security
www.cisecurity.org

CMU/SEI – Carnegie-Mellon University Software Engineering Institute
www.cmu.edu

ISSA – Information Systems Security Association
www.issa.org

NACD – National Association of Corporate Directors
www.nacd.org

SANS Institute
www.sans.org

GTAG — Table of Contents:

In my previous role as a chief audit executive (CAE), I noted a need for guidance on IT management and control written specifically for executives. So one of my first acts as president of The IIA was to initiate a project to produce this IT Controls guide. This guide is for the executive, not the technical staff — although it will help those personnel better relate to management and governance perspectives.

The purpose of this document is to explain IT controls and audit practice in a format that allows CAEs to understand and communicate the need for strong IT controls. It is organized to enable the reader to move through the framework for assessing IT controls and to address specific topics based on need. This document provides an overview of the key components of IT control assessment with an emphasis on the roles and responsibilities of key constituents within the organization who can drive governance of IT resources. You may already be familiar with some aspects of this document, while other segments will provide new perspectives on how to approach this key audit strategy. It is our hope that the components can be used to educate others about what IT controls are and why management and internal auditing must ensure proper attention is paid to this fundamental methodology for good governance.

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

- Why should I understand IT controls? One word: Assurance. Executives play a key role in assuring information reliability. Assurance comes primarily from an interdependent set of business controls, plus the evidence that controls are continuous and sufficient. Management and governance must weigh the evidence provided by controls and audits and conclude that it provides reasonable assurance. This guide will help you understand the evidence.
- What is to be protected? Let's start with *trust*. Trust enables business and efficiency. Controls provide the basis for trust, although they are often unseen. Technology provides the foundation for many — perhaps most — business controls. Reliability of financial information and processes — now mandated for many companies — is all about trust.
- Where are IT controls applied? Everywhere. IT includes technology components, processes, people, organization, and architecture — collectively known as infrastructure — as well as the information itself. Many of the infrastructure controls are technical, and IT supplies the tools for many business controls.
- Who is responsible? Everybody. But you must specify control ownership and responsibilities, otherwise no one is responsible. This guide addresses specific responsibilities for IT controls.
- When do we assess IT controls? Always. IT is a rapidly changing environment, fueling business change. New risks emerge at a rapid pace. Controls must present continuous evidence of their effectiveness, and that evidence must be assessed and evaluated constantly.
- How much control is enough? You must decide. Controls are not the objective; controls exist to help meet business objectives. Controls are a cost of doing business and can be expensive — but not nearly as expensive as the probable consequences of inadequate controls.

IT controls are essential to protect assets, customers, and partners, and sensitive information; demonstrate safe, efficient, and ethical behavior; and preserve brand, reputation, and trust. In today's global market and regulatory environment, these are all too easy to lose.

Use this guide as a foundation to assess or build your organization's framework and audit practices for IT business control, compliance, and assurance. Use it to help make sense of the conflicting advice you receive. Make sure all the elements are in place to meet the challenges of constant change, increasing complexity, rapidly evolving threats, and the need to improve efficiency constantly.

The IIA produced this guide, but it is truly a team effort. The principal writers are Charles H. Le Grand, of CHL Global, and Alan S. Oliphant, FIIA, MIIA, QiCA, of Mair International. We owe a great debt of gratitude to our partners, IIA international affiliates, and members of the Global Technology Audit Guide (GTAG) team. We are grateful for their support and encouragement. This guide is a testimony to what The IIA does best: "Progress Through Sharing."

Sincerely,

David A. Richards, CIA, CPA
President, The Institute of Internal Auditors, Inc.

GTAG Information Technology Controls describes the knowledge needed by members of governing bodies, executives, IT professionals, and internal auditors to address technology control issues and their impact on business. Other professionals may find the guidance useful and relevant. The guide provides information on available frameworks for assessing IT controls and describes how to establish the right framework for an organization. Moreover, it sets the stage for future GTAGs that will cover specific IT topics and associated business roles and responsibilities in greater detail.

The objectives of the *IT Controls* guide are to:

- Explain IT controls from an executive perspective.
- Explain the importance of IT controls within the overall system of internal controls.
- Describe the organizational roles and responsibilities for ensuring IT controls are addressed adequately within the overall system of internal controls.
- Describe the concepts of risk inherent in the use and management of technology by any organization.
- Describe the basic knowledge and understanding of IT controls needed by the CAE to ensure effective internal audit assessments of IT controls.
- Describe the relevant elements of the IT controls assessment process as provided by the internal audit function.

2.1 Introduction to IT Controls

IT controls do not exist in isolation. They form an interdependent continuum of protection, but they may also be subject to compromise due to a weak link. They are subject to error and management override, may range from simple to highly technical, and may exist in a dynamic environment.

IT controls have two significant elements: the automation of business controls and control of IT. Thus, IT controls support business management and governance as well as provide general and technical controls over IT infrastructures.

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

2.2 Understanding IT Controls

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

You don't need to "everything" about IT controls, but remember two key control concepts:

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

Many frameworks exist for categorizing IT controls and their objectives. This guide recommends that each organization use the applicable components of existing frameworks to categorize and assess IT controls, and to provide and document its own framework for:

- Compliance with applicable regulations and legislation.
- Consistency with the organization's goals and objectives.
- Reliable evidence (reasonable assurance) that activities comply with management's governance policies and are consistent with the organization's risk appetite.

2.3 Importance of IT Controls

Many issues drive the need for IT controls, ranging from the need to control costs and remain competitive through the need for compliance with internal and external governance. IT controls promote reliability and efficiency and allow the organization to adapt to changing risk environments. Any control that mitigates or detects fraud or cyber attacks enhances the organization's resiliency because it helps the organization uncover the risk and manage its impact. Resiliency is a result of a strong system of internal controls because a well-controlled organization has the ability to manage challenges or disruptions seamlessly.

Key indicators of effective IT controls include:

- The ability to execute and plan new work such as IT infrastructure upgrades required to support new products and services.
- Development projects that are delivered on time and within budget, resulting in cost-effective and better product and service offerings compared to competitors.
- Ability to allocate resources predictably.
- Consistent availability and reliability of information and IT services across the organization and for customers, business partners, and other external interfaces.
- Clear communication to management of key indicators of effective controls.
- The ability to protect against new vulnerabilities and

threats and to recover from any disruption of IT services quickly and efficiently.
- The efficient use of a customer support center or help desk.
- Heightened security awareness on the part of the users and a security-conscious culture throughout the organization.

2.4 IT Roles and Responsibilities

Many different roles have emerged in recent years for positions within the organization with IT control responsibilities and ownership. Each position within the governance, management, operational, and technical levels should have a clear description of its roles, responsibilities, and ownership for IT controls to ensure accountability for specific issues. This section addresses the various IT control roles and responsibilities within the organization and allocates them to specific positions within a hypothetical organizational structure.

2.5 Analyzing Risk

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

2.6 Monitoring and Techniques

The implementation of a formal control framework facilitates the process of identifying and assessing the IT controls necessary to address specific risks. A control framework is a structured way of categorizing controls to ensure the whole spectrum of control is covered adequately. The framework can be informal or formal. A formal approach will more readily satisfy the various regulatory or statutory requirements for organizations subject to them. The process of choosing or constructing a control framework should involve all positions in the organization with direct responsibility for controls. The control framework should apply to, and be used by, the whole organization — not just internal auditing.

2.7 IT Control Assessment

Assessing IT controls is a continuous process. Business processes are changing constantly as technology continues to evolve. Threats emerge as new vulnerabilities are discovered. Audit methods improve as auditors adopt an approach where IT control issues in support of the business objectives are near the top of the agenda.

Management provides IT control metrics and reporting. Auditors attest to their validity and opine on their value. The auditor should liaise with management at all levels and with the audit committee to agree on the validity and effectiveness of the metrics and assurances for reporting.

IT is an integral part of all processes that enable businesses and governments to accomplish their missions and objectives. IT facilitates local and global communications and fosters international business cooperation. IT controls have two significant components: automation of business controls and control of IT. They support business management and governance, and they provide general and technical controls over the policies, processes, systems, and people that comprise IT infrastructures.

IT controls do not exist in isolation. They form an interdependent continuum of protection, but they also may be subject to compromise due to a "weak link." They are subject to error and management override, may range from simple to highly technical, and may exist in a dynamic environment. IT controls support the concept of "defense in depth," so a single weakness does not always result in a single point of failure.

Controls exist to protect stakeholder interests:

- The owner's equity.
- Customer concerns, such as privacy and identity.
- Employees' jobs and abilities to prove they did the right thing.
- Management's comfort with the assurance provided by automated processes.

IT control assurance addresses the ability of controls to protect the organization against the most important threats and provides evidence that remaining risks are unlikely to harm the organization and its stakeholders significantly. These controls also are essential for assuring the reliability of financial processes and reporting.

They are all connected.

When a security administrator selects the settings in a firewall configuration file (a technical task requiring specific skills and knowledge), he or she implements a policy (which may or may not be documented elsewhere) that, when deployed, determines the messages that will or will not be allowed into or out of the communications network, and establishes the "ports" through which they may travel.

Your organization gets an element of protection from its firewalls that is vital to the protection of information and the infrastructures where that information is collected, processed, stored, and communicated.

When CAEs review and assess the controls over IT, they should ask:

- What do we mean by IT controls?
- Why do we need IT controls?
- Who is responsible for IT controls?
- When is it appropriate to apply IT controls?
- Where exactly are IT controls applied?
- How do we perform IT control assessments?

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

The internal auditor's role in IT controls begins with a sound conceptual understanding and culminates in providing the results of risk and control assessments. Internal auditors interact with the people responsible for controls and must pursue continuous learning and reassessment as new technologies emerge and the organization's opportunities, uses, dependencies, strategies, risks, and requirements change.

"I keep six honest serving-men
(They taught me all I knew);
Their names are
What and Why and When
and How and Where and Who"

— Rudyard Kipling,
from "Elephant's Child"
in *Just So Stories*.

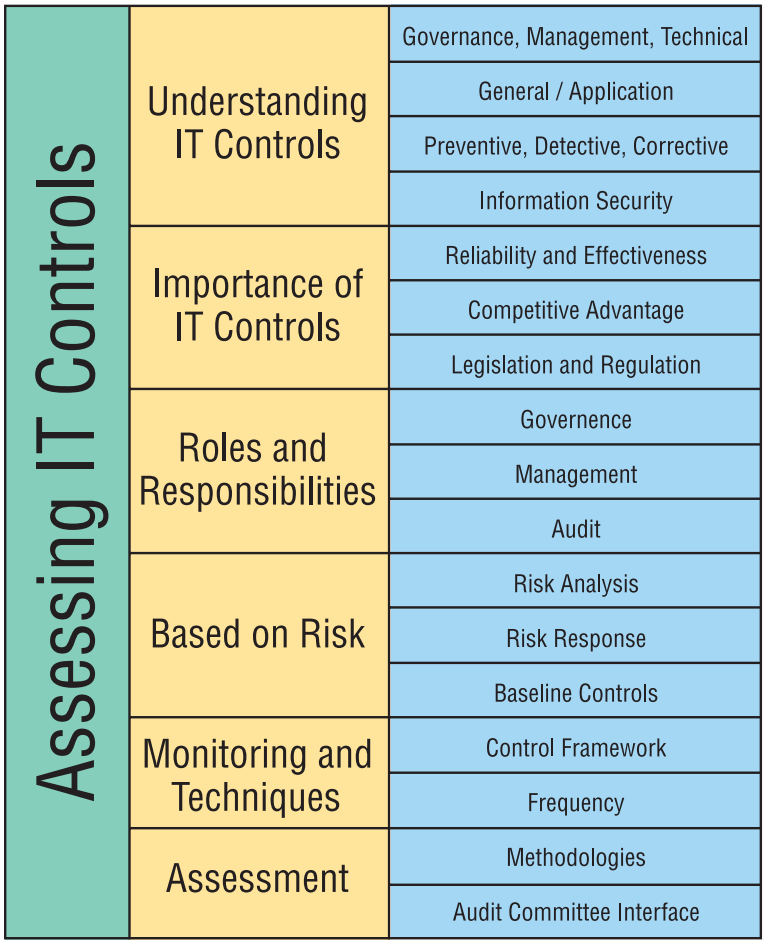


Figure 1 - The Structure of IT Auditing

COSO[1] defines *internal control* as: "A process, effected by an organization's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

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

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

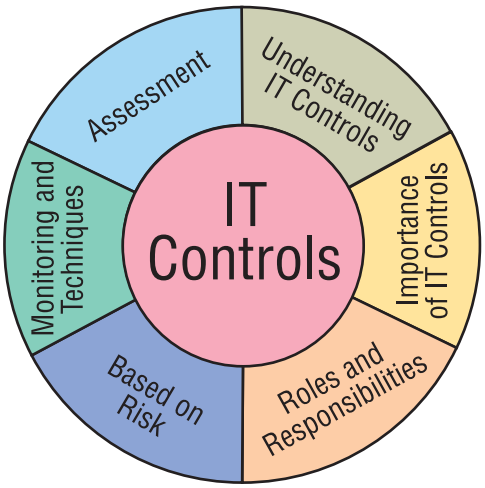


Figure 2

5.1 Control Classifications

Controls may be classified to help understand their purposes and where they fit into the overall system of internal controls (See Figure 3, *Some Control Classifications*, page 4). By understanding these classifications, the control analyst and auditor are better able to establish their positions in the control framework and answer key questions such as: Are the detective controls adequate to identify errors that may get past the preventive controls? Are corrective controls sufficient to fix the errors once detected? A common classification of IT controls is *general* versus *application*.

General controls (also known as infrastructure controls) apply to all systems components, processes, and data for a given organization or systems environment. General controls include, but are not limited to: information security policy, administration, access, and authentication; separation of key IT functions; management of systems acquisition and implementation; change management; backup; recovery; and business continuity.

Application controls pertain to the scope of individual business processes or application systems. They include such controls as data edits, separation of business functions (e.g., transaction initiation versus authorization), balancing of processing totals, transaction logging, and error reporting.

The function of a control is highly relevant to the assessment of its design and effectiveness. Controls may be classified as *preventive*, *detective*, or *corrective*.

Preventive controls prevent errors, omissions, or security incidents from occurring. Examples include simple data-entry edits that block alphabetic characters from being entered into numeric fields, access controls that protect sensitive data or system resources from unauthorized people, and complex and dynamic technical controls such as antivirus software, firewalls, and intrusion prevention systems.

It is not necessary to know "everything" about IT controls.

Do not be concerned if you do not understand the full continuum or all the technical intricacies of IT controls. Many of these controls are the domain of specialists who manage specific risks associated with individual components of the systems and network infrastructure. In keeping with good separation of duties practices, some people who have specialized knowledge in a technology, such as database management, may know little about network components or communication protocols, and vice versa.

There are two key control concepts to remember:

1. *Assurance must be provided by the IT controls within the whole system of internal control and must be continuous and produce a reliable and continuous trail of evidence.*
2. *The auditor's assurance is an independent and objective assessment of the first assurance. It is based on understanding, examining, and assessing the key controls related to the risks the auditors manage, as well as performing sufficient tests to ensure the controls are designed appropriately and function effectively.*

[1] COSO – Committee of Sponsoring Organizations for the Commission on Fraudulent Financial Reporting (The Committee of Sponsoring Organizations of the Treadway Commission). See www.coso.org.

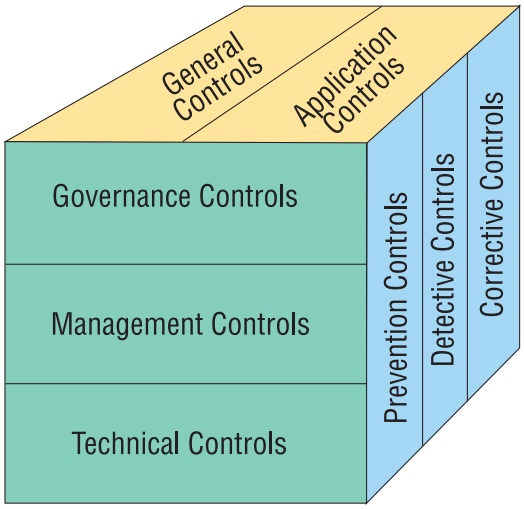


Figure 3 - Some Control Classifications

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

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

Generally, it is most efficient to prevent errors or detect them as close as possible to their source to simplify correction. These corrective processes also should be subject to preventive and detective controls, because they represent another opportunity for errors, omissions, or falsification.

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

5.2 Governance, Management, Technical

Another common classification of controls is by the group responsible for ensuring they are implemented and maintained properly. For the purpose of assessing roles and responsibilities, this guide primarily categorizes IT controls as *governance*, *management*, and *technical*. Information security program elements for these three categories are described in Appendix A (page 25). The first two levels — governance and management — are the most applicable to the scope of this guide, although it may also be useful to understand how higher-level controls specifically are established within the technical IT infrastructures. Technical controls will be the subject of more topic-specific GTAGs.

5.2.1 Governance Controls

The primary responsibility for internal control resides with the board of directors in its role as keeper of the governance framework. IT control at the governance level involves ensuring that effective information management and security principles, policies, and processes are in place and performance and compliance metrics demonstrate ongoing support for that framework.

Governance controls are those mandated by, and controlled by, either the entire board of directors or a board committee in conjunction with the organization's executive management. These controls are linked with the concepts of corporate governance, which are driven both by organizational goals and strategies and by outside bodies such as regulators.

An important distinction between governance and management controls is the concept of "noses in, fingers out." The board's responsibility involves oversight rather than actually performing control activities. For example, the audit committee of the board does no auditing, but it does oversee both the internal and external auditing of the organization.

5.2.2 Management Controls

Management responsibility for internal controls typically involves reaching into all areas of the organization with special attention to critical assets, sensitive information, and operational functions. Consequently, close collaboration among board members and executive managers is essential. Management must make sure the IT controls needed to achieve the organization's established objectives are applied and ensure reliable and continuous processing. These controls are deployed as a result of deliberate actions by management to:

- Recognize risks to the organization, its processes, and assets.
- Enact mechanisms and processes to mitigate and manage risks (protect, monitor, and measure results).

5.2.3 Technical Controls

Technical controls form the foundation that ensures the reliability of virtually every other control in the organization. For example, by protecting against unauthorized access and intrusion, they provide the basis for reliance on the integrity of information — including evidence of all changes and their authenticity. These controls are specific to the

The Center for Internet Security (www.cisecurity.org) reports that applying controls consistently over system and network component configuration will protect the organization from more than 85 percent of the top vulnerabilities identified by the U.S. National Institute of Standards and Technology (NIST), Federal Bureau of Investigation (FBI), SANS Institute, and Computer Security Institute (CSI).

technologies in use within the organization's IT infrastructures. The ability to automate technical controls that implement and demonstrate compliance with management's intended information-based policies is a powerful resource to the organization.

5.3 IT Controls – What to Expect

Individual control mechanisms a CAE can expect to find within the organization can be defined within the hierarchy of IT controls, from the overall high-level policy statements issued by management and endorsed by the board of directors, down to the specific control mechanisms incorporated into application systems.

The hierarchy in Figure 4, *IT Controls*, this page, represents a logical "top-down" approach, both when considering controls to implement and when determining areas on which to focus audit resources during reviews of the entire IT operating environment. The different elements of the hierarchy are not mutually exclusive; they are all connected and can intermingle. Many of the control types within the elements are described below.

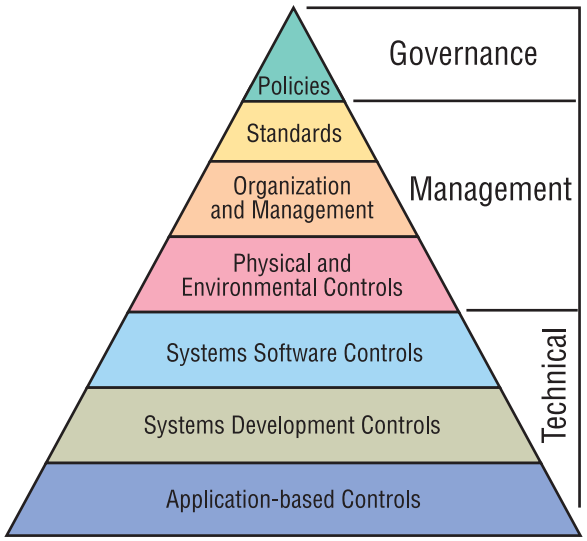


Figure 4 – IT Controls

5.3.1 Policies

All organizations need to define their aims and objectives through strategic plans and policy statements. Without clear statements of policy and standards for direction, organizations can become disoriented and perform ineffectively. Organizations with clearly defined aims and objectives tend to be successful.

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

IT policy statements include, but are not restricted to:

- A general policy on the level of security and privacy throughout the organization. This policy should be consistent with all relevant national and international legislation and should specify the level of control and security required depending on the sensitivity of the system and data processed.
- A statement on the classification of information and the rights of access at each level. The policy should also define any limitations on the use of this information by those approved for access.
- A definition of the concepts of data and systems ownership, as well as the authority necessary to originate, modify, or delete information. Without these guidelines, it is often difficult to coordinate change within large organizations, because there may not be anyone designated to have overall responsibility for the data or systems.
- A general policy that defines the extent to which users can deploy intelligent workstations to create their own applications.
- Personnel policies that define and enforce conditions for staff in sensitive areas. This includes the positive vetting of new staff prior to joining the organization, carrying out annual credit checks, and having employees sign agreements accepting responsibility for the required levels of control, security, and confidentiality. This policy would also detail related disciplinary procedures.
- Definitions of overall business continuity planning requirements. These policies should ensure that all aspects of the business are considered in the event of

a disruption or disaster — not just the IT elements.

A good source of IT and security policies is the SANS Security Policy Resource page (http://www.sans.org/resources/policies/#intro), a consensus research project of the SANS Institute community. The project offers free resources for rapid development and implementation of information security policies, including policy templates for 24 important security requirements. Although the templates were compiled to help the people attending SANS training programs, SANS makes them available to the world because Internet security depends on vigilance by all participants.

5.3.2 Standards

Standards exist to support the requirements of policies. They are intended to define ways of working that achieve the required objectives of the organization. Adopting and enforcing standards also promotes efficiency because staff are not required to reinvent the wheel every time a new business application is built or a new network is installed. Standards also enable the organization to maintain the whole IT operating environment more efficiently.

Large organizations with significant resources are in a position to devise their own standards. On the other hand, smaller organizations rarely have sufficient resources for this exercise. There are many sources of information on standards and best practice, some of which are listed in Appendix I (See page 45).

As a guideline, the CAE should expect to see standards adopted for:

- **Systems Development Processes** – When organizations develop their own applications, standards apply to the processes for designing, developing, testing, implementing, and maintaining systems and programs. If organizations outsource application development or acquire systems from vendors, the CAE should ascertain that agreements require the providers to apply standards consistent with the organization's standards, or acceptable to the organization.
- **Systems Software Configuration** – Because systems software provides a large element of control in the IT environment, standards related to secure system configurations, such as the CIS Benchmarks from the Center for Internet Security, are beginning to gain wide acceptance by leading organizations and technology providers. The way products such as operating systems, networking software, and database management systems are configured can either enhance security or create weaknesses that can be exploited.
- **Application Controls** – All applications which support business activities need to be controlled. Standards are necessary for all applications the organization develops or purchases that define the types of controls that must be present across the whole range of business activities, as well as the specific controls that should apply to sensitive processes and information.
- **Data Structures** – Having consistent data definitions across the full range of applications ensures disparate systems can access data seamlessly and security controls for private and other sensitive data can be applied uniformly.
- **Documentation** – Standards should specify the minimum level of documentation required for each application system or IT installation, as well as for different classes of applications, processes, and processing centers.

As with policies, standards should be approved by management, should be written in clear and understandable language, and should be made available to all who implement them.

5.3.3 Organization and Management

Organization and management plays a major role in the whole system of IT control, as it does with every aspect of an organization's operations. An appropriate organization structure allows lines of reporting and responsibility to be defined and effective control systems to be implemented.

5.3.3.1 Separation of Duties

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

Traditional separation of duties within the IT environment is divided between systems development and operations. Operations should be responsible for running production systems — except for change deployment — and should have little or no contact with the development process. This control includes restrictions preventing operators from accessing or modifying production programs, systems, or data. Similarly, systems development personnel should have little contact with production systems. By assigning specific roles during implementation and other change processes to both the personnel responsible for application systems and those responsible for operations, appropriate separation of duties can be enforced. In large organizations, many other functions should be considered to ensure appropriate separation of duties, and these controls can be quite detailed. For example, privileged accounts, such as the Administrator group in Windows and Super User in UNIX, can modify log entries, access any file, and in many cases act as any user or role. It is important to restrict the number of individuals with this privilege to a minimum.

Software tools are also available and should be considered to limit the power and monitor the activities of individuals with privileged accounts.

5.3.3.2 Financial Controls

Because organizations make considerable investments in IT, budgetary and other financial controls are necessary to ensure the technology yields the protected return on investment or proposed savings. Management processes should be in place to collect, analyze, and report information related to these issues. Unfortunately, new IT developments often suffer massive cost over-runs and fail to deliver the expected cost savings because of insufficient planning. Budgetary controls can help identify potential failings early in the process and allow management to take positive action. They may also produce historical data that organizations can use in future projects.

5.3.3.3 Change Management

Change management processes can be specified under organizational and management control elements. These processes should ensure that changes to the IT environment, systems software, application systems, and data are applied in a manner that enforces appropriate division of duties; makes sure changes work as required; prevents changes from being exploited for fraudulent purposes; and reveals the true costs of inefficiencies and system outages that can be obscured by ineffective monitoring and reporting processes. Change management is one of the most sensitive areas of IT controls and can seriously impact system and service availability if not administered effectively. The IT Process Institute has published research demonstrating that effective IT change management can bring significant benefits organizations.

5.3.3.4 Other Management Controls

Other typical management controls include vetting procedures for new staff, performance measurement, provision of specialist training for IT staff, and disciplinary procedures. These are listed in the Information Security Program Elements in Appendix A and will be covered in greater detail in other GTAG publications.

5.3.4 Physical and Environmental Controls

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

Some typical physical and environmental controls include:

- Locating servers in locked rooms to which access is restricted.
- Restricting server access to specific individuals.
- Providing fire detection and suppression equipment.
- Housing sensitive equipment, applications, and data away from environmental hazards such as low-lying flood plains or flammable liquid stores.

When considering physical and environmental security, it is also appropriate to consider contingency planning — also known as disaster recovery planning — which includes response to security incidents. What will the organization do if there is a fire or flood, or if any other threat manifests itself? How will the organization restore the business and related IT facilities and services to ensure normal processing continues with minimum effect on regular operations? This type of planning goes beyond merely providing for alternative IT processing power to be available and routine backup of production data; it must consider the logistics and coordination needed for the full scope of business activity. Finally, history consistently demonstrates that a disaster recovery plan that has not been tested successfully in a realistic simulation is not reliable.

5.3.5 Systems Software Controls

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

Systems software can be highly complex and can apply to components and appliances within the systems and network environment. It may be configured to accommodate highly specialized needs and normally requires a high degree of specialization to maintain it securely. Configuration techniques can control logical access to the applications, although some application systems contain their own access controls, and may provide an opening for hackers to use to break into a system. Configuration techniques also provide the means to enforce division of duties, generate specialized audit trails, and apply data integrity controls through access control lists, filters, and activity logs.

IT audit specialists are required to assess controls in this area. Small organizations are unlikely to have the resources to employ such specialists and should consider outsourcing the work. Whether IT auditors are employed or outsourced, they require a highly specific set of knowledge. Much of this knowledge can come from experience, but such knowledge must be updated constantly to remain current and useful. Certification confirms that a technical specialist has acquired a specified set of knowledge and experience and has passed a related examination. In the IT audit world, global certificates include the Qualification in Computer Auditing (QiCA), from IIA–United Kingdom and Ireland; Certified Information Systems Auditor (CISA), available through the

Information Systems Audit and Control Association (ISACA); and Global Information Assurance Certification (GIAC) Systems & Network Auditor (GSNA), from the SANS Institute's GIAC program. Additional certifications address general and specialized competence in information security, network administration, and other areas closely related to IT auditing and are useful for identifying an IT auditor's potential ability.

Some key technical controls the CAE should expect to find in a well-managed IT environment include:

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

5.3.6 Systems Development and Acquisition Controls

Organizations rarely adopt a single methodology for all systems development projects. Methodologies are chosen to suit the particular circumstances of each project. The IT auditor should assess whether or not the organization develops or acquires application systems using a controlled method that subsequently provides effective controls over and within the applications and data they process. All computer application systems should perform only those functions the user requires in an efficient way. By examining application development procedures, the auditor can gain assurance that applications work in a controlled manner.

Some basic control issues should be evident in all systems development and acquisition work:

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

Where systems development is outsourced, the outsourcer or provider contracts should require similar controls.

Project management techniques and controls need to be part of the development process, whether developments are performed in-house or are outsourced. Management should know projects are on time and within budget and that resources are used efficiently. Reporting processes should ensure that management completely understands the current status of development projects and does not receive any surprises when the end product is delivered.

5.3.7 Application-based Controls

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

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

Reviewing the application controls traditionally has been the "bread and butter" of the IT auditor. However, because application controls now represent a huge percentage of business controls, they should be the priority of every internal auditor. All internal auditors need to be able to evaluate a business process and understand and assess the controls provided by automated processes.

There are several types of generic controls that the CAE should expect to see in any application:

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

5.4 Information Security

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

The universally accepted elements of information security are:

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

5.5 IT Controls Framework

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

Many frameworks exist for categorizing IT controls and their objectives. Each organization should use the most applicable components of these frameworks to categorize or assess IT controls and to provide and document its own internal control framework for:

- Compliance with applicable regulations and legislation.
- Consistency with the organization's goals and objectives.
- Reliable evidence (assurance) that activities are in compliance with management's governance policies and are consistent with the organization's risk appetite.

Risk Appetite

An organization's risk appetite defines the degree of risk a company or other organization is willing to accept in pursuit of its goals, as determined by executive management and governance. Risk appetite can specify, for example, whether or not an organization will take an aggressive role in the deployment of new and emerging technologies. An organization's risk appetite can be affected by its industry and regulatory environment. Closely related to risk appetite is an organization's risk tolerance, which measures how far it is willing to deviate from its stated measure of risk appetite.

Many issues drive the need for IT controls, including controlling costs and remaining competitive, protecting against information theft by hackers, and complying with legislation and regulation such as the U.S. Sarbanes-Oxley Act of 2002[2], the European Union's Data Protection Directive, and related legislation in other countries. IT controls promote reliability and efficiency and allow the organization to adapt to changing risk environments. For example, any control that mitigates or detects fraud or cyber attacks enhances the organization's resiliency by helping the organization uncover the risk and manage its impact. Resiliency is a result of a strong system of internal controls that give an organization the ability to manage disruptions seamlessly.

Legislation and regulations in some countries now require organizations to report on the effectiveness of internal control and, by implication, the effectiveness of IT control. The most prominent new law is Sarbanes-Oxley, which requires all companies with shares that are publicly traded in the United States and their foreign subsidiaries to report on their system of internal controls over financial reporting, performed in conjunction with an audit of financial statements. A list of some of the legislation and regulations applicable to internal controls is provided in Appendix B (See page 24).

The need for controls is further driven by the complexity resulting from the necessity for diverse technical components to work with one another. While flexibility and adaptability of IT are crucial to meeting the changing needs of customers and business partners and responding to competitive pressures, they also add complexity to business and IT infrastructures. In addition, information security has been acknowledged as a key component of internal control with the emergence and widespread acceptance of standards such as the International Organization for Standardization Code of Practice for Information Security Management (ISO 17799).

Organizations that implement effective IT controls experience improvements in efficiencies, reliability of services, flexibility of systems, and availability of assurance evidence — all of which add value and increase stakeholder and regulator confidence in the organization. Some key indicators of effective IT controls include:

- The ability to execute planned, new work such as the IT infrastructure upgrades required to support new products and services.
- Delivery of development projects on time and within budget, resulting in cheaper and better product and service offerings when compared with competitors.
- Ability to allocate resources predictably.
- Consistent availability and reliability of information and IT services across the organization and for customers, business partners, and other external interfaces.
- Clear communication to management of effective controls.
- The ability to protect against new vulnerabilities and threats quickly and efficiently and to recover from any disruption of IT services.
- The efficient use of a customer support center or help desk.
- A security-conscious culture among end users throughout the organization.

Although the internal audit function likely will include specialist IT auditors to address IT issues in detail, the CAE also should understand IT control issues at a high level, particularly their interactions with other IT and non-IT controls. This understanding is particularly important when discussing compliance or control deficiencies with high-level managers such as the chief executive officer (CEO), chief financial officer (CFO), or chief information officer (CIO), and with the various board committees.

The CAE should be able to discuss relevant regulations and legislation with the audit committee, the chief legal counsel, and other relevant individuals and committees. The CAE also should understand how IT controls support reliability and effectiveness and help promote competitive advantage. Moreover, the CAE should thoroughly understand the major issues that drive the need for controls within the organization's particular sector to ensure they are considered during audit assessments. Without a thorough knowledge and understanding of IT controls, the auditor will be unable to grasp their significance or to assess them adequately as part of the overall review of internal control.

[2] Public Accounting Reform and Investor Protection Act of 2002, known as Sarbanes-Oxley after its sponsors U.S. Sen. Paul Sarbanes and U.S. Rep. Michael Oxley.

Many different roles have emerged in recent years for positions within the organization with responsibilities and ownership of IT controls. Each position at the governance, management, operational, and technical levels should have a clear description of its roles and responsibilities for IT controls to avoid confusion and ensure accountability for specific issues. This section addresses the various IT control roles and responsibilities within the organization and allocates them to specific positions within a hypothetical organizational structure.

There is no universally applicable means of defining the organizational structure for IT control. The CAE should identify where IT control responsibilities lie and assess their appropriateness with regard to separation of duties, as well as any gaps that may exist in assigned responsibilities. Once this is done, the CAE will know whom to approach to discuss specific IT issues and where specific information can be obtained.

Overall, the objectives for the use of IT within any organization are:

- To deliver reliable information efficiently and secure IT services in line with the organization's strategies, policies, external requirements, and risk appetite.
- To protect stakeholder interests.
- To enable mutually beneficial relationships with customers, business partners, and other outside parties that accomplish business objectives.
- To identify and respond to threats and potential violations of control appropriately.

Specific roles within the organization support these objectives. The position descriptions and titles will differ across different countries, industries, and organizations, and some of the roles may be merged within smaller organizations. However, some individuals within the organization must address the IT control function and interact with the CAE and internal audit staff members.

7.1 Board of Directors/Governing Body

One important role of the full board of directors is to determine and approve strategies, set objectives, and ensure that objectives are being met to support the strategies. In relation to IT, this requires:

- Awareness of the key IT topics, such as the IT and information security policies, and the concepts of risk as they relate to IT. An example of board roles in IT oversight is provided in The IIA's "Information Security Management and Assurance Series" at www.theiia.org/iia/index.cfm?doc_id=2458.
- Understanding of the IT strategy's infrastructure and components as well as awareness of key system development and acquisition projects and how they support and impact overall corporate strategies, objectives, and short- and long-term budgets.
- Approval of the data classifications structure and the related access rights.

The board will establish various committees based on its relationships with the organization. The most common committees of the board are audit, compensation, and governance, but some boards have additional committees such as a risk management committee or finance committee. These committees may bear different names from those identified below, and their roles may vary. The functions, rather than the names, are important.

7.1.1 Audit Committee

The role of the audit committee encompasses oversight of financial issues, internal control assessment, risk management, and ethics. IT control is a strong element of each of these duties and calls for:

- Understanding of financial management (financial expert role) and the organization's reliance on IT for financial processing and reporting.
- Ensuring IT topics are included in the committee meeting agenda — especially CIO reporting.
- Ensuring general IT controls and controls in business application systems and processes involved in preparing financial statements are assessed and tested adequately.
- Overseeing the overall assessment of IT controls.
- Reviewing the business and control issues related to new systems development and acquisition.
- Examining internal and external audit plans and work to ensure IT topics are covered adequately.
- Reviewing the results of audit work and monitoring the resolution of issues raised.
- Understanding the IT topics that impact ethics monitoring.

7.1.2 Compensation Committee

The compensation committee has no direct relationship with IT. However, it can improve the board's oversight of IT by making IT one of the performance elements of any compensation plan it approves.

7.1.3 Governance Committee

The Governance Committee is responsible for board member selection and assessment and for leadership of the board's operations. In relation to IT, this committee should:

- Ensure that potential and current board members have a suitable IT knowledge or background.
- Assess board committees' performance in terms of their oversight of IT.
- Review any external regulatory governance assessments in relation to IT topics.
- Ensure that the board reviews IT policies periodically and that board meetings focus on IT with adequate frequency.

7.1.4 Risk Management Committee

The risk management committee is responsible for oversight

of all risk analysis and assessment, risk response, and risk monitoring. Its role includes:

- Assessing the extent to which management has established effective enterprise risk management in the organization.
- Being aware of, and concurring with, the organization's risk appetite and tolerance.
- Appreciating the impact of IT-related risks.
- Reviewing the organization's risk portfolio — including IT risks — and considering it against the organization's risk appetite.
- Being apprised of the most significant IT risks and determining whether or not management's response to changes in risk and threats is appropriate.
- Monitoring and evaluating all activities performed by management to minimize all known and documented risks.

7.1.5 Finance Committee

The main role of the finance committee is to review financial statements, cash flow projections, and investment management. Members of this committee need to understand the control elements of IT that ensure the accuracy of information used to make key financing decisions and generate financial reports. They also should consider, and ask management to report on, the benefits and costs of maintaining — versus replacing — critical IT systems. Management's report should consider "soft" efficiency issues, such as gains or losses to productivity based on ease and efficiency of use; the "hard" costs of repairs and upgrades, and the potential for risk due to loss or corruption of data.

7.2 Management

Several specific roles have emerged in large organizations in relation to IT risk and control. As stated previously, small organizations might not allocate an individual for each role, although the function must still be performed. An individual may perform multiple roles, but care must be taken so that allocating these roles does not compromise the need for division of duties where roles are incompatible. Where IT is outsourced, there is still a requirement for organizations to keep many of these roles in-house to provide oversight of the outsourced functions.

7.2.1 Chief Executive Officer

The individual with overall strategic and operational control of the organization must consider IT in most aspects of the role. In particular, the CEO will:

- Define corporate objectives and performance measures in relation to IT.
- Act as custodian over the organization's critical success factors in relation to IT.
- Understand and approve the short-term and long-range strategy for IT.
- Approve IT resources for the organization, including structure and oversight/monitoring.
- Determine IT issues for periodic management, board, and staff discussion.
- Operate as the highest-level control owner, having ultimate responsibility for the success or failure of controls and for coordinating all other operational managers within their responsibilities framework who act as control owners of their particular areas.

7.2.2 Chief Financial Officer

The CFO has overall responsibility for all financial matters in the organization and should have a strong understanding of the use of IT both to enable financial management and to support corporate objectives. This individual should have an overall understanding of:

- The total cost of ownership for IT initiatives.
- The entity's IT strategies for remaining technologically competitive.
- The technologies used to implement financial applications.
- The operation of specific financial applications.

IT Controls and Ethics

As evidenced in the Equity Funding cases in the 1970s to the scandals that continue to emerge today, the use of technology creates significant opportunities to initiate and perpetuate fraud and deception. The authority to override certain controls brings with it the temptation to initiate improper actions. If such improprieties go unnoticed, or are tacitly allowed to continue, they can grow into outright fraud. Therefore, when an organization provides an individual the opportunity to perform actions on behalf of the organization, it has a corresponding responsibility to provide monitoring to detect and correct improper activities quickly. The organization also has a responsibility to identify threats of this sort and to establish safeguards as a preventive measure.The same technology tools that can create the opportunity for fraud can be used to identify activities, or even unusual patterns, in transactions or other data that may indicate evidence of fraud or questionable behavior.

- The limitations and benefits of IT.
- The IT control structure for general controls that apply to all business systems and data as well as controls that are specific to financial applications.

The CFO should operate as the highest-level control owner for financial systems and data.

7.2.3 Chief Information Officer

The CIO has overall responsibility for the use of IT within the organization. In relation to IT controls, the CIO should:

- Understand the business requirements that drive the need to implement IT.
- Develop IT partnerships with business management to:
  - Ensure IT strategy is aligned with the business strategy.
  - Ensure compliance.
  - Profit from process-efficiency gains.
  - Mitigate assessed risks.
- Design, implement, and maintain an IT internal control framework.
- Plan, source, and control IT resources.
- Explore, assess, select, and implement technology advances (e.g. wireless communications).
- Provide training for IT personnel to ensure that levels of knowledge and skills remain current.
- Operate as the highest-level data/system custodian and IT control owner.
- Measure the operational performance of IT in support of business objectives by:
  - Setting expectations.
  - Evaluating results.
- Developing all necessary means to verify and acknowledge that IT is providing services and support as expected by its users and final customers such as regulators and external and internal auditors.

7.2.4 Chief Security Officer

The chief security officer (CSO) is responsible for all security across the entire organization, including information security, which may be the responsibility of a chief information security officer as well. The CSO:

- Has responsibility for documenting the enterprise security policy and for ensuring mechanisms have been established to communicate and enforce the policy.
- Has overall responsibility for logical and physical security in the organization and for all external connections to the Internet or other networks.
- Acts as a key link between the compliance, legal, CIO, and audit functions.
- Is at the forefront of implementing key compliance programs affecting IT, such as Sarbanes-Oxley and the European Union (EU) Data Protection Directive.
- Is responsible for business continuity planning, including incident handling and disaster recovery.
- Ensures that security staff provide support for implementing controls at all levels.
- Acts as the key leader for investigating and evaluating new best practices that may be incorporated into the organization.

7.2.5 Chief Information Security Officer (CISO)

Information security is a subset of the overall security role. The CISO:

- Develops and implements the information security policy in coordination with the CSO.
- Controls and coordinates information security resources, ensuring they are allocated adequately to meet the organization's security objectives.
- Ensures alignment of information security and business objectives.
- Manages operational information risks throughout the organization.
- Oversees security within the IT organization.
- Provides education and awareness on information security issues and new best practices.
- Develops end-user policies for the usage of IT information, in conjunction with the human resources function.
- Coordinates information security work with the chief risk officer (CRO) and CIO.
- Advises the CEO, CRO, CIO, and board on IT risk issues.
- Acts as a key link for the CAE when internal auditing performs IT control-related audits.

7.2.6 Chief Legal Counsel (CLC)

Legal counsel may be an employee or officer of the organization or an external legal adviser. The role involves:

- Understanding and dealing with the liabilities arising out of information disclosures and providing policy-level guidance to help manage risks related thereto.
- Ensuring financial reports and presentations comply with laws and regulations.
- Understanding IT legal issues and advising on legal risks related to IT.
- Managing organizational reputation in relation to legal issues, compliance, and public relations.
- Understanding fraud involving IT.
- Managing IT contractual issues.
- Understanding investigative forensics protocols regarding suspected criminal activity.

7.2.7 Chief Risk Officer

The CRO is concerned with managing risk at all levels of the organization. Because IT risks form a part of this function, the CRO will consider them, with the help of the CISO. This includes:

- Analysis and assessment of IT risk exposures, including information compromises such as loss,

damage, unauthorized disclosure, and interrupted access.
- Assessment of IT events such as interruptions, disasters, and changes.
- Analysis and assessment of business risk as it is affected by IT risk.
- Monitoring, supporting, and acting as a mentor for all IT activities related to minimizing risks.

7.3 Audit

7.3.1 Internal Auditing – CAE and Audit Staff

Internal auditing is an essential part of the corporate governance process, whether or not a specific internal audit group is employed. Internal auditors need a general understanding of IT, but the level of their understanding will vary depending on the category of auditing or audit supervision they perform (IIA Standard 1210.A3). The IIA defines three categories of IT knowledge for internal auditors. Appendix C (See page 28) describes these categories.

The internal audit role in relation to IT involves:

- Advising the audit committee and senior management on IT internal control issues.
- Ensuring IT is included in the audit universe and annual plan (selecting topics).
- Ensuring IT risks are considered when assigning resources and priorities to audit activities.
- Defining IT resources needed by the internal audit department, including specialized training of audit staff.
- Ensuring that audit planning considers IT issues for each audit.
- Liaising with audit clients to determine what they want or need to know.
- Performing IT risk assessments.
- Determining what constitutes reliable and verifiable evidence.
- Performing IT enterprise-level controls audits.
- Performing IT general controls audits.
- Performing IT applications controls audits.
- Performing specialist technical IT controls audits.
- Making effective and efficient use of IT to assist the audit processes.
- During systems development or analysis activities, operating as experts who understand how controls can be implemented and circumvented.
- Helping to monitor and verify the proper implementation of activities that minimize all known and documented IT risks.

7.3.2 External Auditor

Independent external audits are a requirement for most organizations and normally are performed annually. Topics to be considered by the internal audit department and the audit committee include:

- The extent of the external auditor's responsibilities for understanding and evaluating the IT system and related IT controls during financial audits.
- The scope of the external auditor's responsibilities for examining the IT system and controls during any formal attestation that may be required by statute or regulation, such as internal controls over financial reporting and other regulatory requirements.

8.1 Risk Determines Response

IT controls are selected and implemented on the basis of the risks they are designed to manage. As risks are identified — through experience or formal risk assessment — suitable risk responses are determined, ranging from doing nothing and accepting the risk as a cost of doing business to applying a wide range of specific controls, including insurance.

It would be a relatively straightforward task to create a list of recommended IT controls that *must* be implemented within each organization. However, each control has a specific cost that may not be justified in terms of cost effectiveness when considering the type of business done by the organization. Furthermore, no list of controls is universally applicable across all types of organizations. Although there is a lot of good advice available on the choice of suitable controls, strong judgment must be used. Controls must be appropriate for the level of risk faced by the organization.

The CAE should be able to advise the audit committee that the internal control framework is reliable and provides a level of assurance appropriate to the risk appetite of the organization. In this respect, the risk appetite of the organization is defined by COSO[3] as:

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

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

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

Thus, the CAE should consider whether or not:

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

8.2 Risk Considerations in Determining the Adequacy of IT Controls

Risk management applies to the entire spectrum of activity within an organization, not just to the application of IT. IT cannot be considered in isolation, but must be treated as an integral part of all business processes. Choosing IT controls is not simply a matter of implementing those recommended as best practices. They must add value to the organization by reducing risk efficiently and increasing effectiveness.

When considering the adequacy of IT controls within the organization's internal control framework, the CAE should consider the processes established by management to determine:

- The value and criticality of information.
- The organization's risk appetite and tolerance for each business function and process.
- IT risks faced by the organization and quality of service provided to its users.
- The complexity of the IT infrastructure.
- The appropriate IT controls and the benefits they provide.
- Harmful IT incidents in the past 24 months.

The frequency of risk analysis is important and is influenced greatly by technological change. In a static business and technical infrastructure environment, the risk assessment process could be as infrequent as yearly or could be performed in concert with a major implementation project.

8.2.1 The IT Infrastructure

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

The inventory of IT infrastructure components reveals basic information about the vulnerabilities of the environment. For example, business systems and networks connected to the Internet are exposed to threats that do not exist for self-contained systems and networks. Because Internet connectivity is an essential element of most business systems and networks, organizations must make certain that their systems and network architectures include the fundamental controls that ensure basic security.

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

[3] These definitions are taken from the COSO *Enterprise Risk Management – Integrated Framework* (Oct 2004)

8.2.2 IT Risks Faced by the Organization

The CAE discusses IT risk issues with the CIO and process owners to ensure that all related parties have an appropriate awareness and understanding of the technical risks faced by the organization through the use of IT and their roles in applying and maintaining effective controls.

8.2.3 Risk Appetite and Tolerance

Armed with the knowledge of IT risks, the auditor can validate the existence of effective controls to meet the established risk appetite of the organization and its risk tolerance in relation to IT. The auditor's assessment will involve discussions with many members of management and ultimately with the board. The level of detail of these discussions can be determined by the CRO with input from the CIO, CISO, CSO, CAE, and process owners. The final decision regarding risk appetite and tolerance must be made by the risk committee — with input from the audit committee — and must be endorsed by the full board. The definitions of *risk appetite* and *tolerance* must be communicated to all relevant managers for implementation.

The goal of enterprise risk management is to ensure that everyone is working with the same level and understanding of risk and that decisions made at all levels of management are consistent with the organization's risk appetite.

8.2.4 Performing Risk analysis

Performing risk analysis is not the sole preserve of either the CRO or the CAE, although both of them, or their representatives, should be involved, along with representatives from IT and the business areas.

There are eight basic questions associated with the risk assessment process. The first five include:

- What are the assets at risk and the value of their confidentiality, integrity, and availability?
- What could happen to affect that information asset value adversely (threat event)? Implicit to this question is the vulnerability analysis and mapping of vulnerabilities to threats and potentially impacted information assets.
- If a threat event happened, how bad could its impact be?
- How often might the event be expected to occur (frequency of occurrence)?
- How certain are the answers to the first four questions (uncertainty analysis)?

The next three questions apply to risk mitigation analysis:

- What can be done to reduce the risk?
- How much will it cost?
- Is it cost-efficient?

8.2.5 Value of Information

Determining the value of the information processed and stored is not an easy task due to the multidimensional nature of value. The Generally Accepted Information Security Principles (GAISP), *Guidelines for Information Valuation*, published by the Information Systems Security Association (www.ISSA.org), address information value within the following categories:

- Exclusive possession – cost in the event of a breach of confidentiality.
- Utility – cost in the event of a loss of integrity.
- Cost of creation/re-creation.
- Liability in the event of litigation.
- Convertibility/negotiability – represents market value.
- Operational impact of unavailability.

8.2.6 Appropriate IT Controls

Finally, appropriate IT controls must be chosen and implemented to address the risks identified. Much advice is available on this subject. See Appendix I (See page 45).

The CAE and internal audit group should be involved in the process of analyzing and assessing risk. While they should operate in a manner that maintains the independence and objectivity of their function, they also must provide an opinion on the effectiveness of the internal control framework.

8.3 Risk Mitigation Strategies

When risks are identified and analyzed, it is not always appropriate to implement controls to counter them. Some risks may be minor, and it may not be cost effective to implement expensive control processes for them.

In general, there are several ways to mitigate the potential impact of risks:

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

8.4 Control Characteristics to Consider

Some of the issues to be addressed during the IT control evaluation process include:

- Is the control effective?
- Does it achieve the desired result?
- Is the mix of preventive, detective, and corrective controls effective?
- Do the controls provide evidence when control parameters are exceeded or when controls fail? How is management alerted to failures, and which steps are expected to be taken?
- Is evidence retained (audit or management trail)?

8.5 Baseline IT Controls

IT controls are to be applied when mitigating the risks is the best option. While IT controls should be applied with due regard to the relevant risks, there is a basic set of controls that need to be in place to provide a fundamental level of IT hygiene. For example, the use of a firewall to control traffic between a corporate network and a public network such as the Internet, or between internal network domains, is a baseline control. The level of risk associated with the business value and sensitivity of the network traffic, the services provided, and the information stored in the infrastructure determines the extent to which firewalls restrict traffic coming into and departing from an organization's networks. Firewalls are a physical and logical manifestation of information security policy elements that dictate what is allowed into or out of an organization.

IT controls most widely applicable to all IT infrastructures are known as *baseline controls*. There are many types of baseline controls. Two baselines that apply to IT security controls are the Digital Dozen, from the VISA Cardholder Information Security Program (CISP) and the Fundamental Five, from the Center for Internet Security (see sidebars on this page). The Fundamental Five and Digital Dozen complement each other.

It is not easy to define the baseline IT controls, because the general threats, such as malicious software and hacking, change and newer technologies and applications frequently are implemented across the organization. The following questions can be considered when selecting a suitable set of baseline controls:

- Do IT policies — including for IT controls — exist?
- Have responsibilities for IT and IT controls been defined, assigned, and accepted?
- Are IT infrastructure equipment and tools logically and physically secured?
- Are access and authentication control mechanisms used?
- Is antivirus software implemented and maintained?
- Is firewall technology implemented in accordance with policy (e.g., where external connections such as the Internet exist and where separation between internal networks is needed)?
- Are external and internal vulnerability assessments completed and risks identified and appropriately resolved?
- Are change and configuration management and quality assurance processes in place?
- Are structured monitoring and service measurement processes in place?
- Are specialist IT audit skills available (either internally or outsourced)?

Further information on baseline controls can be found in Appendix I (See page 45). More comprehensive information on risk analysis and management can be found in the IIA paper *Information Security Management and Assurance: A Call to Action for Corporate Governance*. http://www.theiia.org/eSAC/pdf/BLG0331.pdf.

Digital Dozen

One of the most concise and broadly useful summaries of security guidance is the VISA CISP, which has proven its value for over two years in use by VISA credit card network service providers, including banks, processors, merchants, and others. VISA refers to these requirements as its "Digital Dozen."

1. *Install and maintain a working firewall to protect data.*
2. *Keep security patches up-to-date.*
3. *Protect stored data.*
4. *Encrypt data sent across public networks.*
5. *Use and regularly update anti-virus software.*
6. *Restrict access by "need to know."*
7. *Assign an unique Identification Code (ID) to each person with computer access.*
8. *Don't use vendor-supplied defaults for passwords and security parameters.*
9. *Track all access to data by unique ID.*
10. *Regularly test security systems and processes.*
11. *Implement and maintain an information security policy.*
12. *Restrict physical access to data.*

Fundamental Five

The Consensus Benchmarks, from the Center for Internet Security (www.cisecurity.org), provide guidance on the "Fundamental Five" of basic security hygiene. Use of these benchmarks typically results in an 80 percent to 95 percent reduction of known vulnerabilities.

1. *Identity and Access Management (including privilege assignment and authentication)*
2. *Change Management (including patch management)*
3. *Configuration Management*
4. *Firewalls (workstation, host, sub-network, and perimeter)*
5. *Malware protection (including worms and viruses)*

9.1 Choosing a Control Framework

The process of identifying and assessing the IT controls necessary to address specific risks is aided considerably by the organization's adoption of a formal control framework. This framework should apply to, and be used by, the whole organization — not just internal auditing. Although many frameworks exist, no single framework covers every possible business type or technology implementation.

A control framework is a structured way of categorizing controls to ensure that the whole spectrum of control is adequately covered. The framework can be informal or formal. A formal approach will satisfy the various regulatory or statutory requirements faced by many organizations more readily .

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

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

Finally, the assessment of IT controls involves selecting key controls for testing, evaluating test results, and determining whether or not evidence indicates any significant control weaknesses. The checklist in Appendix H can help the CAE ensure all relevant issues have been considered when planning and directing internal audit assessments of IT controls. Several existing frameworks and approaches can assist the CAE and other managers when determining IT control requirements. However, organizations should investigate enough frameworks to determine which one best fits their own needs and culture. A partial list of available frameworks is provided in Appendix D (See page 29).

The COSO *Internal Control – Integrated Framework* (1992) is accepted by the U.S. Public Company Accounting Oversight Board (PCAOB) for the purpose of reporting

COSO Model for Technology Controls

Monitoring:
- Monthly metrics from technology performance
- Technology cost and control performance analysis
- Periodic technology management assessments
- Internal audit of technology enterprise
- Internal audit of high risk areas

Control Activities:
- Review board for change management
- Comparison of technology initiatives to plan and return on investment
- Documentation and approval of IT plans and systems architecture
- Compliance with information and physical security standards
- Adherence to business continuity risk assessment
- Technology standards compliance enforcement

Information and Communication:
- Periodic corporate communications (intranet, e-mail, meetings, mailings)
- Ongoing technology awareness of best practices
- IT performance survey
- IT and security training
- Help desk ongoing issue resolution

Risk Assessment:
- IT risks included in overall corporate risk assessment
- IT integrated into business risk assessments
- Differentiate IT controls for high risk business areas/functions
- IT Internal audit assessment
- IT Insurance assessment

Control Environment:
- Tone from the top – IT and security controls considered Important
- Overall technology policy and Information security policy
- Corporate Technology Governance Committee
- Technology Architecture and Standards Committee
- Full representation of all business units

Figure 5 - COSO Model for Technology Controls

compliance with financial reporting provisions, but it is not specific to all areas of IT. This framework is considered to be a "suitable, recognized" framework to adopt for Sarbanes-Oxley compliance because it covers all areas of IT implementation, albeit at a high level of abstraction (See Figure 5, COSO Model for Technology Controls, page 18).

9.2 Monitoring IT Controls

Determining where to apply control monitoring and assessment and their frequency is not easy. Participation by the auditor in risk analysis exercises and implementation of a suitable control framework help ensure that the CAE has sufficient information to create a suitable audit plan to address the major IT risks.

Ultimately, management is responsible for monitoring and assessing controls. The auditor's monitoring and assessments are performed to independently attest to management's assertions regarding the adequacy of controls. Management's control monitoring and assessment activities should be planned and conducted within several categories as follows:

9.2.1 Ongoing Monitoring

- **Daily/Periodic** – Some information must be checked daily to ensure controls are working as required. Management normally performs such monitoring, which traditionally involves checking data-processing control reports to reconcile satisfactory task and job completion. Such controls, where they exist, are most often automated. The CAE will ensure such management monitoring is in place and that it is subjected to internal audit assessment.
- **Event-driven** – Discrepancies, or even frauds, may result within normal processing or in special circumstances, such as where there are large-value transactions. In many IT environments, malicious attacks are likely. Consequently, specific controls should be in place to detect and report unusual activities to an entity within the organization that is chartered specifically to investigate and determine if preventive or corrective actions should be applied. Such monitoring controls are complementary to the normal controls employed and provide assurance on the effectiveness of those controls or early warning that they may have been breached.
- **Continuous** – Technology now provides the ability to monitor and assess certain sensitive controls continuously. A good example of continuous monitoring is the use of intrusion detection software, which continually monitors network traffic for evidence that other protective controls, such as firewalls and virus protection, may have been breached.

9.2.2 Special Reviews

- **Annual (or quarterly) control assessment** – Sarbanes-Oxley legislation in the United States requires cyclical control assessments. Although the board of directors is required to make statements regarding the effectiveness of internal controls, management actually must provide the assurances to the board, and the internal and external auditors must perform sufficient audit work to attest to these assurances.
- **Audit reviews** – A regular program of audit reviews is still necessary, despite the proliferation of new audit approaches. It is only through the formal review of infrastructure, process, and technology implementation that the CAE can assess the overall reliability and robustness of the system of internal controls. In the past, such reviews were planned on a cyclical basis. However, given the fast-changing world of IT, audit reviews should now be scheduled based on the level of risk.

Suitable Recognized Framework

"….the framework on which management's assessment of the issuer's internal control over financial reporting is based must be a suitable, recognized, control framework that is established by a body or group that has followed due-process procedures, including the distribution of the framework for public comment. By far, the best-known framework that meets that definition is the framework designed by The Committee of Sponsoring Organizations of the Treadway Commission, otherwise known as the COSO report, which was published in 1992."

— Scott A. Taub, Deputy Chief Accountant, U.S. Securities and Exchange Commission (SEC), SEC and Financial Reporting Conference, Pasadena, California, May 29, 2003

10.1 What Audit Methodology to Use?

A lot has changed in the 40 years that IT auditing has existed: Technology components have become smaller, faster, and cheaper even as overall IT costs to the organization have increased significantly. The majority of business processes have been automated, typically to provide efficiencies, but also to enable certain business processes that cannot be performed manually. Ubiquitous network communications, including the Internet, have eliminated any distinction between business and electronic business.

The audit process similarly has evolved to match the automation of business processes. In the early days of automation, auditors "audited around the computer." Now they use software routinely to test or analyze data and technical controls within systems.

A widely used audit approach involves operational analysis of the processing of important business transactions by automated systems. In such audits, the auditor identifies activities and information subject to control and assesses the ability of existing controls to provide reliable protection — including sufficient evidence of the reliability of controls. Because operational audits of automated business processes frequently identify internal control deficiencies, internal auditors may sometimes shift their attention to audits of — or even involvement in — the processes whereby business activities are automated, such as systems design, development and acquisition, implementation, and maintenance.

Experienced auditors develop extensive knowledge of internal controls and their strengths and weaknesses. Therefore, it is not uncommon for internal auditors to provide consulting services to the management responsible for designing and implementing internal controls. The scope and limitations on such consulting activity are prescribed in the *International Standards for the Professional Practice of Internal Auditing* (See http://www.theiia.org/iia/index.cfm?doc_id=124.). However, internal auditor involvement in design, development, or implementation activities does not absolve management from responsibility for those activities.

Today, no specific audit methodologies can be regarded as the sole current best practice. Internal auditors adopt the methods and practices that best suit the work needed. For example:

- When performing an assessment against Sarbanes-Oxley requirements, a systems-based audit approach may be the best method.
- Fraud investigations may require the use of audit software to analyze data and look for evidence. Audit software provides strong analytical capability, plus the ability to examine all relevant records and files.
- Performing annual audit work in support of the main internal audit objectives will most likely follow a risk-based approach.

10.2 Testing IT Controls and Continuous Assurance

In addition to assessing the adequacy of IT control mechanisms, regular reviews should be performed to ensure that controls continue to function as required. A traditional method used by internal auditors is to create a population of test data that can be processed through the business systems to check the results to ensure, for example, that controls continue to accept valid data and reject incorrect and invalid items. However, given the widespread, complex, and interactive nature of business systems today, audit testing tends to focus more specifically on key automated controls and analysis of the data.

10.2.1 Automated Continuous Monitoring

Continuous monitoring and audit tools have been used for many years. Previously called *embedded audit software*, program code in business systems checks data being processed against predetermined criteria and reports anomalies it detects. The benefit of such monitoring is obvious: Any discrepancies can be identified and acted upon immediately. Many proprietary business software products now provide such continuous monitoring functionality. The concept has also gone beyond business applications. For example, most firewall products and intrusion detection systems continu-

How Auditing Contributes to IT Controls

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

ously check for potential attack scenarios and provide instant alerts when potential attacks are detected. This type of monitoring can cause problems due to the considerable volume of data and potential errors that are highlighted, not all of which will be worthy of attention. The task of refining the analysis techniques and monitoring thresholds requires constant vigilance to determine which alerts to highlight and which to accept as normal events.

10.2.2 Automated Internal Control Analysis Tools

Audit software can be used to analyze stored data and check its validity to ensure the continuous, reliable operation of internal controls. Originally designated *audit interrogation software*, products such as ACL (www.acl.com) or CaseWare IDEA (www.caseware.com) now provide sophisticated features and specific analysis that can reduce the control assessment workload while increasing effectiveness and efficiency. Spreadsheet products like Microsoft Excel also contain powerful analysis tools auditors may use.

10.2.3 Automated Risk Analysis

Tools also are available for automating the risk analysis process. These tools are invaluable to the entire internal audit function, not just the IT auditor or risk specialist. Performing a proper risk analysis in today's complex IT environments is not easy without the assistance of automated tools.

Management is responsible for performing risk assessments to determine the controls to implement or improve. Internal auditors perform similar analysis when assessing the adequacy of controls for audit plan and scope purposes. Automated tools can assist both processes. The automation of internal audit management is a major topic in its own right.

10.3 Audit Committee/Management/ Audit Interfaces

It is impractical to establish rules for reporting on every special IT control situation. The CAE must apply prudent judgment when expressing an opinion or submitting a report to the audit committee. This is no different from the way the CAE interacts with the audit committee regarding other internal control issues.

The CAE will discuss internal control issues with the audit committee to determine the optimum level of information to be provided to enable the audit committee to achieve its statutory, regulatory, policy, due care, or other governance obligations.

"Metrics and reporting" and "audit report summaries" are two areas where the CAE should interact with the audit committee regarding internal controls. Further interactions will depend on the needs of the specific audit committee and any legislative or regulatory requirements.

Metrics and reporting. Metrics and reports must present meaningful information on the status of IT controls. While management provides the metrics and reporting, the CAE should be able to attest to their validity and opine on their value. This is accomplished through audit examination of the relevant control areas to produce an independent and objective assessment. The CAE should liaise with management at all levels and with the audit committee to agree on the validity and effectiveness of the metrics and assurances chosen for reporting.

A basic set of governance and management metrics for information security is included in Appendix G (See page 40). These metrics do not include specific data regarding the operation of detailed technical controls, although the technical controls may provide the information used in measurement. The actual metrics used will depend on the organization and the needs of the audit committee. The CAE can select examples of measurements taken at any level of the organization to help illustrate matters that can impact controls at the governance level materially.

Audit Report Summaries. Prepared on a regular basis for the audit committee, these reports summarize findings, conclusions, and opinions regarding the status of IT controls. They also can report on the agreed-upon actions from prior audit reports and the status of those actions — probably on an exception basis for actions not taken within the designated time frame. IT controls summaries cannot be presented in isolation, but should be presented in the context of the entire internal control framework.

The frequency of reporting depends on the organization's needs. In a strong regulatory environment, such as provided by Sarbanes-Oxley in the United States, quarterly reporting is required. Otherwise, the frequency of reporting will be driven by the organization's governance framework and philosophy and the extent to which IT risks exist.

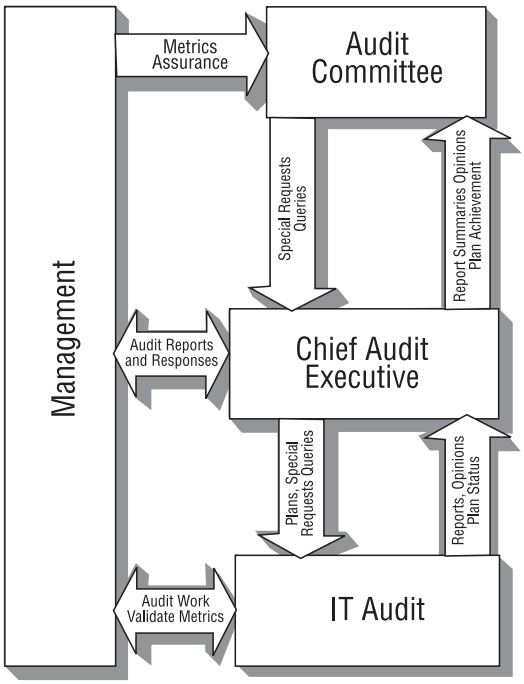


Figure 6 – Audit Interfaces

Assessing IT controls is an ongoing process, because business processes are constantly changing, technology continues to advance, threats evolve as new vulnerabilities emerge, and audit methods keep improving. The CAE should keep assessments of IT controls that support business objectives near the top of the audit agenda.

Assessing IT controls is not a case of determining whether best practices are employed, as controls are specific to the organization's mission, objectives, culture, deployed processes and technologies, and risks. Technology should be tailored to provide effective control, and the CAE should ensure internal auditing adopts appropriate and effective methods. Auditing IT is a continuous learning process.

The CAE is rarely in a position to understand all the technologies used in his or her environment and their specific control implications. That is why properly certified and experienced IT auditors are a major asset for any internal audit function. However, the CAE should understand the overall control issues and be able to communicate them to senior management and to appropriate committees of the board of directors in a form they will understand and in a manner that will result in an appropriate response. The key to assessing IT controls effectively is communication with technical staff, management, and board members.

Note: This appendix is extracted from the report of the Best Practices and Metrics team of the Corporate Information Security Working Group (CISWG) as provided on November 17, 2004 to the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census; Government Reform Committee; U.S. House of Representatives and subsequently amended on January 10, 2005. Additional information may be obtained from the "Technology" section of http://www.theiia.org

12.1 Governance (Board of Directors):

- Oversee risk management and compliance programs pertaining to information security (e.g., Sarbanes-Oxley, Health Insurance Portability and Accountability Act, Gramm-Leach-Bliley Act).
- Approve and adopt broad information security program principles and approve assignment of key managers responsible for information security.
- Strive to protect the interests of all stakeholders dependent on information security.
- Review information security policies regarding strategic partners and other third parties.
- Strive to ensure business continuity.
- Review provisions for internal and external audits of the information security program.
- Collaborate with management to specify the information security metrics to be reported to the board.

12.2 Management

- Establish information security management policies and controls and monitor compliance.
- Assign information security roles, responsibilities, and required skills, and enforce role-based information access privileges.
- Assess information risks, establish risk thresholds, and actively manage risk mitigation.
- Ensure implementation of information security requirements for strategic partners and other third parties.
- Identify and classify information assets.
- Implement and test business continuity plans.
- Approve information systems architecture during acquisition, development, operations, and maintenance.
- Protect the physical environment.
- Ensure internal and external audits of the information security program with timely follow-up.
- Collaborate with security staff to specify the information security metrics to be reported to management.

12.3 Technical

Establishing a complete information security program requires attention to the following technical program elements:

- User identification and authentication.
- User account management.
- User privileges.
- Configuration management.
- Event and activity logging and monitoring.
- Communications, e-mail, and remote access security.
- Malicious code protection, including viruses, worms, and trojans.
- Software change management, including patching.
- Firewalls.
- Data encryption.
- Backup and recovery.
- Incident and vulnerability detection and response.
- Collaboration with management to specify the technical metrics to be reported to management.

There is an increasing volume of legislation impacting on the internal control framework that organizations choose to implement. Although much of this legislation has emerged over recent years in the United States as a result of various corporate scandals, it has impacted organizations in other countries, as well. Organizations should be aware of the relevant legislation, regulation, and business practices around the world — particularly in all countries in which they do business — to assess the organizational impacts and requirements.

For example, data protection legislation in Europe inhibits the transfer of information across borders to countries that do not have comparable data-protection regulation in place. This impacts trading relationships where the information to be transferred refers to identifiable individuals. Sarbanes-Oxley contains requirements for reporting on the system of internal controls for all organizations publicly traded in the United States, as well as their foreign subsidiaries.

This appendix provides a summary of requirements and the impact of some of the major legislation and regulation that should be considered in assessing and managing IT controls. Although this GTAG is aimed at a global audience, it covers Sarbanes-Oxley in some depth because it is one of the most significant pieces of legislation to emerge in recent years. The Organisation for Economic Co-operation and Development (OECD) Corporate Governance Principles provide a general framework for the implementation of business controls. The Basel II Accords have a major impact on the international financial sector, and many have suggested Basel II guidance may also influence other sectors.

13.1 U.S. Sarbanes-Oxley Act of 2002

Sarbanes-Oxley (http://www.theiia.org/iia/guidance/issues/sarbanes-oxley.pdf) was intended to reform public accounting practices and other corporate governance processes and shore up the capital markets in the wake of the Enron and WorldCom corporate governance scandals. The PCAOB provides a comprehensive collection of information and advice on Sarbanes-Oxley at its Web site (http: www.sarbanes-oxley.com/). The key requirements of Sarbanes-Oxley, the SEC, and U.S. stock listing exchanges are fully compared and contrasted in an IIA Research Foundation analysis titled "Assessment Guide for U.S. Legislative, Regulatory, and Listing Exchanges Requirements Affecting Internal Auditing" (www.theiia.org/iia/download.cfm?file=519).

However, Sarbanes-Oxley does not address the issue of IT controls specifically. This does not mean IT can be ignored when performing the compliance reviews required by the act. The act is neutral with regard to technology, but the implication is clear that IT controls are critical to an organization's overall system of internal controls. As IT controls address the secure, stable, and reliable performance of hardware, software, and personnel to ensure the reliability of financial applications, processes, and reporting, they must be a significant element of compliance reviews.

Some key IT control areas have been interpreted as not being incorporated in Sarbanes-Oxley compliance. These include privacy, business continuity, business systems, data classification, and information not specific to financial processing and reporting. Therefore, any audit specifically limited to Sarbanes-Oxley compliance will not assess all the risks faced by the organization and must be supplemented to ensure full audit coverage of the organization's risk management and internal controls.

Tools and resources for corporate governance initiatives and current legislation can be found on The IIA's Web site at http://www.theiia.org/iia/index.cfm?doc_id=4061.

13.1.1 Sarbanes-Oxley Sections Relevant to IT Controls

The following briefly describes the sections of Sarbanes-Oxley that relate to auditors and IT controls.

13.1.1.1 Sections 103 and 802

These sections establish rules for the public accounting firm relating to the audit and report. In particular, they require the board to establish standards for the audit work. They also require auditors to test the internal control structures and attest to the strength of those structures. This review must include a thorough examination of the IT controls that are fundamental to the system of internal control over financial reporting.

One specific requirement relates to the retention of records "that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets." Again, this is influenced greatly by the way in which IT records are maintained and retained.

13.1.1.2 Section 201

This section requires that external auditors be independent. This precludes them from performing work for a client in the capacity of IT consultants or providing outsourced internal audit services. Organizations that do not wish to employ their own IT auditors cannot outsource the work to their external auditors.

13.1.1.3 Section 301

Section 301 defines the need for audit committee members to be independent and precludes them from performing any other consulting work on behalf of the organization. It also requires audit committees to establish procedures to handle "confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters" (whistle-blower complaints). This would also relate to any issues arising from the control of IT.

13.1.1.4 Section 302 and 404

Section 302 of the act requires the CEO and CFO — who

are responsible for financial information and the system of internal controls — to evaluate the system of internal controls every 90 days and report on their conclusions and any changes.

They must disclose:

- "All significant deficiencies in the design or operation of internal controls that could adversely affect the issuer's ability to record, process, summarize, and report financial data and identify for the issuer's auditors any material weaknesses in internal controls."
- "Any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls."

Section 404 requires the CEO and CFO to produce an annual audit report that:

- Assesses the effectiveness of the internal control structure over financial reporting.
- Discloses all known internal control weaknesses.
- Discloses all known frauds.

This report will cover all applicable IT controls, including program logic and related change controls, access controls, and data protection. The PCAOB Auditing Standard No. 2 suggests the COSO *Internal Control – Integrated Framework* as a basis for Section 404 compliance management. References to Statement of Auditing Standards (SAS) 95 also emphasize the importance of IT and information security controls to Sarbanes-Oxley.

13.1.1.5 Section 409

Section 409 requires organizations to disclose any material changes to operations in real time and in plain English. Some contend these requirements establish a foundation or need for continuous monitoring, auditing, and assurance processes to become part of significant internal control processes.

13.2 Basel II Accord

The Basel II Accord is a global regulatory treaty that defines the global standards for enterprisewide risk management practices in the financial sector with the intent to mitigate risks of losses in the industry. The focus is on the banking sector, but there is a clear intent to harmonize standards across all segments of the industry. All areas of bank operations are included — people, processes, systems, governance, and supplier management.

A bank willing to qualify for the Advanced Measurement Approach (AMA) under the Operational Risk (OR) Treaty must implement best practice in operations and risk management. For risk management, this means:

- Senior management is actively involved.
- The bank has an OR management system, processes, policies, and procedures enterprisewide.
- The bank has the right governance and sufficient resources to manage operational risks.
- The bank has an OR management function that is responsible for:
  - Designing and implementing the OR management framework.
  - Codifying policies, procedures, and controls.
  - Designing and implementing an OR measurement methodology.
  - Designing and implementing an OR management reporting system.
  - Developing strategies to identify, measure, monitor, and control or mitigate OR.
- An OR measurement system is closely integrated into the day-to-day risk management process.
- The OR exposures and loss experiences are regularly reported.
- The OR management system is documented.
- Internal and external auditors regularly review the OR management processes and measurement system.

Key to success in OR management is an information system that supports OR exposure self-assessment, allows process mapping, consists of an OR loss database and reporting function, and entails an action-plan management function.

The Basel Committee does not specify the approach or distributional assumptions to be used to generate the OR measure for regulatory capital purposes. However, the framework allows for three basic approaches that essentially are dependent on the quality and quantity of risk management data. Whereas using more data and historical metrics to prove good performance may allow banks to maintain less capital reserves and to quantify OR, the banks must be able to demonstrate that their approaches capture potentially severe "tail" loss events (severe unexpected losses). Moreover, consistency with the scope of OR as defined by the Basel Committee is required.

First, a bank's organization-wide risk assessment methodologies must capture key business environmental and internal control factors that can change its OR profile. In addition, the bank should have a process for assessing overall capital adequacy.

Next, the risk measurement system must be granular enough to capture the tails of the loss estimates. Banks are expected to use expert opinion in conjunction with external data for scenario analysis to evaluate its exposure to high-severity events. Because a bank does not have enough of its own data in the area of high-impact, low-frequency risks, they must acquire data from an external provider such as Zurich-based ORX, Global Operational Loss Database (GOLD), or MORE Exchange.

The banks must have a credible, transparent, well-documented, and verifiable approach for weighting these fundamental elements in its overall OR measurement system. There are additional prerequisites to qualify for the AMA.

- Internal loss and performance data — successes, near misses, and failures — all must be tracked and accounted for (reconciled to the books of the bank).

- Internal loss data must be linked to the bank's current business activities.
- An observation period of at least five years is required for internal loss data, with a minimum of three years necessary when moving to AMA.
- According to the internal loss collection process:
  - OR losses related to credit risk and historically included in banks' credit risk databases continue to be treated as credit risk for the purpose of calculating minimum regulatory capital under this framework. Such losses should be flagged separately.
  - OR losses related to market risk are treated as OR for the purposes of calculating minimum regulatory capital under this framework and are subject to the OR capital charge.
- The OR measurement system must use relevant external data.

Third, Basel II disclosure requires banks to describe their risk management objectives and policies for each separate risk area, including:

- Strategies and processes.
- Structure and organization of the risk management function.
- Scope and nature of risk reporting.
- Policies for hedging and mitigating risks (including operations).

Note: The BITS Key Risk Measurement Tool for Information Security Operational Risks, or "BITS Kalculator" (http://www.bitsinfo.org/bitskalculator july04.pdf), is a tool financial institutions of all sizes can use to evaluate critical information security risks to their businesses. It can be downloaded at no cost from the BITS Web site (http://www.bitsinfo.org/wp.html).

13.3 Data Protection

The concept of data protection was developed when computerization issues were raised at United Nations and OECD conferences in the late 1960s. The first national law was enacted in 1974 in Sweden, and the OECD published its Data Protection Guidelines in 1980 (OECD C (80) 58 final). Regional bodies like the Council of Europe (Data Protection Convention 108/1981, human rights-based) and the European Commission (EC) (Directive 95/46/EC, consumer protection-oriented) have enacted binding frameworks for implementation in their member states. Depending on their legal system, many countries around the globe have constitutional provisions and omnibus laws or a broad spectrum of sector regulations for data protection. To bridge the differences in U.S. and European Union (EU) privacy regulations, the EC and the U.S. Department of Commerce developed a safe harbor framework for U.S. companies. The safe harbor is a framework agreement consisting of seven principles and a series of frequently asked questions. (See also: http://www.was4.hewitt.com/hewitt/resource/legislative_updates/europe/eu_data1.htm).

The EU legislation requires organizations to protect the personal information of individuals. The legislation also mandates that appropriate technical measures be taken to ensure the security of personal data, whether electronic or manual. Further information regarding data protection can be found at the Electronic Privacy Information Center (EPIC) (http://www.epic.org), Privacy International (http://www.privacyinternational.org), and the UK Office of the Information Commissioner (http://www.information commissioner.gov.uk/).

13.4 The U.S. Gramm-Leach-Bliley Act (GLBA) - The Financial Modernization Act of 1999

The GLBA was introduced to protect the privacy of customer information in the financial sector, but it extends beyond financial companies. Any company that handles non-public financial customer information may be held accountable under this law, depending on the circumstances. More information is available from EPIC (http://www.epic.org/privacy/glba/) and the U.S. Federal Trade Commission (http://www.ftc.gov/bcp/conline/pubs/buspubs/glblong.htm-whois).

13.5 U.S. Health Insurance Portability and Accountability Act (HIPAA) 1996

HIPAA contains requirements for the privacy of personal information and for information security. The law applies to US-based companies in the health care sector, but can also pertain to any company that provides health care benefits to employees, depending on the circumstances. Further details can be found at http://www.hipaa.org.

13.6 California Security Breach Information Act, Civil Code Sections 1798.29 and 1798.82 (Frequently Referenced by the Bill – CA SB 1386)

California's State Bill 1386 amended the Information Practices Act of 1977 of the California Civil Code to create a sweeping regulation that mandates public disclosure of computer-security breaches in which confidential information of any California resident may have been compromised. Every enterprise — public or private — doing business with California residents is potentially affected. Confidential information covered by the law includes Social Security numbers, California driver's license numbers, account numbers, and credit or debit card numbers. A more detailed article on this regulation can be found at http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5501.Although case law for this legislation is not cited here, some discussions on the subject have indicated the courts may not view an organization's statement favorably if it treats its California customers differently from its other customers.

13.7 Global National Regulations

Many countries have national regulations covering internal control, including Germany (KonTraG, risk management requirement) and France (LSF, internal control reporting requirement). In addition, external auditors may be required to certify the adequacy of financial reporting mechanisms and controls. Although most of these regulations do not address IT directly, they imply the need for an adequately controlled IT infrastructure. For this reason many national bodies of the International Federation of Accountants (IFAC) provide detailed guidance for evaluating IT controls.

14.1 Auditor Knowledge Considerations

Standard 1210 – Proficiency of The IIA's *Standards* require that the internal audit activity collectively should possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities[4]. Varying levels of IT knowledge are needed throughout the organization to provide a systematic, disciplined approach to evaluating and improving the effectiveness of risk management, control, and governance processes. Knowledge of how IT is used, the related risks, and the ability to use IT as a resource in the performance of audit work is essential for auditor effectiveness at all levels.

The IIA's International Advanced Technology Committee has identified three categories of IT knowledge for internal auditors.

14.1.1 Category 1 – All Auditors

Category 1 is the knowledge of IT needed by all professional auditors, from new recruits up through the CAE. Basic IT knowledge encompasses understanding concepts such as the differences in software used in applications, operating systems and systems software, and networks. It includes comprehending basic IT security and control components such as perimeter defenses, intrusion detection, authentication, and application system controls. Basic knowledge includes understanding how business controls and assurance objectives can be impacted by vulnerabilities in business operations and the related and supporting systems, networks, and data components. It is fundamentally about ensuring that auditors have sufficient knowledge to focus on understanding IT risks without necessarily possessing significant technical knowledge.

14.1.2 Category 2 – Audit Supervisors

Category 2 applies to the supervisory level of auditing. In addition to having basic IT knowledge, audit supervisors must understand IT issues and elements sufficiently to address them in audit planning, testing, analysis, reporting, follow-up, and assigning auditor skills to the elements of audit projects. Essentially, the audit supervisor must:

- Understand the threats and vulnerabilities associated with automated business processes.
- Understand business controls and risk mitigation that should be provided by IT.
- Plan and supervise audit tasks to address IT-related vulnerabilities and controls, as well as the effectiveness of IT in providing controls for business applications and environments.
- Ensure the audit team has sufficient competence — including IT proficiency — for audits.
- Ensure the effective use of IT tools in audit assessments and testing.
- Approve plans and techniques for testing controls and information.
- Assess audit test results for evidence of IT vulnerabilities or control weaknesses.
- Analyze symptoms detected and relate them to causes that may have their sources in business or IT: planning, execution, operations, change management, authentication, or other risk areas.
- Provide audit recommendations based on business assurance objectives appropriate to the sources of problems noted rather than simply reporting on problems or errors detected.

14.1.3 Category 3 – Technical IT Audit Specialists

Category 3 applies to the technical IT audit specialist. Although IT auditors may function at the supervisory level, they must understand the underlying technologies supporting business components and be familiar with the threats and vulnerabilities associated with the technologies. IT auditors also may specialize in only certain areas of technology.

IIA programs and products are designed primarily to meet the information needs of the Category 1 and 2 auditor. The Category 1 auditor will seek IIA guidance in relating IT threats, vulnerabilities, and controls to business assurance objectives. IIA products also provide information that can be useful in explaining the business impacts of technical problems. In addition, IIA products can help Category 3 technical IT auditors gain proficiency in areas of technology with which they are not already familiar and in striving to reach supervisory or management audit competence.

The SANS Institute provides information security training and awards Global Information Assurance Certification (GIAC) relevant to information security professionals, including auditors. The course offerings and accompanying certifications match the growing demands of students, new threats, and new technologies. GIAC certifications (http://www.giac.org/subject_certs.php) are grouped by subject matter and level of difficulty. Some are full certifications that accompany five-to six-day training courses, while others are certificates related to one-to two-day courses. Certificates are less involved but more intensely focused than certifications.

Also of interest and benefit to all categories of IT auditor are the materials provided by the Information Systems Audit and Control Association (ISACA). ISACA offers standards, guidelines, and procedures for IT audit professionals; technical research focused on IT audit topics; the Certified Information Systems Auditor (CISA) certification, earned by more than 35,000 individuals worldwide; and publications, education, and conferences targeted to IT audit professionals.

[4]Note: The "Three Categories of IT Knowledge for Internal Auditors" document is not part of The IIA's *Standards*, but is practical guidance provided by The IIA's International Advanced Technology Committee.

15.1 COSO

Formed in 1985, COSO is an independent private-sector initiative that studied the factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, the SEC and other regulators, and educational institutions. COSO produced the *Internal Control – Integrated Framework* Appendix E, (See page 36), a widely accepted tool for both management and auditors, in September 2004, and it published *Enterprise Risk Management – Integrated Framework* in fall 2004. Details of both frameworks can be found at http://www.coso.org.

15.2 CICA CoCo

The Canadian Institute of Chartered Accountants (CICA) produced the *Criteria of Control Framework* (CoCo) in 1992 to address public and institutional concerns that the traditional view of control was no longer effective in preventing corporate failures. The mission of CoCo is to improve organizational performance and decision making through better understanding of control, risk, and governance. Moreover, the framework provides a basis for making judgments about the effectiveness of control.

In 1995, *Guidance on Control* was produced, which describes the CoCo framework and defines control in a way that goes beyond the traditional internal control over financial reporting. The CoCo model is a way of focusing on the future of an organization to ensure it is in control by having a clear sense of shared purpose, collective commitment to achieve that purpose, the resources it needs to do the job, and the ability to learn from experience.

15.3 CICA IT Control Guidelines

The *IT Control Guidelines*, published by the CICA, is a reference source for evaluating IT controls. It is organized in a manner that is easy to use and written in straightforward business language.

15.4 ITGI Control Objectives for Information and Related Technology (CobiT)

Established in 1998, the IT Governance Institute (ITGI) provides guidance on current and future issues related to IT governance, security and assurance. The ITGI's leading guidance publication is *Control Objectives for Information Technology* (CobiT) (See Appendix F). ITGI's CobiT provides a reference framework and common language across the entire information systems life cycle for IS and business leaders and IS audit, control, and security practitioners. CobiT is one of the most popular and internationally accepted set of guidance materials for IT governance.

15.5 ISO 17799 (Code of Practice for Information Security Management)

ISO/IEC 17799:2000(E), promulgated by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), defines information security principles that ultimately can provide assurance to trading partners and regulators that an organization's information is protected properly. Derived from the British Standards Institution's BS 7799 standard, the Code of Practice for Information Security Management is built around specific security elements required within 10 areas, including physical and environmental security, communication and operational management, and access control. Although as a code of practice, ISO/IEC 17799:2000 provides guidance and recommendations, it is not intended to be a specification, and care should be taken to ensure that claims of compliance are not misleading.

The original BS 7799 standard has two parts:

- Part 1 is the Code of Practice and is identical to ISO/IEC 17799:2000.
- Part 2 is a specification for implementing an information security management system (ISMS).

To comply with BS 7799 Part 2 (BS 7799-2:2002) an organization's installed ISMS must conform to the set of requirements described in the standard, which are in the form of *shall* statements. Third-party bodies have been accredited to certify, or register, organizations to BS 7799-2:2002.

15.5.1 What Is Information Security?

BS 7799 treats information as an asset, which like other important business assets, has value to an organization and consequently needs to be protected. Information security protects information from a wide range of threats to ensure business continuity, minimize business damage, and maximize return on investments and business opportunities.

Information can exist in many forms: printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, BS 7799 indicates that it always should be protected appropriately.

Information security is characterized within BS 7799 as the preservation of:

- **Confidentiality** – ensuring that information is accessible only to those authorized to have access.
- **Integrity** – safeguarding the accuracy and completeness of information and processing methods.
- **Availability** – ensuring that authorized users have access to information and associated assets when required.

Information security is achieved by implementing a suitable set of controls from BS 7799, which could be policies, practices, procedures, organizational structures, and software functions. These controls should be established to ensure the specific security objectives of the organization are met.

15.5.2 How to Establish Security Requirements

BS 7799 states that it is essential that an organization

identify its security requirements. There are three main sources:

- Assessing risks to the organization. BS 7799 does not prescribe a methodology.
- The legal, statutory, regulatory, and contractual requirements that an organization, its trading partners, contractors, and service providers have to satisfy.
- The particular set of principles, objectives, and requirements for information processing that an organization has developed to support its operations.

15.5.3 Assessing Security Risks

BS 7799 suggests that security requirements be identified by a methodical assessment of security risks. Expenditure on controls should be balanced against the business harm likely to result from security failures. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems, and it is important to review security risks and implemented controls periodically.

15.5.4 Selecting Controls

Once security requirements have been identified, controls from BS 7799 should be selected and implemented to ensure risks are reduced to an acceptable level. Controls should be selected based on the cost of implementation in relation to the risks being reduced and the potential losses if a security breach occurs. Nonmonetary factors, such as loss of reputation, should also be taken into account. For more information on BS 7799, see http://www.bs7799-iso17799.com/.

15.5.5 Topics Addressed in BS 7799

1. Scope.
2. Terms and definitions.
3. Security policy:
   3.1 Information security policy document.
   3.2 Review and evaluation.
4. Security organization:
   4.1 Information security infrastructure.
   4.2 Security of third-party access.
   4.3 Outsourcing.
5. Asset classification and control:
   5.1 Accountability for assets.
   5.2 Information classification.
6. Personnel security:
   6.1 Security in job definition and resourcing.
   6.2 User training.
   6.3 Responding to security incidents and malfunctions.
7. Physical and environmental security:
   7.1 Secure areas.
   7.2 Equipment security.
   7.3 General control.
8. Communications and operations management:
   8.1 Operational procedures and responsibilities.
   8.2 System planning and acceptance.
   8.3 Protection against malicious software.
   8.4 Housekeeping.
   8.5 Network management.
   8.6 Media handling and security.
   8.7 Exchanges of information and software.
9. Access control:
   9.1 Business requirement for access control.
   9.2 User access management.
   9.3 User responsibilities.
   9.4 Network access control.
   9.5 Operating system access control.
   9.6 Application access control.
   9.7 Monitoring system access and use.
   9.8 Mobile computing and teleworking.
10. Systems development and maintenance:
    10.1 Security requirements of systems.
    10.2 Security in application systems.
    10.3 Cryptographic controls.
    10.4 Security of system file.
    10.5 Security in development and support processes.
11. Business continuity management:
    11.1 Business continuity management process.
12. Compliance:
    12.1 Compliance with legal requirements.
    12.2 Reviews of security policy and technical compliance.
    12.3 System audit considerations.

15.6 ISF Standard of Good Practice for Information Security

The Information Security Forum (ISF) *Standard of Good Practice for Information Security* aims at managing the risks associated with every aspect of information systems, irrespective of an organization's market sector, size, or structure. The standard prepared by ISF's global working groups is a publicly available document split into five key areas: security management, critical business applications, computer installations, networks, and systems development. For more information and details, see http://www.isfsecuritystandard.com.

15.7 Generally Accepted Information Security Principles (GAISP)

The Generally Accepted Information Security Principles (GAISP) culls best practice from all other similar frameworks. Developed in 1991 as the Generally Accepted System Security Principles, GAISP provides a comprehensive hierarchy of guidance for securing information and supporting technology, including:

- **Pervasive Principles** – board-level guidance.
- **Broad Functional Principles** – designed for executive-level information management (exposure draft distributed September 1999).

- **Detailed Principles** – guidance for operational information security management (under development).

GAISP is now being developed by the Information Systems Security Association (ISSA) (http://www.issa.org), which can provide details.

15.7.1 Pervasive Principles

The Pervasive Principles address the confidentiality, integrity, and availability of information. They provide general guidance to establish and maintain the security of information and supporting technology.

- **Accountability Principle** – Information security accountability and responsibility must be defined clearly and acknowledged.
  Rationale – Accountability characterizes the ability to audit the actions of all parties and processes that interact with information. Roles and responsibilities should be clearly defined, identified, and authorized at a level commensurate with the sensitivity and criticality of information. The relationship between all parties, processes, and information must be defined clearly, documented, and acknowledged by all parties. All parties must have responsibilities for which they are held accountable.
- **Awareness Principle** – All parties with a need to know — including, but not limited to, information owners and information security practitioners — should have access to available principles, standards, conventions, or mechanisms for securing information and information systems, and should be informed of applicable threats to the security of information.
  Rationale – This principle applies between and within organizations. Awareness of information security principles, standards, conventions, and mechanisms enhances and enables controls and can help to mitigate threats. Awareness of threats and their significance also increases user acceptance of controls. Without awareness of the necessity for particular controls, users can pose a risk to information by ignoring, bypassing, or overcoming existing control mechanisms. The awareness principle applies to unauthorized and authorized parties.

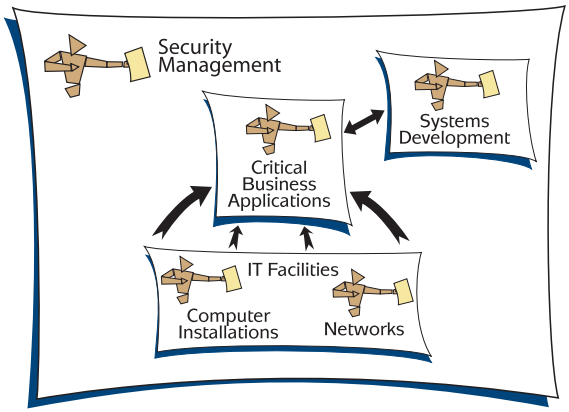


Figure 7 – Security Management

- **Ethics Principle** – Information should be used and information security should be administered in an ethical manner.
  Rationale – Information systems pervade our societies. Rules and expectations are evolving with regard to the appropriate provision and use of information systems and the security of information. Use of information and information systems should match the expectations established by social norms and obligations.
- **Multidisciplinary Principle** – Principles, standards, conventions, and mechanisms for securing information and information systems should address the considerations and viewpoints of all interested parties.
  Rationale – Information security is achieved by the combined efforts of information owners, users, custodians, and information security personnel. Decisions made with due consideration of all relevant viewpoints and technical capabilities can enhance information security and receive better acceptance.
- **Proportionality Principle** – Information security controls should be proportionate to the risks of modification, denial of use, or disclosure of information.
  Rationale – Security controls should be commensurate with the value and vulnerability of information assets. Consider the value, sensitivity, and criticality of the information, as well as the probability, frequency, and severity of direct and indirect harm or loss. This principle recognizes the value of approaches to information security ranging from prevention to acceptance.
- **Integration Principle** – Principles, standards, conventions, and mechanisms for the security of information should be coordinated and integrated with each other and with the organization's policies and procedures to create and maintain security throughout an information system.
  Rationale – Many information security breaches involve the compromise of more than one safeguard. The most effective control measures are components of an integrated system of controls. Information security is most efficient when planned, managed, and coordinated throughout the organization's system of controls and the life of the information.
- **Timeliness Principle** – All accountable parties should act in a timely, coordinated manner to prevent or respond to breaches of, and threats to, the security of information and information systems.
  Rationale – Organizations should be able to coordinate and act swiftly to prevent or mitigate threat

events. This principle recognizes the need for the public and private sectors to jointly establish mechanisms and procedures for rapid and effective threat-event reporting and handling. Access to threat-event history could support effective response to threat events and may help prevent future incidents.

- **Assessment Principle** – The risks to information and information systems should be assessed periodically.
  Rationale – Information and security requirements vary over time. Organizations periodically should assess the information, its value, and the probability, frequency, and severity of direct and indirect harm or loss. Periodic assessment identifies and measures the variances from available and established security measures and controls, such as those articulated in the GAISP, as well as the risk associated with such variances. It also enables accountable parties to make informed information risk management decisions about accepting, mitigating, or transferring the identified risks with due consideration of cost effectiveness.
- **Equity Principle** – Management shall respect the rights and dignity of individuals when setting policy and when selecting, implementing, and enforcing security measures.
  Rationale – Information security measures implemented by an organization should not infringe upon the obligations, rights, and needs of legitimate users, owners, and others affected by the information when exercised within the legitimate parameters of the mission objectives.

15.8 AICPA/CICA Trust Services, Principles and, Criteria

The American Institute of Certified Public Accountants (AICPA) Assurance Services Executive Committee and the CICA Assurance Services Development Board developed the Trust Services Principles and Criteria to address the risks and opportunities of IT. Trust Services Principles and Criteria set out broad statements of principles and identify specific criteria that should be achieved to meet each principle. The principles are broad statements of objectives. Criteria are benchmarks used to measure and present the subject matter, and against which the practitioner can evaluate the subject matter. In the Trust Services Principles and Criteria, the criteria are supported by a list of illustrative controls. The Trust Services Principles and Criteria are organized into four broad areas:

- **Policies** – The organization has defined and documented its policies[5] relevant to the particular principle.
- **Communications** – The organization has communicated its defined policies to authorized users.
- **Procedures** – The organization uses procedures to achieve its objectives in accordance with its defined policies.
- **Monitoring** – The organization monitors the system and takes action to maintain compliance with its defined policies.

Following are summaries of the Trust Services Security, Availability, Processing Integrity, Privacy, Confidentiality, and Certification Authority Principles and Criteria. The Trust Services Principles and Criteria can be used to deliver branded SysTrust and WebTrust engagements, which are assurance services designed for a wide variety of IT-based systems. Upon attainment of an unqualified assurance report, the organization would be entitled to display a SysTrust or WebTrust Seal and accompanying auditor's report. In addition, the framework can be used to provide advisory and consulting services. For a detailed listing of the Trust Services Principles and Criteria, see http://www.aicpa.org/ trustservices.

15.8.1 Security Principle – The system is protected against unauthorized access (both physical and logical).

In e-commerce and other systems, the respective parties must ensure that information provided is available only to those individuals who need access to complete the transaction or services or to follow up on questions or issues that may arise. Information provided through these systems is susceptible to unauthorized access during transmission and while it is stored on the other party's systems. Limiting access to the system components helps prevent potential abuse of the system, theft of resources, misuse of software, and improper access to, or use, alteration, destruction, or disclosure of information. Key elements for protecting system components include permitting authorized access and preventing unauthorized access to those components.

15.8.2 Availability Principle – The system is available for operation and use as committed or agreed.

The availability principle refers to the accessibility to the system, products, or services as advertised or committed by contract or by service-level and other agreements. This principle does not, in itself, set a minimum-acceptable performance level for system availability. Instead, the minimum performance level is established by mutual agreement (contract) between the parties.

Although system availability, functionality, and usability are connected, the availability principle does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to specific tasks or problems). It does

[5] The term *policies* refers to written statements that communicate management's intent, objectives, requirements, responsibilities, and standards for a particular subject. Some policies may be described explicitly as such, being contained in policy manuals or similarly labeled documents. However, some policies may be contained in documents without such explicit labeling, including for example, notices or reports to employees or outside parties.

address system availability, which relates to whether or not the system is accessible for processing, monitoring, and maintenance.

15.8.3 Processing Integrity Principle – System processing is complete, accurate, timely, and authorized.

Processing integrity exists if a system performs its intended function in an unimpaired manner, free from unauthorized or inadvertent manipulation. Completeness generally indicates that all transactions and services are processed or performed without exception, and that transactions and services are not processed more than once. Accuracy includes assurances that key information associated with the submitted transaction will remain accurate throughout the processing of the transaction and that the transaction or services are processed or performed as intended. The timeliness of the provision of services or the delivery of goods is addressed in the context of commitments made for such delivery. Authorization includes assurances that processing is performed in accordance with the required approvals and privileges defined by policies governing system processing.

The risks associated with processing integrity are that the party initiating the transaction will not complete the transaction or provide the service correctly and in accordance with the desired or specified request. Without appropriate processing-integrity controls, the buyer may not receive the goods or services ordered, may receive more than requested, or may receive the wrong goods or services altogether. However, if appropriate processing-integrity controls exist and are operational within the system, the buyer can be reasonably assured of receiving the correct goods and services in the correct quantity and price by the promised date. Processing integrity addresses all of the system components including procedures to initiate, record, process, and report the information, product, or service that is the subject of the engagement. The nature of data input in e-commerce systems typically involves the user entering data directly over Web-enabled input screens or forms, whereas in other systems, the nature of data input can vary significantly. Because of this difference in data-input processes, the nature of controls over the completeness and accuracy of data input in e-commerce systems may be somewhat different than for other systems.

Processing integrity differs from data integrity because it does not imply automatically that the information stored by the system is complete, accurate, current, and authorized. If a system processes information from sources outside of the system's boundaries, an organization can establish only limited controls over the completeness, accuracy, authorization, and timeliness of the information submitted for processing. Errors that may have been introduced into the information and control procedures at external sites typically are beyond the organization's control. When the information source is excluded explicitly from the description of the system that defines the engagement, it is important to detail that exclusion in the system description. In other situations, the data source may be an inherent part of the system being examined, and controls over the completeness, accuracy, authorization, and timeliness of information submitted for processing would be included in the scope of the system as described.

15.8.4 Privacy Principle and Components – Personal information is collected, used, retained, and disclosed in conformity with the commitments in the organization's privacy notice and with the AICPA/CICA Trust Services Privacy Criteria.

The Privacy Principle contains 10 components[6] and related criteria that are essential to the proper protection and management of personal information. These privacy components and criteria are based on fair information practices included in privacy laws and regulations of various jurisdictions around the world and many recognized good privacy practices. The privacy components are:

- **Management** – The organization defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
- **Notice** – The organization provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
- **Choice and consent** – The organization describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
- **Collection** – The organization collects personal information only for the purposes identified in the notice.
- **Use and retention** – The organization limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The organization retains personal information only as long as necessary to fulfill the stated purposes.
- **Access** – The organization provides individuals with access to their personal information for review and update.
- **Disclosure to third parties** – The organization discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
- **Security** – The organization protects personal information against unauthorized access, both physical and logical.
- **Quality** – The organization maintains accurate,

[6] Although some privacy regulations use the term *principle*, the term *component* is used in the AICPA/CICA Trust Services Principles and Criteria Framework to represent that concept, because the term *principle* previously has been defined in the Trust Services literature.

complete, and relevant personal information for the purposes identified in the notice.

- **Monitoring and enforcement** – The organization monitors compliance with its privacy policies and procedures and has processes to address privacy-related complaints and disputes.

15.8.5 Confidentiality Principle – Information designated as "confidential" is protected as committed or agreed.

The confidentiality principle focuses on information designated "confidential." There is no widely recognized definition of *confidential information*, unlike personally identifiable information, which many countries currently are defining through regulation. In the course of communicating and transacting business, partners often exchange information they require to be maintained on a confidential basis. In most instances, the respective parties wish to ensure that the information they provide is available only to those individuals who need access to complete the transaction or resolve any questions that arise. To enhance business partner confidence, it is important to inform the partner about the organization's confidentiality practices, including those for providing authorized access to, use of, and sharing of information designated as confidential.

Information that may be subject to confidentiality includes:

- Transaction details.
- Engineering drawings.
- Business plans.
- Banking information about businesses.
- Inventory availability.
- Bid or ask prices.
- Price lists.
- Legal documents.
- Client and customer lists.
- Revenue by client and industry.

Unlike personal information, there are no defined rights for accessing confidential information to ensure its accuracy and completeness. Interpretations of what is considered confidential information can vary significantly from business to business and are driven by contractual arrangements in most cases. As a result, those engaged in business relationships need to understand what information will be maintained on a confidential basis and what, if any, rights of access or other expectations an organization might have for updating that information to ensure its accuracy and completeness.

Information that is provided to another party is susceptible to unauthorized access during transmission and while it is stored on the other party's computer systems. For example, an unauthorized party may intercept business partner profile information and transaction and settlement instructions while they are being transmitted. Controls such as encryption can be used to protect the confidentiality of this information during transmission, while firewalls and rigorous access controls can help protect the information while it is stored on computer systems.

15.8.6 Certification Authority (CA) Principle

The certification authority discloses its key and certificate life cycle-management business and information privacy practices and provides its services in accordance with these practices. This includes the concepts of CA business-practice disclosures, service integrity, and environmental controls.

15.9 IIA Systems Assurance and Control (SAC)

The IIA provides the SAC model The SAC model sets the stage for effective technology risk management by giving companies a framework to guide an evaluation of the e-business control environment. SAC recognizes the importance of governance — both within an organization and between business partners — to ensure effective security, auditability, and control of information. SAC provides current information to understand, monitor, assess, and mitigate technology risks. SAC examines risks in all business system components, including customers, competitors, regulators, and partners. Full details of the model can be found at http://www.theiia.org/eSAC/index.cfm, with a detailed discussion of the model at www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=411.

15.10 Corporate Governance

15.10.1 OECD Principles of Corporate Governance

The OECD Principles of Corporate Governance, amended in April 2004, set out a framework for good practice that has been agreed to by all 30 OECD member countries and has become a generally accepted standard (http://www.oecd.org/corporate). Originally issued in 1999, the principles are designed to assist governments and regulatory bodies in drawing up and enforcing effective rules, regulations, and codes of corporate governance. In parallel, they provide guidance for stock exchanges, investors, companies, and others that have a role in the process of developing good corporate governance. Although the OECD principles do not provide specific guidance on IT controls, other OECD units provide further guidance and research on information security and privacy.

15.10.2 EU Commission

The European Commission's Action Plan on Company Law and Corporate Governance was released in May 2003 to strengthen corporate governance mechanisms in public interest entities (For details, see http://europa.eu.int/comm/internal_market/company/index_en.htm). The EU's Corporate Governance initiatives do not address IT issues specifically, but activities of the Information Society

directorate (http://europa.eu.int/information_society/index_en.htm) address many specific IT control issues.

15.10.3 United Kingdom's Combined Code and Turnbull Guidance

The Combined Code and Turnbull guidance were the United Kingdom's approach to corporate governance. Like Sarbanes-Oxley, they are not specific on the issue of IT controls, but are focused on the whole internal control framework. More details can be found from IIA-UK and Ireland at http://www.iia.org.uk/knowledgecentre/keyissues/corporategovernance.cfm?Action=1&ARTICLE_ID=1185.

15.10.4 King Report on Corporate Governance for South Africa 2002 (King II)

Similar to the Combined Code and the Turnbull guidance, this code of practice is intended for organizations in South Africa. Copies of the reports can be accessed online at http://www.ecgi.org/codes/country_pages/codes_south_africa.htm.

15.10.5 Other Corporate Governance Requirements

Many other countries have similar corporate governance requirements. A comprehensive list and copies of these can be found at http://www.ecgi.org/codes/all_codes.htm.

15.11 Other Related Issues

15.11.1 IT Infrastructure Library (ITIL)

The IT Infrastructure Library (ITIL) is a generic approach to IT service management, providing a set of best practices, drawn from public and private sectors internationally. Originating in the United Kingdom, it is supported by a qualification scheme, accredited training organizations, and implementation and assessment tools. The best-practice processes promoted in ITIL support and are supported by the British Standards Institution's *Standard for IT Service Management* (BS 15000). While ITIL does not claim specifically to be a framework for IT control, its use needs to be recognized and taken into account when determining which control framework to apply. Further information can be obtained from http://www.itil.co.uk/.

15.11.2 ISO 9000:2000

While ISO 9000 relates specifically to the requirements of quality management, it does contain elements that contribute to IT control in respect to the control and documentation of processes. Although it does not constitute a complete IT control framework, ISO 9000 can provide elements that contribute to the strength of IT controls for implementing strong processes. More information on the standard can be found at http://www.iso.ch/iso/en/iso9000-14000/iso9000/iso9000index.html.

15.11.3 National Quality Institute (NQI) Canadian Framework for Business Excellence

The Canadian Quality Criteria/Framework for Business Excellence, developed by the National Quality Institute (NQI), is a framework for improvement. Based on the Quality Principles, the original private-sector criteria has been adapted for the public sector, as well. In addition, they form the evaluation basis for the Manitoba Quality Awards and Canada Awards for Excellence programs and are used by Canadian organizations of all sizes and in all sectors. More information can be found at http://www.qnet.mb.ca/quality_cdncriteria.htm.

15.11.4 Carnegie Mellon University Software Engineering Institute (CMU/SEI) OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a self-directed, risk-based, strategic assessment and planning technique for organizations that want to understand their information security needs. A small team of people from an organization's operational, or business, units and the IT department work together to address the security needs of the enterprise. This team draws on the knowledge of many employees to define the current state of security, identify risks to critical assets, and set a security strategy. OCTAVE focuses on organizational risk and strategic, practice-related issues, balancing operational risk, security practices, and technology. Separate methods are available for large and small organizations. For more information, see http://www.cert.org/octave/.

The COSO *Internal Control – Integrated Framework* is recognized as a formal model for the purpose of Sarbanes-Oxley attestation by the SEC and provides a hierarchical categorization of controls. In addition, the audit standard from the PCAOB states:

> "Because of the frequency with which management of public companies is expected to use COSO as the framework for the assessment, the directions in the standard are based on the COSO framework. Other suitable frameworks have been published in other countries and likely will be published in the future. Although different frameworks may not contain exactly the same elements as COSO, they should have elements that encompass all of COSO's general themes."

The COSO model was refined and enhanced during 2004 through development of the COSO *Enterprise Risk Management – Integrated Framework* (http://www.coso.org). This appendix describes the earlier framework, which is the version referenced for regulatory compliance. Nonetheless, the CAE should investigate the *Enterprise Risk Management – Integrated Framework*.

16.1 COSO Definition of *Internal Control*

COSO defines *internal control* (http://www.coso.org/key.htm) as "a process, effected by an organization's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

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

These distinct, but overlapping, categories address different needs such that each require a directed focus. The first category addresses an entity's basic business objectives, including performance and profitability goals and safeguarding of resources, which are impacted greatly by the use of IT.

The second category relates to the preparation of reliable published financial statements, including interim and condensed financial statements, as well as earnings releases and other selected publicly reported financial data derived from such statements. IT systems frequently produce such reports, and the controls over these systems play a major part in the level of internal control.

The third category deals with complying with those laws and regulations to which the entity is subject.

Internal control systems operate at different levels of effectiveness. Internal control can be judged effective in each of the three categories if the board of directors and management have reasonable assurance that:

- They understand the extent to which the entity's operations objectives are being achieved.
- Published financial statements are being prepared reliably.
- There is compliance with applicable laws and regulations.

Although internal control is a process, its effectiveness is a state or condition of the process at one or more points in time.

16.2 COSO *Internal Control — Integrated Framework*

Internal control consists of five interrelated components that are derived from the way management runs a business and are integrated with the management process. Although the components apply to all entities, small and mid-size organizations may implement them differently than large enterprises. A small organization's controls may be less formal and less structured, yet it can still have effective internal control. The components are:

16.2.1 Control Environment

The control environment sets the tone for an organization, influencing the control consciousness of its people, establishing the foundation for all other components of internal control, and providing discipline and structure. Control environment factors include the integrity, ethical values, and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility and organizes and develops its people; and the attention and direction provided by the board of directors.

16.2.2 Risk Assessment

Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is the establishment of objectives that are linked at different levels and are consistent internally . Risk assessment identifies and analyzes the relevant risks to achieving these objectives and forms a basis for determining how the risks should be managed. Because economic, industry, regulatory, and operating conditions will continue to change, organizations need mechanisms to identify and deal with the special risks associated with change.

16.2.3 Control Activities

Control activities are the policies and procedures that help ensure management directives are carried out and that necessary actions are taken to address risks to achieving these objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.

16.2.4 Information and Communication

Pertinent information must be identified, captured, and communicated in a form and time frame that enables people to perform their responsibilities. Information systems produce reports containing operational, financial, and compliance-related information that make it possible to run and

control the business. They deal not only with internally generated data, but also with information about external events, activities, and conditions necessary for informed business decision-making and external reporting. Effective communication must also occur in a broader sense, flowing down, across, and up the organization. All personnel must receive a clear message from top management that control responsibilities have to be taken seriously. They need to understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators, and shareholders.

16.2.5 Monitoring

Internal control systems need to be monitored to assess the quality of their performance over time. This is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two. Ongoing monitoring occurs in the course of operations and includes regular management and supervisory activities and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board.

There is synergy and linkage among the components, forming an integrated system that reacts dynamically to changing conditions. The internal control system is intertwined with the entity's operating activities and exists for fundamental business reasons. Internal control is most effective when controls are built into the entity's infrastructure and are a part of the essence of the enterprise. Built-in controls support quality and empowerment initiatives, avoid unnecessary costs, and enable quick response to changing conditions.

There is a direct relationship between the three COSO categories (effectiveness, reliability, compliance) of objectives — which are what an entity strives to achieve — and the components needed to achieve the objectives. All components are relevant to each objectives category. When looking at any one category — the effectiveness and efficiency of operations, for instance — all five components must be present and functioning effectively to conclude that internal control over operations is effective.

The internal control definition — with its underlying fundamental concepts of a process, affected by people, providing reasonable assurance — together with the categorization of objectives, and the components and criteria for effectiveness, the associated discussions, constitute this internal control framework.

Organizations must satisfy the quality, fiduciary, and security requirements for their information, as for all assets. Management must also optimize the use of available resources, including data, application systems, technology, facilities, and people. To discharge these responsibilities, as well as to achieve its objectives, management must establish an adequate system of internal control. Thus, an internal control system or framework must be in place to support the business processes, and it must be clear how each individual control activity satisfies the information requirements and impacts the resources. Impact on IT resources is highlighted in the CobiT framework together with the business requirements for effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability of information that need to be satisfied. Control, which includes policies, organizational structures, practices, and procedures, is management's responsibility. Management, through its corporate and IT governance, must ensure that due diligence is exercised by all individuals involved in the management, use, design, development, maintenance, or operation of information systems.

Business orientation is the main theme of CobiT. It is designed not only to be employed by users and auditors, but also, and more importantly, as a comprehensive checklist for business process owners. Increasingly, business practice involves the full empowerment of business process owners so they have total responsibility for all aspects of the business process. In particular, this includes providing adequate controls. The CobiT framework provides a tool for the business process owner that facilitates the discharge of this responsibility. The framework starts from a simple and pragmatic premise: In order to provide the information that the organization needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes.

CobiT continues with a set of 34 high-level control objectives, one for each of the IT processes, grouped into four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.

Plan and Organize – This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of business objectives.

1. Define a strategic IT plan.
2. Define the information architecture.
3. Determine the technological direction.
4. Define the IT organization and relationships.
5. Manage the IT investment.
6. Communicate management aims and direction.
7. Manage human resources.
8. Ensure compliance with external requirements.
9. Assess risks.
10. Manage projects.
11. Manage quality.

Acquire and Implement – To realize the IT strategy, IT solutions need to be identified, developed, or acquired, as well as implemented and integrated into the business process. In addition, changes in, and maintenance of, existing systems are covered by this domain to make sure that the life cycle is continued for these systems.

12. Identify automated solutions.
13. Acquire and maintain application software.
14. Acquire and maintain technology architecture.
15. Develop and maintain IT procedures.
16. Install and accredit systems.
17. Manage changes.

Deliver and Support – This domain is concerned with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training. This domain includes the actual processing of data by application systems.

18. Define and manage service levels.
19. Manage third-party services.
20. Manage performance and capacity.
21. Ensure continuous service.
22. Ensure systems security.
23. Identify and allocate costs.
24. Educate and train users.
25. Assist and advise IT customers.
26. Manage the configuration.
27. Manage problems and incidents.
28. Manage data.
29. Manage facilities.
30. Manage operations.

Monitor and Evaluate – All IT processes need to be assessed regularly over time for their quality and compliance with control requirements. This domain thus addresses management's oversight of the organization's control process and independent assurance provided by internal and external auditing or obtained from alternative sources.

31. Monitor the processes.
32. Assess internal control adequacy.
33. Obtain independent assurance.
34. Provide for independent audit.

This structure covers all aspects of information and the technology that supports it. By addressing these 34 high-level control objectives, the business process owner can ensure that an adequate control system is provided for the IT environment.

CobiT is comprised of:

- An executive summary, which provides an overview of CobiT's issues and foundational premise*.
- CobiT framework, which describes in detail the high-level IT control objectives and identifies the business requirements for information and IT resources primarily impacted by each control objective.
- Control objectives, statements of the desired results or purposes to be achieved by implementing the specific, detailed control objectives*.
- Audit guidelines, suggested audit steps corresponding to each of the IT control objectives.

- An implementation tool set, which provides lessons learned from those organizations that successfully applied CobiT in their work environments and several tools to help management assess their control environment related to information and IT resources.
- Management guidelines, which are composed of maturity models, to help determine the stages and expectation levels of control; critical success factors, to identify the most important actions for achieving control over the IT processes; key goal indicators, to define target levels of performance; and key performance indicators, to measure whether an IT control process is meeting its objective*.

* Designated by the IT Governance Institute (ITGI) and ISACA as an open standard, this portion of CobiT may be downloaded from http://www.itgi.org and http://www.isaca.org.

CobiT, now in its third edition and available in hard copy or interactive online format (CobiT Online), increasingly is accepted internationally as good practice for control over information, IT, and related risks. Its guidance enables an enterprise to implement effective governance over the IT that is pervasive and intrinsic throughout the enterprise.

The following metrics descriptions are taken from the Corporate Information Security Working Group (CISWG) draft report of the Best Practices and Metrics teams, November 17, 2004. During Phase I of the CISWG, convened in November 2003 by Rep. Adam Putnam (R-FL), the Best Practices team surveyed available information security guidance. It concluded in its March 2004 report[7] that much of this guidance is expressed at a relatively high level of abstraction and therefore is not useful immediately as actionable guidance without significant and often costly elaboration. A one-page listing of Information Security Program Elements regarded as essential content for comprehensive enterprise management of information security was created, upon which it was hoped future actionable guidance could be built for use by a wide variety of organizations.

The Best Practices and Metrics teams of CISWG Phase II, convened in June 2004, were charged with expanding on the work of Phase I by refining the Information Security Program Elements and developing metrics to support each of the elements. The goal was to develop a resource that would help board members, managers, and technical staff establish a comprehensive structure of principles, policies, processes, controls, and performance metrics to support the people, process, and technology aspects of information security.

These generic metrics can be used as the basis for determining regular reporting requirements for the audit committee, although they are not meant to be a "one-size-fits-all" solution. The full set of draft metrics, along with explanatory notes and descriptions, can be found under the "Technology" section of http://www.theiia.org.

The Information Security Program Elements and Supporting Metrics are intended to enable boards, management, and technical staff to monitor the status and progress of their organization's information security program over time. Each organization should thoughtfully consider which program elements and metrics might be helpful in its own circumstances. It should then set its own implementation priorities and establish an appropriate policy, process, and control structure. Larger and more complex organizations will create policies, processes, and controls in each program element that inevitably will be more extensive than those a smaller organization might choose to implement.

18.1 Metrics for Boards of Directors/Trustees

Establishing a competent information security program requires board members to devote attention to certain program elements. Board members can use the following metrics as part of their information security responsibilities. Board members generally should find the best target value for each metric — higher or lower — to be self-evident.

- Oversee risk management and compliance programs pertaining to information security.
  - Percentage of key information assets for which a comprehensive strategy has been implemented to mitigate information security risks as necessary and to maintain these risks within acceptable thresholds.
  - Percentage of key organizational functions for which a comprehensive strategy has been implemented to mitigate information security risks as necessary and to maintain these risks within acceptable thresholds.
  - Percentage of key external requirements for which the organization has been deemed to be in compliance by an objective audit or other means.
- Approve and adopt broad information security program principles and approve assignment of key managers responsible for information security.
  - Percentage of information security program principles for which approved policies and controls have been implemented by management.
  - Percentage of key information security management roles for which responsibilities, accountabilities, and authority are assigned and required skills identified.
- Strive to protect the interests of all stakeholders who depend on information security.
  - Percentage of board meetings and/or designated committee meetings for which information security is on the agenda.
  - Percentage of security incidents that caused damage, compromise, or loss beyond established thresholds to the organization's assets, functions, or stakeholders.
  - Estimated damage or loss in dollars resulting from all security incidents in each of the past four reporting periods.
- Review information security policies regarding strategic partners and other third parties.
  - Percentage of strategic partner and other third-party relationships for which information security requirements have been implemented in agreements.
- Strive to ensure business continuity.
  - Percentage of organizational units with an established business-continuity plan.
- Review provisions for internal and external audits of the information security program.
  - Percentage of required internal and external audits completed and reviewed by the board.
  - Percentage of audit findings that have not been resolved.
- Collaborate with management to specify the information security metrics to be reported to the board.

18.2 Metrics for Management

The following program elements and metrics are intended to help management implement the information security goals

7 http://reform.house.gov/TIPRC/

and policies established by the board as part of an effective information security program:

- Establish information security management policies and controls and monitor compliance.
  - Percentage of information security program elements for which approved policies and controls are operational.
  - Percentage of staff assigned responsibilities for information security policies and controls who have acknowledged accountability for their responsibilities in connection with those policies and controls.
  - Percentage of information security policy compliance reviews that noted violations.
  - Percentage of business-unit heads and senior managers who have implemented operational procedures to ensure compliance with approved information security policies and controls.
- Assign information security roles, responsibilities, and required skills, and enforce role-based, information-access privileges.
  - Percentage of new employees hired this reporting period who satisfactorily completed security-awareness training before being granted network access.
  - Percentage of employees who have completed periodic security-awareness refresher training as required by policy.
  - Percentage of position descriptions that define the information security roles, responsibilities, skills, and certifications for:
    + Security managers and administrators.
    + IT personnel.
    + General staff system users.
  - Percentage of job performance reviews that evaluate information security responsibilities and policy compliance.
  - Percentage of user roles, systems, and applications that comply with the separation-of-duties principle.
- Number of individuals with access to security software who are not trained and authorized security administrators.
- Number of individuals who are able to assign security privileges for systems and applications who are not trained and authorized security administrators.
  - Percentage of users whose access privileges have been reviewed this reporting period, including:
    + Employees with high-level system and application privileges.
    + All other employees.
    + Contractors.
    + Vendors.
    + Terminated employees and contractors.
  - Percentage of users who have undergone background checks.
- Assess information risks, establish risk thresholds, and actively manage risk mitigation.
  - Percentage of critical information assets and information-dependent functions for which some form of risk assessment has been performed and documented as required by policy.
  - Percentage of critical assets and functions for which the cost of compromise — loss, damage, disclosure, or disruption of access — has been quantified.
  - Percentage of identified risks that have a defined risk mitigation plan against which status is reported in accordance with policy.
- Ensure implementation of information security requirements for strategic partners and other third parties.
  - Percentage of known information security risks that are related to third-party relationships.
  - Percentage of critical information assets or functions to which third-party personnel have been given access.
  - Percentage of third-party personnel with current information access privileges who a designated authority has deemed to have continued need for access in accordance with policy.
  - Percentage of systems with critical information assets or functions that are connected to third-party systems electronically.
  - Percentage of security incidents that involve third-party personnel.
  - Percentage of third-party agreements that include or demonstrate external verification of policies and procedures.
  - Percentage of third-party relationships that have been reviewed for compliance with information security requirements.
  - Percentage of out-of-compliance review findings that have been corrected since the last review.
- Identify and classify information assets.
  - Percentage of information assets that have been reviewed and classified by the designated owner in accordance with the classification scheme established by policy.
  - Percentage of information assets with defined access privileges that have been assigned based on role and in accordance with policy.
  - Date when the asset inventory was last updated.
- Implement and test business-continuity plans.
  - Percentage of organizational units with a documented business-continuity plan for which specific responsibilities have been assigned.
  - Percentage of business-continuity plans that have been reviewed, exercised and tested, and updated in accordance with policy.
- Approve information systems architecture during acquisition, development, operations, and maintenance.
  - Percentage of information security risks related to

systems architecture identified in the most recent risk assessment that have been mitigated adequately.
  - Percentage of system architecture changes — additions, modifications, or deletions — that were reviewed for security impacts, approved by the appropriate authority, and documented via change-request forms.
  - Percentage of critical information assets or functions residing on systems that are out of compliance with the approved systems architecture.
- Protect the physical environment.
  - Percentage of critical organizational information assets and functions that have been reviewed from the perspective of physical risks such as controlling physical access and physical protection of backup media.
  - Percentage of critical organizational information assets and functions exposed to physical risks for which risk mitigation actions have been implemented.
  - Percentage of critical assets that have been reviewed from the perspective of environmental risks such as temperature, fire, and flooding.
  - Percentage of servers in locations with controlled physical access.
  - Percentage of information security requirements of applicable laws and regulations that are included in the internal and external audit program and schedule.
  - Percentage of information security audits conducted in compliance with the approved internal and external audit program and schedule.
  - Percentage of management actions in response to audit findings and recommendations that were implemented as agreed upon regarding timeliness and completeness.
- Collaborate with security personnel to specify the information security metrics to be reported to management.

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

Action	Questions
1. Identify the IT control environment of the organization, including: a. Values. b. Philosophy. c. Management style. d. IT awareness. e. Organisation. f. Policies. g. Standards.	1. Do corporate policies and standards that describe the need for IT controls exist?
2. Identify relevant legislation and regulation impacting IT control such as: a. Governance. b. Reporting. c. Data protection. d. Compliance.	2. What legislation exists that impacts on the need for IT controls? 3. Has management taken steps to ensure compliance with this legislation?
3. Identify the roles and responsibilities for IT control in relation to: a. Board of directors. i. Audit committee. ii. Risk committee. iii. Governance committee. iv. Finance committee. b. Management. i. CEO ii. CFO and controller iii. CIO iv. CSO v. CISO vi. CLC vii. CRO c. Audit. i. Internal Audit. ii. External Audit.	4. Have all the relevant responsibilities for IT controls been allocated to individual roles? 5. Is the allocation of responsibilities compatible with the need to apply division of duties? 6. Are IT responsibilities documented? 7. Are IT control responsibilities communicated to the whole organization? 8. Do individual role holders clearly understand their responsibilities in relation to IT controls? 9. What evidence is there of individual role holders exercising their responsibilities? 10. Does internal auditing employ sufficient IT audit specialists to address the IT control issues?

Action	Questions
4. Identify the risk assessment process. Does it cover: a. Risk appetite? b. Risk tolerances? c. Risk analysis? d. Matching risks to IT controls?	11. How is the risk appetite and tolerance of the organization determined? 12. Is the risk appetite and tolerance of the organization authorized at board level? 13. Is the risk appetite and tolerance clearly understood by all those with a responsibility for IT control? 14. Is a formal risk analysis process used by the organization? 15. Is the process understood by all those with responsibility for IT control? 16. Is the process used consistently throughout the organization?
5. Identify all monitoring processes, including: a. Regulatory. b. Normal in-house c. Other than internal auditing.	17. What processes exist to monitor compliance with all relevant legislation plus internal policies and standards? 18. Are there monitoring processes carried out by management outside of internal audit?
6. Identify information and communication mechanisms: a. Control information. b. Control failures.	19. What metrics are provided to the board of directors, its committees and management in relation to IT security? 20. What additional reports are provided to the board of directors and to management on a regular basis? 21. Is management always provided with reports when there are IT control failures? 22. Do the board of directors and its committees receive similar reports of IT control failures?

The following list of information security reference material is taken from a list compiled by the CISWG of the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census; and the Government Reform Committee of the U.S. House of Representatives. The full list can be found at http://www.reform.house.gov/TIPRC/ or under the "Technology" section of http://www.theiia.org.

The documents are classified into three sections relating to governance, management, and technical issues.

20.1 Governance

Board Briefing on IT Governance, ITGI http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&CONTENTID=6658&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

Information Security Governance: Guidance for Boards of Directors and Executive Management, ITGI, http://www.itgi.org.

Information Security Management and Assurance, Three report series from The IIA National Association of Corporate Directors (NACD), U.S. Critical Infrastructure Assurance Office, et al., http://www.theiia.org/esac/index.cfm?fuseaction=or&page=rciap.

Information Security Oversight: Essential Board Practices, NACD, http://www.nacdonline.org/publications/pubDetails.asp?pubID=138&user=6158BBEB9D7C4EE0B9E4B98B601E3716.

IT Governance Implementation Guide, ISACA, http://www.isaca.org/Template.cfm?Section=Browse_By_Topic&Template=/Ecommerce/ProductDisplay.cfm&ProductID=503.

Turnbull Report - Internal Control - Guidance for Directors on the Combined Code, Institute of Chartered Accountants in England & Wales, http://www.icaew.co.uk/index.cfm?AUB=TB2I_6242,MNXI_47896.

20.2 Management

BS 7799 – Parts 1 & 2, Code of Practice for Information Security Management, British Standards Institution, http://www.bsi.org.uk.

Common Sense Guide for Senior Managers, Internet Security Alliance, www.isalliance.org.

Corporate Information Security Evaluation for CEOs, TechNet, http://www.technet.org/cybersecurity.

Generally Accepted Information Security Principles (GAISP), Information Systems Security Association. Currently available: ***Generally Accepted Systems Security Principles (GASSP)*** consisting of Pervasive Principles and Broad Functional Principles. Detailed Principles are under development. http://www.issa.org/gaisp/gaisp.html.

Generally Accepted Principles and Practices (GAPP), NIST SP 800-18. "Guide for Developing Security Plans for Information Technology Systems," December 1998 (Marianne Swanson & Barbara Guttman), eight generally accepted principles (see OECD) and "Common IT Security Practices." http://csrc.nist.gov/publications/nistpubs/index.html.

ICC Handbook on Information Security Policy for Small to Medium Enterprises, International Chamber of Commerce (ICC), http://www.iccwbo.org/home/e_business/word_documents/SECURITY-final.pdf.

IFAC International Guidelines on Information Technology Management – Managing Information Technology Planning for Business Impact, International Federation of Accountants, http://www.ifac.org.

Information Security for Executives, Business and Industry Advisory Committee to the OECD and ICC, http://www.iccwbo.org/home/e_business/word_documents/SECURITY-final.pdf.

ISO 17799 – Information Technology – Code of Practice for Information Security Management, International Organization for Standardization (ISO), http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35&ICS2=40&ICS3.

OECD Guidelines for the Security of Information Systems and Networks, nine pervasive principles for information security upon which several other guides are based, OECD, http://www.oecd.org/document/42/0,2340,en_2649_33703_15582250_1_1_1_1,00.html.

Standard of Good Practice for Information Security, Information Security Forum, http://www.isfsecuritystandard.com/index_ie.htm.

Trust Services Criteria (including SysTrust and WebTrust), American Institute of Certified Public Accountants, http://www.aicpa.org/trustservices.

20.3 Technical Issues

Consensus Benchmarks, Center for Internet Security, http://www.cisecurity.org.

DISA Security Technical Implementation Guides, http://www.csrc.nist.gov/pcig/cig.html.

ISO 15408 Common Criteria, http://www.csrc.nist.gov/cc/ccv20/ccv2list.htm.

ISO TR 13335 – Guidelines for the Management of Information Security, Parts 1-5, http://www.iso.org/iso/en/StandardsQueryFormHandler.StandardsQueryFormHandler.

IT Baseline Protection Manual (P BSI 7152 E 1), Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.bund.de/gshb/english/menue.htm.

ITCG: Information Technology: Control Guidelines, Canadian Institute of Chartered Accountants (CICA), http://www.cica.ca.

NIST Configuration Guides, National Institute of Standards and Technology (NIST), http://www.csrc.nist.gov/pcig/cig.html.

NIST 800-12 The Computer Security Handbook, NIST, http://www.csrc.nist.gov/publications/nistpubs/index.html.

NIST 800-30 Risk Management Guide for Information Technology Systems, NIST, http://www.csrc.nist.gov/publications/nistpubs/index.html.

NSA Configuration Guides, http://www.nsa.gov/snac.

SANS Step-by Step Guides, SANS Institute, http://www.store.sans.org.

20.4 Auditing IT

Control Objectives for Information and Related Technologies (CobiT), ISACA, http://www.isaca.org.

Federal Information Systems Controls Audit Manual (FISCAM), U.S. Government Accountability Office, http://www.gao.gov.

Information Technology: Control Guidelines (ITCG), CICA, http://www.cica.ca.

Systems Assurance and Control (SAC), IIA Research Foundation, http://www.theiia.org/eSAC.

Systems Auditability and Control (SAC), IIA Research Foundation, http://www.theiia.org/eSAC.

A listing of technical terms used in the guide with a simple, plain English definition.

Application Control – A control related to the specific functioning of an application system that supports a specific business process. Common applications include accounts payable, inventory management, and general ledger. Integrated applications combine the functions of many business processes into integrated systems sharing common databases.

Assurance – The act of assuring; a declaration tending to inspire full confidence; that which is designed to give confidence.

CAE – Chief audit executive.

CEO – Chief executive officer.

CFO – Chief financial officer (and controller).

CIO – Chief information officer.

CISO – Chief information security officer.

CLC – Chief legal council.

COSO – The Committee of Sponsoring Organizations of the Treadway Commission (the Commission on Fraudulent Financial Reporting). See http://www.coso.org/key.htm.

CRM – Customer resource management.

CSO – Chief Security Officer.

Cyber attack – A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.

Effective – Getting a job done with or without regard for efficiency. If the law requires you to do something, it probably does not require you to do it efficiently, as evidenced by Sarbanes-Oxley compliance and the frequent complaint that companies are spending huge sums with no apparent value added to the organization or stakeholders.

Efficient – To be efficient, a process or activity must also be effective. Information Technology Process Institute studies show that best-of-breed organizations enjoy considerable efficiencies by maintaining an effective set of control and monitoring practices and resolving the source of the problem rather than only responding to the symptoms.

Framework – A structure for organizing something (e.g., governance issues, controls) to highlight needs at the various levels of an organization, as well as for its activities and processes. A control framework is an outline that identifies the need for controls, but does not depict how they are applied. Each organization and organizational unit provides a level of detail related to its own control objectives and control practices.

General control – A control that applies generally to the IT environment or overall mix of systems, networks, data, people, and processes (also known as IT infrastructure).

GLBA – U.S. Gramm-Leach-Bliley Act.

Governance – The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

GTAG – Global Technology Audit Guide.

HIPAA – U.S. Health Information Portability and Accountability Act.

Information asset – Information assets are based in the value of information to the worth and continued existence of the organization. A distinction is made between *information assets* and information resources because *information resources* are generally considered to include the related human resources, and human resources are not considered to be owned by the organization.

Information resource – Includes all elements of the organization involved in information processing (e.g., acquisition, processing, communication, and storage), including the related hardware, software, processes, and personnel.

Information security – The concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use.

Information technology (IT) – All the computer hardware and software used to process information and provide communications, the processes for administering and maintaining the technology, and the human resources associated with the use of technology.

ISO 17799 – *Code of Practice for Information Security Management*. See http://www.iso.org.

IT controls – Those controls that provide reasonable assurance of the secure, reliable, and resilient performance of hardware, software, processes, and personnel, as well as the reliability of the organization's information.

IT infrastructure – The overall IT environment, including systems, networks, data, people, and processes. Infrastructures can also include the interaction of businesses and industries in mutual support through shared media and services, such as the Internet, energy, financial services, utilities, government, and transportation. To the extent that infrastructures support national and regional economies, defenses, and business continuity, they are known as critical infrastructures.

ITPI – IT Process Institute. See http://www.itpi.org.

Public Company Accounting Oversight Board (PCAOB) – A board of the US Securities and Exchange Commission established by the Sarbanes-Oxley Act of 2002 as an oversight body for public financial reporting and auditing.

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

Risk management – The ongoing identification, measurement, and mitigation of risk through the demonstrably cost-efficient implementation and administration of control over the known and knowable risks of threat events that can affect the confidentiality, integrity, or availability of an organization's information assets adversely.

Risk Tolerance – Defined by COSO as "the acceptable level of variation relative to the achievement of objectives. In setting specific risk tolerances, management considers the relative importance of the related objectives and aligns risk tolerances with its risk appetite."

This IT controls guide is the first in a series of GTAGs which will give CAEs and internal auditors a source of information for educating and informing themselves and others within the organization who have responsibilities related to IT control.

The GTAGs will provide guidance on a variety of IT topics. Each guide will describe the underlying technology facts and issues sufficiently to explain business opportunities, risks and related controls, and their impacts on the overall system of internal controls. Subjects to be addressed in the GTAG series will be determined by current and emerging technology areas and their potential ramifications for internal controls and assurance. Planned topics for guides include intrusion protection, security management, change management, wireless security, identity management, and authentication.

22.1 Parties to the GTAG Program

Each GTAG guide is developed through interaction with technical audit and security experts, audit executives, technology vendors, and the associations and individuals that represent board members, chief executives, financial executives, information technology professionals, and security executives. Involvement from The IIA's international affiliates and partners support the global perspective of the guides. Other professionals representing specialized views such as legal, insurance, regulatory, and standards will be included, as appropriate, within individual GTAG projects.

The IIA is joined in this GTAG project by a specially selected team of professional associations, academic institutions, and practitioners in both auditing and technology. IIA is grateful for the support provided by this team, as the guide would not have been possible without them. For The IIA to provide meaningful guidance to auditors about how to relate to audit customers, it is essential to gain agreement with the key representatives of those customers. To speak to a global audience, the guide needs consensus from a broad group representing many of the countries where internal auditors operate. So we thank both the individuals and the organizations who contributed so much to this guide.

23.1 IT Controls Advisory Council

The Advisory Council is made up of individuals who contributed to the development of this guide from the outset of planning the GTAG project, through design and development of the IT Controls Guide outline and various drafts, to the completion of the final product. These individuals went beyond the role of a volunteer support team to truly act in a leadership role.

Julia H Allen, CMU/SEI Carnegie-Mellon University/Software Engineering Institute

Michael R. Dickson, Business Technology Group, LLC

Clint Kreitner, President/CEO, CIS, The Center for Internet Security

Alex Lajoux, NACD, National Association of Corporate Directors

Will Ozier, Vice Chair, the ISSA GAIS Committee CEO & President OPA Inc., The Integrated Risk Management Group, USA

Mark Salamasick, CIA, University of Texas at Dallas

Karyn Waller, AICPA, American Institute of Certified Public Accountants

23.2 Partner Organizations

AICPA – Michael R. Dickson, Karyn Waller, American Institute of Certified Public Accountants

CIS – Clint Kreitner, Center for Internet Security

CMU/SEI – Julia Allen, Bob Rosenstein, Carnegie-Mellon University/Software Engineering Institute

ISSA – Dave Cullinane, President; Bob Daniels, Exec Vice President, Information Systems Security Association

NACD – Peter Gleason, Alex Lajoux, National Association of Corporate Directors

SANS Institute – Alan Paller, Director of Research, Stephen Northcutt, COO

23.3 Project Review Team

Peter Allor, ISS, Internet Security Systems

Jack Antonelli, ADP

Ken D. Askelson, CIA, JC Penney Co. Inc.

Becky Bace, Infidel Inc.

Kevin Behr, IPSI, Institute for Integrated Publication and Information Systems

Jeff Benson, BearingPoint

Robert S. Block, Chairman, 3D Business Tools, USA

Sylvia Boyd, The IIA

Alexandra Branisteanu, Information Security Officer, Scripps Health, San Diego, USA

Larry Brown, Options Clearing Corp.

Stephanie Bryant, University of South Florida

Phil Campbell, Specialized IT, LLC, USA

John Carlson, BITS, Banking Industry Technology Secretariat

Chris Compton, Intrusion Labs

Guy Copeland, CSC, Computer Sciences Corp.

Rich Crawford, Vice President/Senior Security Advisor, Janus Risk Management, USA

Bob Daniels, EDS

Bob Dix, U.S. House of Representatives

Jerry E. Durant, CIA, President, Certifiable Technologies Ltd., Orlando, Fla., USA

Emily Frye, Critical Infrastructure Protections Program, George Mason University, School of Law, USA Protections Program

Greg Garcia, ITAA, Information Technology Association of America

Russ Gates, Dupage Consulting LLC

Lou Giles, Chevron Phillips Chemical Co.

Doug Guerrero, EDS

Kai Tamara Hare, Nuserve

Michael S. Hines, CIA, Purdue University

Bob Hirth, Protiviti

Don Holden, CISSP, Concordant Inc., USA

Dave Kern, Ethentica

Gene Kim, CTO, Tripwire Inc., USA

Jim Kolouch, BearingPoint

David Kowal, VP, JP Morgan Chase

Paul Kurtz, CSIA, Cyber Security Industry Alliance

Cindy LeRouge, Ph.D., Decision Sciences/MIS Department,

John Cook School of Business, St. Louis University, USA

Andrée Lavigne, CICA, Canadian Institute of Chartered Accountants

Debbie Lew, Guidance Software

Brenda Lovell, CIA, CCSA, CGAP, The IIA

Warren Malmquist, Adolph Coors Co.

Stacy Mantzaris, CIA, IIA

Dennis Miller, Heritage Bank

Patrick Morrissey, Auditwire

Bruce Moulton, Symantec

Paul Moxey, ACCA, Association of Chartered Certified Accountants

Roseane Paligo, CIA, Chief Financial Officer, 1st Choice Community Federal Credit Union, USA

Fred Palmer, Palmer Associates

Xenia Parker, CIA, CFSA, VP, Enterprise Technology Group, Marsh Inc.,

Bernie Plagman, TechPar Group

Heriot Prentice, MIIA, FIIA, QiCA, The IIA

Dick Price, Beacon IT Ltd., BS 7799 Consultancy, USA

Michael Quint, Corporate Compliance Officer, EDS Corporate Audit, USA

Sridhar Ramamoorti, CIA, CFSA, Ernst & Young LLP, Chicago, IL, USA

Amy Ray, Bentley College

Martin Ross, GSC, Global Security Consortium

Chip Schilb, EDS, USA

Howard Schmidt, eBay

Mark Silver, Symantec

George Spafford, President, Spafford Global Consulting, Saint Joseph, IL, USA

Adam Stone, Assurant

Jay H. Stott, CIA, Fidelity Investments

Dan Swanson, CIA, IIA

Jay R. Taylor, CIA, CISA, CFE, General Motors Corporation

Bill Tener, University & Community College System of Nevada

Archie Thomas

Fred Tompkins, BearingPoint

Don Warren, Rutgers University

Dominique Vincenti, CIA, The IIA

Mark Winn, Intrusec

Amit Yoran

23.4 IIA International Affiliates

Frank Alvern, CIA CCSA, Nordea Bank, Norway

Alexandre Alves Apparecido, Brazil

Dror Aviv, Israel

David F. Bentley, England, UK and Ireland

Gerardo Carstens, CIA, IIA Argentina

Richard Cascarino, South Africa

Iftikhar Chaudry, Pakistan

Hisham T. El Gindy, Manager, KPMG Hazem Hassan, Egypt

Dr. Ulrich Hahn, CIA, Switzerland

Rossana S. Javier, Makati City, Philippines

Andras Kovacks, Hungary

Christopher McRostie, Australia

Furqan Ahmad Saleem, Partner, Avais Hyder Nauman Rizwani RSM, Pakistan

Kyoko Shimizu, CIA, Japan

John Silltow, Security Control and Audit Ltd., United Kingdom

Ken Siong, International Federation of Accountants,

Anton van Wyk, PwC, South Africa

Nick Wolanin, Adjunt Senior Lecturer, Australian Graduate

Julie Young, Australia

23.5 Other International

Carolee Birchall, Vice President and Senior Risk Officer, Bank of Montreal, Canada

P. J. Corum, Quality Assurance Institute, Middle East and Africa, United Arab Emirates

Ariel Peled, President, ISSA Israeli Chapter

P. Shreekanth, India

Karen Woo, Selangor, Malaysia

23.6 IIA International Advanced Technology Committee

Anton van Wyk, (Chairman), CIA, PricewaterhouseCoopers, South Africa

Alexandre Alves Apparecido, Brasil Telecom, Brazil

Ken D. Askelson, CIA, JC Penney Co. Inc., USA

Dror Aviv, CFSA, IIA Israel

Donald L. Bailey, Grant Thornton, LLP, USA

E.W. Sean Ballington, PricewaterhouseCoopers, LLP, USA (originally South Africa)

Norman F. Barber, Microsoft Corp., USA

David F. Bentley, QiCA, Consultant, England

Claude Cargou, GIE AXA, France

Michael P. Fabrizius, CIA, Bon Secours Health System Inc., USA

Ramiz Tofigi Ganizade, Azerbaijan Republic Chamber of Auditors, Azerbaijan

Douglas Guerrero, EDS Corp., USA

Dr. Ulrich Hahn, CIA, Syngenta International, Switzerland

David J Hill, IBM Corp., USA

Michael S. Hines, CIA, Purdue University, USA

Mark J. Hornung, Ernst & Young LLP, USA

Gene Kim, CTO, Tripwire Inc., USA

David S. Lione, KPMG LLP Southeast Region, USA

Peter B. Millar, ACL Services Ltd., Canada

Allan M. Newstadt, CIA, World Bank/International Finance Corp., USA

Brenda J. S. Putman, CIA, City Utilities of Springfield, USA

Kyoko Shimizu, CIA, Shin Nihon & Co., Japan

Brian M. Spindel, CIA., SecurePipe Inc., USA

Rajendra P. Srivastava, University of Kansas, USA

Jay Stott, CIA, Fidelity Investments, USA

Jay R. Taylor, CIA, CISA, CFE, General Motors Corp., USA

Thomas Jason Wood, CIA, Ernst & Young LLP, USA

Akitomo Yamamoto, IIA, Japan

23.7 The Writing Team

David A. Richards, CIA, President, The IIA

Alan S. Oliphant, MIIA, QiCA, MAIR International

Charles H. Le Grand, CIA, CHL Global

23.8 IIA Headquarters Staff Production Team

Michael Feland

Trish Harris

Tim McCollum

Change and Patch Management: Critical for Organizational Success

The next publication for CAEs in the GTAG series will deal with IT change and patch management. Why has The IIA chosen to provide guidance on this subject? After all, isn't this something IT auditors already are handling?

Ultimately, this GTAG will be about managing risks that are a growing concern to those involved in the governance process. Like information security, management of IT changes is a fundamental process that can cause damage to the entire enterprise if it is not performed well. This enterprisewide impact makes change management of interest to many audit committees and, as a result, to top management.

The objective of this guide is to convey how effective and efficient IT change and patch management contributes to organizational success. The target audience is CAEs, their peers, and their staff. Because auditing's role requires it to assess risks and provide assurance to the organization, auditors cannot ignore the potential impact that changes to information systems and other IT assets can have on business operations. More importantly, this guide will give readers the necessary knowledge to talk more intelligently with their boards about change-management risks and controls and to help their organizations comply with constantly changing regulatory requirements.

What is the Internal Auditor's Role?

In most companies, the IT department has two primary roles: 1) operate and maintain existing services and commitments, and 2) deliver new products and services to help the business achieve its objectives. To accomplish their mission, IT departments implement processes that deliver services, create value, and manage resources. Each of these IT processes has inherent risks that must be managed.

Internal auditors are responsible for providing assurance that appropriate risk management processes are in place, including within IT. To this end, the importance of an effective change-management process — and performing regular internal audits — cannot be underestimated. The key point to remember is that change management is a process with a managerial and human focus, which is supported by technical and automated controls.

Using recently published research findings, this guide will help internal auditors ask the right questions of the IT organization to assess its change-management capability. It will describe a step-by-step approach, addressing the tough questions necessary to identify needed improvements in change-management process controls. Using the COSO Enterprise Risk Management model and other frameworks, the guide will provide the tools to identify effective and ineffective practices, including metrics that the IT department should be using to drive continuous improvement. Finally, it will feature a full audit program linked to CobiT control objectives for Information and Related Technology Infrastructure Library best practices.

Look for this new GTAG offering in July 2005.

GTAG — White Papers

The purpose of the following white papers is to provide insight into the internal controls around continuous auditing and the best practices for information security and risk management. These white papers use easy-to-read language to demonstrate how to identify problems and address solutions within these technical areas.

BUILDING AND IMPLEMENTING A CONTINUOUS CONTROLS MONITORING AND AUDITING FRAMEWORK

A White Paper

Authored by:
John G. Verver CA, CISA, CMC
Vice President, Professional Services
ACL Services Ltd

BUILDING AND IMPLEMENTING A CONTINUOUS CONTROLS MONITORING AND AUDITING FRAMEWORK

Ensuring the effectiveness of internal control systems is a key component of the audit process. Two primary stages are involved: ensuring that appropriate controls have been designed within a system and testing the effectiveness of these control systems using actual transactions.

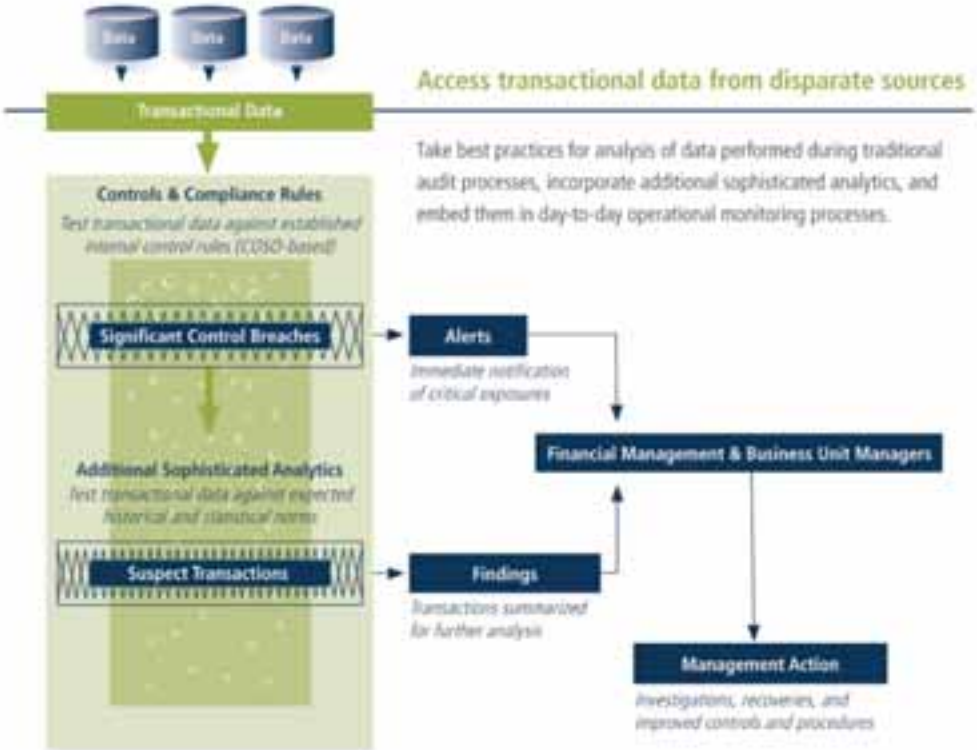
During the past 10 years, the audit profession has widely accepted data analysis technology as a critical tool to support both stages of the control validation process. This technology is used to examine transactions for indications of events that occur without an established control and to determine whether any transactions appear to have failed to meet the control standard. Data analysis also has a role to play in testing controls that are not directly evidenced by transactional data. For example, ERP access and authorization tables can be analyzed to determine whether there are failures to maintain appropriate segregation of duties.

The traditional audit process often relies on a representative sample of events and circumstances, rather than assessing a complete population of data. The audit process also generally takes place some considerable period of time after the business activities (transactions) have occurred. As a result, control problems have a greater opportunity to escalate and have a significant negative impact on the business. In terms of maximizing the effectiveness of the overall audit and control process, this traditional approach has clear limitations.

The solution to these deficiencies in the audit and control process can be addressed by developing a model for continuously monitoring and auditing transactions at, or almost immediately after, the point at which they occur. The key stages within the continuous monitoring and auditing model (see diagram below) include:

- Identifying the control rule for each internal control point within a given business process area according to an accepted controls framework, such as COSO
- Establishing the tests that, using transactional data analysis, will validate each control rule
- Establishing tests that will identify suspect transactions using transactional profiling techniques
- Testing all transactions on a regular, timely basis – preferably daily
- Identifying all transactions that fail the tests and notifying management according to the priority of the exception
- Investigating any transactions that fail and, as appropriate:
  - Correcting the transactions
  - Correcting the control problem

A Model for Continuous Controls Monitoring and Audit



The primary benefits of this model are the timeliness of notification to management of problem transactions and the independence of the process. It could be claimed that this model is redundant in an environment in which all transactions are processed through an enterprise resource planning (ERP) system where all appropriate controls have been activated. In practice, however, it is unusual for any ERP application to be implemented with all of the potential internal control mechanisms activated in an effective and comprehensive fashion. Even in cases where controls are initially well implemented, no ERP or other accounting system can be assured to continue to work on all occasions in a way that effectively maintains all desired controls. Users frequently circumvent controls to speed up or simplify the transaction entry process. There are also certain types of desirable transaction verification controls that simply are not practical to perform in the timeframes required to allow a system to operate effectively.

One of the greatest advantages of a model that *independently* monitors transactional data is just that – its independence from the underlying operational and financial systems. This adds to and strengthens an organization's existing management and control infrastructure and provides a mechanism that auditors can use and rely upon to support their review and assessment activities.

Ideally, an independent continuous monitoring process takes place in a timeframe that prevents any suspect transaction from completing. In practice, this can only be achieved in limited circumstances. The decision on the timing of the monitoring process depends on a variety of factors, including the degree of business risk specific control breaches represent, as well as the underlying technologies of the related application systems and data. Most objectives of the continuous monitoring model can be achieved by testing transactions on a daily basis.

The continuous monitoring model can directly support the goals of both organizational management and audit. Management is responsible for implementing and maintaining effective control systems. A continuous monitoring system allows management to gain assurance that the control systems are working effectively and to immediately respond to correct any deficiencies that may arise. Internal and external auditors are responsible for assessing whether management has successfully performed its control responsibilities. To the extent that a continuous monitoring system is part of a control framework, auditors need to confirm the effectiveness of the controls monitoring process itself. Having done that, auditors can review the output of the controls

monitoring system as evidence that will help them assess the overall effectiveness of control systems. Auditors also need to review the actions that have been taken to address the control exceptions that have been identified.

The key functional requirements of a continuous controls monitoring system include the ability to:

- Access and normalize disparate data from across the enterprise
- Perform a comprehensive range of tests designed to effectively address control points
- Vary the parameters used within the tests
- Test data and report results in a timely manner
- Handle large transactional volumes without having a negative impact on operational system performance
- Manage alert notifications
- Secure access to the continuous monitoring system and change its operating processes
- View and manage results

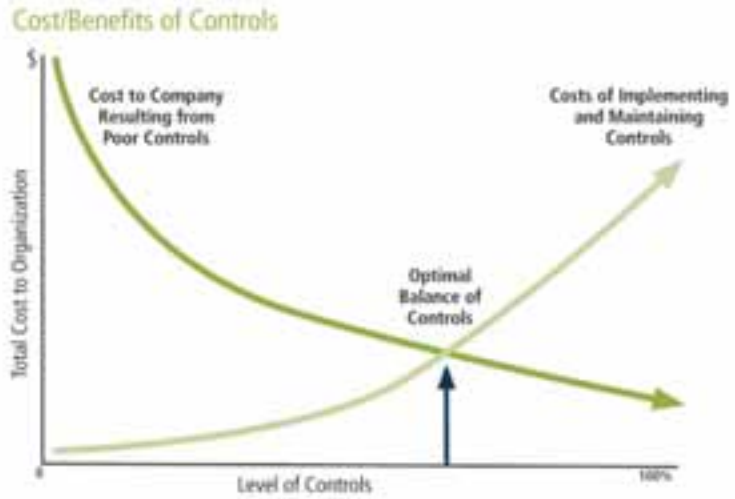
The goal of implementing a continuous controls monitoring system should ultimately be to subject all transactions within an enterprise to its processes. In practice, these systems are best implemented by starting with the business process areas in which identifying control exceptions will provide the most immediate and largest payback. In many organizations, this includes all of the key expenditure-related processes — such as purchases, payments, and payroll — as well as inventory, billing, and receivable systems.

The most significant challenges that are typically encountered when implementing a continuous controls monitoring system include:

- Gaining access to all relevant data in a timely manner
- Avoiding a significant impact on systems operational performance
- Defining the appropriate analytic that will effectively identify an exception to the control point
- Identifying the most effective point in time at which to perform the monitoring process
- Understanding the nature of the control tests when investigating the exceptions identified
- Accumulating and quantifying the total risk exposures that have been identified within the monitoring process
- Tuning the system to produce a manageable amount of results
- Balancing the costs and efforts of reviewing large volumes of exceptions against the cost and risk of the exposures themselves
- Developing a suitable scoring/weighting mechanism to prioritize exceptions

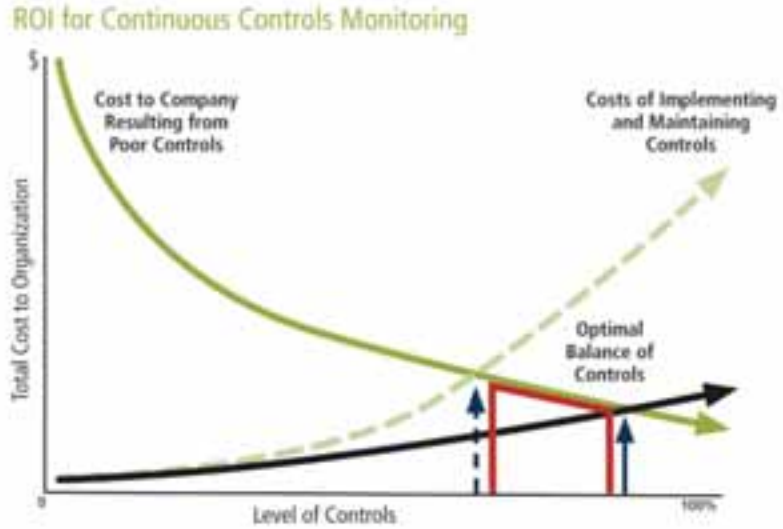
When managed effectively, the benefits of implementing a continuous controls monitoring system invariably outweigh the costs. The overall business case is usually twofold. First, good controls make sound business sense and directly benefit an enterprise by reducing instances of error, fraud, and inefficiency. Second, continuous controls monitoring is a powerful tool that supports compliance with increasingly widespread and complex regulatory requirements such as the U.S. Sarbanes-Oxley Act.

There is also a more specific business case for implementing a continuous controls monitoring system within most organizations. When considering any control structure, an organization should assess the cost of implementing the control versus the cost of no control.



The usual objective is to balance the cost of maintaining assurance over controls against an acceptable level of control. As the diagram below indicates, a 100 percent level of assurance over controls is unacceptably expensive. With traditional control and audit processes, the acceptable balance point provides far less than 100 percent assurance that no control exceptions have occurred.

However, when a continuous controls monitoring system is implemented, it effectively moves the balance point to provide a far higher level of assurance over controls for a relatively small increase in costs (see ROI for Continuous Controls Monitoring below).



In addition to achieving greater controls assurance, continuous monitoring frequently provides an immediate positive financial return to an organization by identifying inappropriate expenditures and missed revenues (billings) rapidly. Because problems can be discovered sooner, the chances of correcting the errors and recovering potential losses may be greatly increased, and small problems can be prevented from escalating into large ones.

By adopting a transactional analysis model for continuous monitoring and auditing of controls, auditors can assess controls effectiveness based on the evidence of the transactions. An additional level of assurance can be achieved by directly testing certain types of IT system controls within the continuous monitoring process. Such controls are usually defined according to an information systems controls framework such as the IT Governance Institute's Control Objectives for Information and Related Technology (CoBIT). These controls include, for example, systems access and authorization rights to ensure effective segregation of duties, as well as configuration settings within an ERP system.

The concept of continuous monitoring and auditing is not new to the internal audit profession. However, in organizations where the concept has been put into practice it has usually been on a limited basis, involving automated testing of a few controls on a recurring schedule. The opportunity now facing the internal audit profession is to implement continuous auditing on a comprehensive basis across all business process areas. The business reasons for doing so are becoming increasingly persuasive. For example, it is difficult to imagine how organizations that are required to comply with Sarbanes-Oxley Section 404 can perform ongoing internal control assessments in an effective and efficient manner without the use of continuous monitoring systems.

Several sources of further information on continuous monitoring and auditing are available for internal auditors, including general references in such publications as The Institute of Internal Auditors' *Global Technology Audit Guide Information Technology Controls*. More detailed information can also be found in *Continuous Auditing: Potential for Internal Auditors*, published by The Institute of Internal Auditors Research Foundation.

BIND VIEW Insight at Work

White Paper

Closing the Gaps on IT Security and Compliance

The objective of this whitepaper is to provide executives with insight into security and risk management best practices and how to translate these best practices into stronger IT controls through application of the COSO and Enterprise Risk Management framework. The paper also demonstrates how organizations have applied BindView technology to raise audit scores and strengthen overall security and configurations.

To learn more about BindView solutions, visit us at **www.bindview.com**. ***Click the links below to learn more about IT Controls for*** **Sarbanes-Oxley (www.bindview.com/soxtoolkit)** ***or*** **HIPAA Security (www.bindview.com/hipaatoolkit).**

I. COSO's Enterprise Risk Management Framework and its implications for IT Security/Risk Management

COSO is a voluntary private-sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance. In 2004, COSO released a new guideline addressing enterprise risk management in documentation known as the Enterprise Risk Management Integrated Framework. The framework defines essential enterprise risk management components, discusses key ERM principles and concepts, suggests a common ERM language, and provides clear direction and guidance for enterprise risk management.

Although the ERM Framework has broad application to many facets of control activities and risk management, this paper applies components of the ERM Framework only to information security risks. The ERM Framework features eight interrelated components paramount to mitigating risk as it relates to compliance requirements:

i. Internal Environment – Defined as the risk management philosophy of the organization, in which the commitment to competence, integrity, and ethical values is established. To gauge adherence to COSO best practices, ask:

- What is senior management's commitment to information security?
- Is a proactive security management team in place to help assess known vulnerabilities and determine how the organization will remediate problems and mitigate risks?
- Is this group empowered with talent, expertise, and budget?
- Is the team willing to identify and notify management of problems?

ii. Objective Setting – Defined as strategic objectives established in line with the enterprise's mission/vision and consistent with its risk appetite. Applying objective-setting principles to ensure the confidentiality, availability, and integrity of information involves much more than just buying a firewall and antivirus software. Questions to ask include:

- What is the organization's risk appetite regarding the security of information?
- How much risk is management willing to tolerate if systems fail, if confidential data is compromised, or if data integrity is breached?

iii. Event Identification – Uncertainties exist, and certain factors directly affect event occurrence. Events do not often occur in a vacuum; rather, one event creates a domino effect for other events, including those around information security. Security events that can impact your organization fall into two categories: Targeted attacks that include denial of service, information theft, and/or fraud;

WP2025 02.05

and random attacks that include viruses, port scans and hack of the month. To help identify risks associated with targeted and random attacks, ask:

- Is the organization at risk from targeted or random attacks?
- Is the system centralized or distributed, localized or global?
- What is the level of internal risk?

iv. Risk Assessment – Risk assessment allows organizations to consider how potential events might affect the achievement of business objectives. Consider risk perspectives: likelihood and impact. Identify the systems that are the most valuable to the organization and be sure to take only calculated risks. In defining calculated risks, ask:

- What aspects of the IT infrastructure are most vulnerable?
- What would be the consequences if they should fail or be breached?
- What is the likelihood of a successful attack or failure?
- How certain is management about the answers to the previous three questions?

In assessing risk management expenditures, take into account that theft of proprietary information and business disruption are two areas where organizations can potentially suffer the greatest financial loss from a security-related incident.

v. Risk Response – Effective enterprise risk management requires management to select a response that is expected to bring risk likelihood and impact within the organization's acceptable levels of risk tolerance. Risk responses fall into the categories of risk avoidance, reduction, sharing, and acceptance. To help determine the appropriate response, ask:

- What proactive and reactive steps are the organization prepared to take to remediate vulnerabilities and reduce overall risks?
- What automation is in place to reduce remediation time?
- Does the organization have an incident-response policy and procedures?

vi. Control Activities – Policies and procedures are necessary to help ensure risk responses are properly executed. IT security isn't just a technology issue — it's a people and process issue. The key to implementing effective risk management is to develop and employ well-defined, enforceable, and repeatable policies and processes to ensure the gaps are covered and the organization's risk posture is placed in line with its risk appetite. It's important to mandate technical requirements and appropriate rules. Ask:

- How often are policies audited against the system?
- Are policies enforceable?
- What best-practice configurations are in place?
- How is a new server deployed?
- How is the appropriate configuration assured?

vii. Information and Communication – Gathering data from all levels of an organization is imperative to identify, assess and respond to risks. Processing this information — including its identification, management, and communication — is an ever-increasing challenge to the IT department given the other responsibilities it must meet. The solution is to establish an information systems infrastructure that sources, captures, processes, analyzes, and reports relevant information. Ask:

- How are policies communicated company-wide?
- How is the organization tracking accountability for acceptance and adherence to policy?
- How is the organization doing in terms of security today, in comparison to last week, last month and the last audit?
- What reporting, if any, is available to management that communicates the state of compliance to IT policies?

viii. Monitoring – Monitoring is verifying the proper functioning of risk management and the quality of performance over time. Monitoring is performed through ongoing, proactive activities that continuously compare the current environment to the established best practices of the organization. Separate evaluations — purely reactive — take place after an event has occurred. Reporting deficiencies to the appropriate level within the organization is critical.

Deficiencies are conditions where there is a real or potential shortcoming or where this is an opportunity to strengthen the process. Questions to ask include:

- How does the organization monitor compliance of network systems to policies and procedures?
- How often is the environment audited?
- Does the organization spot check systems for compliance?
- How does the organization ensure consistency?

II. Ensuring systems security

When building IT controls organizations need to ensure the confidentiality, integrity, and availability of business-critical information. Supporting this goal are two key control areas defined by the CobiT framework for IT governance and are ensuring systems security and managing the configurations of systems.

Challenges:

- The number of vulnerabilities is growing, and it is becoming increasingly difficult to assess and remediate systems before a new attack is released.
- Having the right policies in place.
- Developing and maintaining effective end-user management and access control.
- Limited scope of security — not enough servers, workstations evaluated.

Common Security Mistakes:

- Limited scope of security — not enough servers, workstations evaluated.
- Security policy, processes, and procedures are inconsistent, nonexistent, outdated, or not approved.
- Security policy is unenforceable and/or has no built-in accountability.
- False belief that most experienced IT administrators are security experts.
- False belief that some manual processes are less expensive.
- Lack of password management leaves an enterprise vulnerable.
- Unsupported Windows 2000 and Windows Server 2003 — system complexities hide full benefits.

"BindView helps to satisfy the regulators who are looking for best practices, regulatory compliance, and the ability to delegate limited functionality, such as password resets to the Help Desk. BindView helps us gain efficiency without sacrificing security."

– Marion Lang,
Manager of Information Security
BankAtlantic

Case Studies:

For one of BindView's customers, security became a top focus as public awareness of security threats grew. The executive team was concerned that failure to identify vulnerabilities in the company's internal networks could lead to a major incident that could compromise critical systems and data.

To take immediate and corrective action, the customer implemented BindView Vulnerability Management solutions to provide timely reporting on its network and eliminate a large volume of stale user accounts created from high employee turnover. The customer required a solution that could scale to a large and complex environment and could enable it to meet previously unattainable security goals without increasing IT headcount.[1]

In a separate case, a BindView financial institution customer faced a familiar challenge in which the organization was growing, but the security staff was not. How could policies be monitored effectively on an ongoing basis? BindView solutions provided the customer with the overview and control features for multi-platform environments that assured adherence to policies not just once, but on an ongoing basis.[2]

A third BindView customer wanted to restrict employee access to available system capabilities. With BindView Directory Administration solutions, the customer was able to restrict access at the user and function levels. Directory Admin overlays the Windows environment, providing customers with the ability to further segregate duties. This technical capability helps customers comply with security best practices.[3]

[1] See B&Q Customer Case Study on bindview.com
[2] See Bank Atlantic Customer Case Study on bindview.com
[3] See Toyota Kreditbank Customer Case Study on bindview.com

III. Manage the configuration

Insufficient configuration controls can lead to security and availability exposures that may permit unauthorized access to systems and data, which would negatively impact an organization's ability to meet the internal control provisions of Section 404. Managing the configuration is a proactive approach to security that implements known best-practice configurations to eliminate security holes.

Challenges:

- Case law has yet to establish minimum due care requirements.
- A *de facto* best-practices standard has not been accepted widely.
- Ever-shorter lapses between patch introductions and new attacks, with new vulnerabilities, are occurring more frequently.
- Shorter lapses compress patch management remediation and testing time, making more automation necessary.

Common Configuration Mistakes:

- Leaving default settings on deployed servers.
- Leaving unnecessary services activated.
- Leaving default passwords on deployed servers.
- Building too many security roadblocks into the patch remediation path.

What are auditors looking for?

When it comes to assessing the *configuration* of internal controls, especially those settings over financial controls, external auditors are required to ask for third-party verification of the objectivity involved in the configuration assessment. The U.S. Sarbanes-Oxley Act of 2002 expressly prohibits an auditor from relying on the results of management-sponsored testing.

"The greatest thing about the Vulnerability Management solution is the automation it provides. Compared to the manual steps, BindView has saved us one workday per week in the auditing process."

– **Andreas Hermsdorf,** *Toyota Kreditbank GmbH*

Case Studies:

One BindView customer encountered added pressure to both increase administration efficiency and maintain strict security measures, a common paradox facing IT management today. At this company, two things had to change: Security had to be improved and auditing needed to become automated. Users needed to access sensitive information quickly, but within a controlled environment that guarded against the data being misused or compromised.

By implementing BindView solutions, the customer was able to document the configuration of file servers and then allow staff to run reports against the initial baseline report, an automation advance that saved considerable time and effort. In addition, BindView's offline data storage capabilities help reduce costs and can provide important historical comparisons and graphics.*

Conclusion

Maintaining compliance within an organization can erode profitability if the proper IT controls and automation of processes and procedures supporting the controls are not in place. With BindView, enterprises have the knowledge, experience, and expertise essential to help solve immediate compliance issues. BindView solutions enable customers to effectively manage their IT/security infrastructures at desired levels of protection, acceptable levels of risk, and the lowest total cost of ownership.

Since 1990, more than 5000 organizations have relied on BindView solutions to make their infrastructure, day-to-day transactions, and financial future more secure. Today, BindView equips organizations with the power to assure regulatory compliance, reduce business disruption and losses, and lower SG&A expenses. BindView software provides organizations with tools to protect and secure their computer systems, applications, and networks. The automated business policies can be tracked and enforced. Configuration and security holes may be identified before they can be attacked, and user security can be managed to ensure proper access and control.

* See Toyota Kreditbank Customer Case Study on bindview.com

GTAG

Information Technology Controls

This guide focuses on how IT roles and responsibilities are dispersed throughout the organization, how accurate assessment of IT controls is achieved, and how an organization can promote IT reliability and efficiency.

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, or security. GTAG is a ready resource series for chief audit executives to use in the education of members of the board and audit committee, management, process owners, and others regarding technology-associated risks and recommended practices.

The Institute of Internal Auditors

247 Maitland Ave. • Altamonte Springs, Florida 32701 USA • www.theiia.org