Figure 1—Control Processes

	PCAOB IT General Control Heading			
CobiT Control Objective Heading	Program Development	Program Changes	Computer Operations	Access to Programs and Data
1. Acquire or develop application software.	●	●	●	●
2. Acquire technology infrastructure.	●	●	●	
3. Develop and maintain policies and procedures.	●	●	●	●
4. Install and test application software and technology infrastructure.	●	●	●	●
5. Manage changes.		●		●
6. Define and manage service levels.	●	●	●	●
7. Manage third-party services.	●	●	●	●
8. Ensure systems security.			●	●
9. Manage the configuration.			●	●
10. Manage problems and incidents.			●	
11. Manage data.			●	●
12. Manage operations.			●	●

The information contained in this document provides a logical starting point for affected organizations. However, a one-size-fits-all approach is not appropriate. This has been explicitly recognized by the PCAOB in Release No. 2004-001, 9 March 2004:

> *Internal control is not "one-size-fits-all," and the nature and extent of controls that are necessary depend, to a great extent, on the size and complexity of the company.*

Note: Each organization should carefully consider the appropriate IT control objectives for its own circumstances. The organization may not include all the control objectives discussed in this document, or it may include others not discussed in this document.

Accordingly, each organization should tailor an IT control approach suitable to its size and complexity. In doing so, it is expected that changes will be made to the controls included in this document to reflect the specific circumstances of each organization. This document should not be a basis for audit reliance, and as such, it is advisable that organizations discuss IT control approaches with their external auditors to obtain their perspective on IT control objectives that should be addressed.

What Has Changed From October 2003?

The original publication of *IT Control Objectives for Sarbanes-Oxley* was released in October 2003 as a discussion document. The document generated significant discussion and comments from SEC-registrant organizations, public accounting firms, lawyers, consultants and others. Comments were varied, ranging from concerns that more controls were needed to concerns that there were too many controls. By far, the most common comment was that guidance on IT controls was needed to provide direction on the nature of IT controls over financial reporting and the extent of testing that should be performed. In response, the contributors weighed the comments from all parties and revised this document to reflect suggested changes and improvements.

The most significant change was made to the appendices. Many of the comments suggested that the control objectives included in the October 2003 document were too numerous. As a result, control objectives that formed part of the Plan and Organize and Monitor and Evaluate components of COBIT were removed and replaced with a company-level IT control environment questionnaire. It was felt that this would provide a more efficient and representative means to understand the IT control environment and its impact on the activities of the IT organization. The control objectives that formed the Acquire and Implement and Deliver and Support areas of COBIT were redrafted, and illustrative control activities and a summary control objective was created for each.

Another change reflected the desire for testing suggestions. To support the illustrative control activities, tests of controls were prepared as examples for senior management and business process owners looking for ways to evaluate the effectiveness of these controls. A further change was made to more closely model the order and categorization of controls after the IT general control concepts discussed in the PCAOB rules, namely program development, program change, computer operations, and access to programs and data.

Disclaimer

The IT Governance Institute, Information Systems Audit and Control Association® and other contributors make no claim that use of this document will assure a successful outcome. This publication should not be considered inclusive of IT controls, procedures and tests, or exclusive of other IT controls, procedures and tests that may be reasonably present in an effective internal control system over financial reporting. In determining the propriety of any specific control, procedure or test, SEC registrants should apply appropriate judgment to the specific control circumstances presented by the particular systems or information technology environment.

Readers should note that this document has not received endorsement from the SEC, the PCAOB or any other standard-setting body. The issues that are dealt with in this publication will evolve over time. Accordingly, companies should seek counsel and appropriate advice from their risk advisors and/or auditors. The contributors make no representation or warranties and provide no assurances that an organization's use of this document will result in disclosure controls and procedures and the internal controls and procedures for financial reporting that are compliant with the requirements and the internal control reporting requirements of the Act, nor that an organization's plans will be sufficient to address and correct any shortcomings that would prohibit the organization from making the required certification or reporting under the Act.

Internal controls, no matter how well designed and operated, can provide only reasonable assurance of achieving an entity's control objectives. The likelihood of achievement is affected by limitations inherent to internal control. These include the realities that human judgment in decision-making can be faulty and that breakdowns in internal control can occur because of human failures such as simple errors or mistakes. Additionally, controls, whether manual or automated, can be circumvented by the collusion of two or more people or inappropriate management override of internal controls.

Acknowledgements

The contributors to this document include many representatives from industry and the public accounting profession. As such, this document is a combination of the input obtained from all contributors and does not expressly represent the viewpoint of any specific contributor, nor the companies or firms at which they are employed.

The IT Governance Institute wishes to thank the following contributors for their participation in developing this document:
Allstate Insurance Corporation
Crowe Chizek LLP
Deloitte & Touche LLP
Ernst &Young LLP
Electrolux AB
EnCana Corporation
Financial Executives Research Foundation
Forsythe Solutions
International Vision & Solutions
IT Winners Ltd.
KPMG LLP
LMS Associates LLP
Meta Group Inc.
Protiviti Inc.
Royal Bank Financial Group
The Great-West Life Assurance Company
The Q Alliance
University of Southern California
Waveset Technologies

The ITGI Board of Trustees, for its support of the project

Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, International President, ITGI
Abdul Hamid Bin Abdullah, CISA, CPA, Auditor General's Office, Singapore, Vice President, ITGI
Ricardo J. Bria, CISA, Argentina, Vice President, ITGI
Everett C. Johnson, CPA, Deloitte & Touche LLP, USA, Vice President, ITGI
Dean R.E. Kingsley, CISA, CISM, CA, Deloitte Touche Tohmatsu, Australia, Vice President, ITGI
Eddy Schuermans, CISA, PricewaterhouseCoopers LLP, Belgium, Vice President, ITGI
Robert S. Roussey, CPA, University of Southern California, USA, Past International President, ITGI
Paul A. Williams, FCA, Paul Williams Consulting, UK, Past International President, ITGI
Emil G. D'Angelo, CISA, Bank of Tokyo-Mitsubishi, USA, Trustee, ITGI
Ronald Saull, CSP, The Great-West Life Assurance Company, Canada, Trustee, ITGI
Erik Guldentops, CISA, CISM, Belgium, Advisor, ITGI

The ITGI Research Board, for overseeing and guiding the project

Chairperson, Lily M. Shue, CISA, CISM, CCP, CITC, LMS Associates, USA
Jayant Ahuja, CISA, CPA, CMA, PricewaterhouseCoopers LLP, USA
Candi Carrera, CF 6 Luxembourg, Luxembourg
John Ho Chi, CFE, Ernst & Young LLP, Singapore
Avinash W. Kadam, CISA, CISSP, CBCP, GSEC, CQA, MIEL E-Security Pvt. Ltd., India
Elsa K. Lee, CISA, CSQA, Crowe Chizek LLP, USA
Robert G. Parker, CISA, CA, FCA, CMC, Deloitte & Touche LLP, Canada
Michael Schirmbrand, Ph.D., CISA, CISM, CPA, KPMG LLP, Austria
Johann Tello Meryk, CISA, CISM, Banco del Istmo, Panama
Frank van der Zwaag, CISA, CISSP, Air New Zealand, New Zealand
Paul A. Zonneveld, CISA, CISSP, CA, Deloitte & Touche LLP, Canada

Sarbanes-Oxley—A Focus on Internal Control

The Sarbanes-Oxley Act demonstrates firm resolve by the US Congress to improve corporate responsibility. The Act was created to restore investor confidence in US public markets, which was damaged by business scandals and lapses in corporate governance. Although the Act and supporting regulations have rewritten the rules for accountability, disclosure and reporting, the Act's many pages of legalese support a simple premise: good corporate governance and ethical business practices are no longer optional niceties.

Sarbanes-Oxley—Enhancing Corporate Accountability

The Sarbanes-Oxley Act has fundamentally changed the business and regulatory environment. The Act aims to enhance corporate governance through measures that will strengthen internal checks and balances and, ultimately, strengthen corporate accountability. However, it is important to emphasize that section 404 does not require senior management and business process owners merely to establish and maintain an adequate internal control structure, but also to assess its effectiveness on an annual basis. This distinction is significant.

For those organizations that have begun the compliance process, it has quickly become apparent that IT plays a vital role in internal control. Systems, data and infrastructure components are critical to the financial reporting process. PCAOB Auditing Standard No. 2 discusses the importance of IT in the context of internal control. In particular, it states:

> *The nature and characteristics of a company's use of information technology in its information system affect the company's internal control over financial reporting.*

To this end, IT professionals, especially those in executive positions, need to be well versed in internal control theory and practice to meet the requirements of the Sarbanes-Oxley Act. CIOs must now take on the challenges of (1) enhancing their knowledge of internal control, (2) understanding their organization's overall Sarbanes-Oxley compliance plan, (3) developing a compliance plan to specifically address IT controls, and (4) integrating this plan into the overall Sarbanes-Oxley compliance plan.

Accordingly, the goal of this publication is to offer support to those responsible for corporate IT systems on the following:

A. Assessing the current state of the IT control environment
B. Designing controls necessary to meet the directives of Sarbanes-Oxley section 404
C. Closing the gap between A and B

Specific Management Requirements of the Sarbanes-Oxley Act

Much of the discussion surrounding the Sarbanes-Oxley Act has focused on sections 302 and 404. A brief primer can be found in **figure 2**.

Figure 2—Sarbanes-Oxley Requirements Primer

	302	404
Who	A company's management, with the participation of the principal executive and financial officers (the certifying officers)	Corporate management, executives and financial officer ("management" has not been defined by the PCAOB)
What	1. Certifying officers are responsible for establishing and maintaining internal control over financial reporting. 2. Certifying officers have designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under their supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles.* 3. Any changes in the company's internal control over financial reporting that have occurred during the most recent fiscal quarter and have materially affected, or are reasonably likely to materially affect, the company's internal control over financial reporting are disclosed. 4. When the reason for a change in internal control over financial reporting is the correction of a material weakness, management has a responsibility to determine whether the reason for the change and the circumstances surrounding that change are material information necessary to make the disclosure about the change not misleading.	1. A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company 2. A statement identifying the framework used by management to conduct the required assessment of the effectiveness of the company's internal control over financial reporting 3. An assessment of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year, including an explicit statement as to whether internal control over financial reporting is effective 4. A statement that the registered public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management's assessment of the company's internal control over financial reporting 5. A written conclusion by management about the effectiveness of the company's internal control over financial reporting included both in its report on internal control over financial reporting and in its representation letter to the auditor. The conclusion about the effectiveness of a company's internal control over financial reporting can take many forms. However, management is required to state a direct conclusion about whether the company's internal control over financial reporting is effective. 6. Management is precluded from concluding that the company's internal control over financial reporting is effective if there are one or more material weaknesses. In addition, management is required to disclose all material weaknesses that exist as of the end of the most recent fiscal year.

Figure 2—Sarbanes-Oxley Requirements Primer *(cont.)*

	302	404
When	Already in effect as of July 2002	Year-ends beginning on or after 15 November 2004**
How Often	Quarterly and annual assessment	Annual assessment by management and independent auditors
	*Annual for foreign private issuers	**Nonaccelerated filers (<US $75 million) can defer to 15 July 2005

Disclosure Controls and Procedures

Disclosure controls and procedures refer to the processes in place designed to ensure that all material information is disclosed by an organization in the reports it files or submits to the SEC. These controls also require that disclosures are authorized, complete and accurate and are recorded, processed, summarized and reported within the time periods specified in the SEC's rules and forms. Deficiencies in controls, as well as any significant changes to controls, must be communicated to the organization's audit committee and auditors in a timely manner. An organization's principal executive officer and financial officer must certify the existence of these controls on a quarterly basis.

Section 302 Management Requirements

Section 302:

> *…Requires a company's management, with the participation of the principal executive and financial officers (the certifying officers), to make the following quarterly and annual certifications with respect to the company's internal control over financial reporting:*
>
> - *A statement that the certifying officers are responsible for establishing and maintaining internal control over financial reporting*
> - *A statement that the certifying officers have designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under their supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles*
> - *A statement that the report discloses any changes in the company's internal control over financial reporting that occurred during the most recent fiscal quarter (the company's fourth fiscal quarter in the case of an annual report) that have materially affected, or are reasonably likely to materially affect, the company's internal control over financial reporting*

When the reason for a change in internal control over financial reporting is the correction of a material weakness, management has a responsibility to determine and the auditor should evaluate whether the reason for the change and the circumstances surrounding that change are material information necessary to make the disclosure about the change not misleading.

Section 404 Management Requirements

The directives of Sarbanes-Oxley section 404 require that management provide an annual report on its assessment of internal control over financial reporting in the annual filing. It states:

> *Management's report on internal control over financial reporting is required to include the following:*
>
> - *A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company*
> - *A statement identifying the framework used by management to conduct the required assessment of the effectiveness of the company's internal control over financial reporting*
> - *An assessment of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year, including an explicit statement as to whether that internal control over financial reporting is effective*
> - *A statement that the registered public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management's assessment of the company's internal control over financial reporting*
>
> *Management should provide, both in its report on internal control over financial reporting and in its representation letter to the auditor, a written conclusion about the effectiveness of the company's internal control over financial reporting. The conclusion about the effectiveness of a company's internal control over financial reporting can take many forms; however, management is required to state a direct conclusion about whether the company's internal control over financial reporting is effective.*
>
> *Management is precluded from concluding that the company's internal control over financial reporting is effective if there are one or more material weaknesses. In addition, management is required to disclose all material weaknesses that exist as of the end of the most recent fiscal year.*

Internal Control Over Financial Reporting

Internal control over financial reporting is defined by the SEC as:

> *A process designed by, or under the supervision of, the registrant's principal executive and principal financial officers, or persons performing similar functions, and effected by the registrant's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:*
>
> *(1) Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the registrant*
>
> *(2) Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the registrant are being made only in accordance with authorizations of management and directors of the registrant*
>
> *(3) Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements.*

The PCAOB uses the same definition except that the word "registrant" has been replaced by the word "company."

Management might be able to accurately represent that internal control over financial reporting, as of the end of the company's most recent fiscal year, is effective even if one or more material weaknesses existed during the period. To make this representation, management must have changed the internal control over financial reporting to eliminate the material weaknesses sufficiently in advance of the "as of" date and have satisfactorily tested the effectiveness over a period of time that is adequate for it to determine whether, as of the end of the fiscal year, the design and operation of internal control over financial reporting is effective.

Auditor Focus Under Sarbanes-Oxley

Auditor Attestation

An added challenge is that section 404 requires a company's independent auditor to attest to management's assessment of its internal control over financial reporting. Not only must organizations ensure that appropriate controls (including IT controls) are in place, they must also provide their independent auditors with documentation, evidence of functioning controls and the documented results of testing procedures.

Under the Sarbanes-Oxley Act, standards for the auditor's attestation are now the responsibility of the PCAOB. While the 404 attestation is "as of" a specific date, PCAOB Auditing Standard No. 2 specifically addresses financial reporting controls that should be in place for a period before the attestation date and controls that may operate after the attestation date. It states:

> *The auditor's testing of the operating effectiveness of such controls should occur at the time the controls are operating. Controls "as of" a specific date encompass controls that are relevant to the company's internal control over financial reporting "as of" that specific date, even though such controls might not operate until after that specific date.*

It is suggested that management meet with the external auditors to determine the period of time a control is required to be operating before the attestation date.

Auditor Evaluation Responsibilities

PCAOB Auditing Standard No. 2 discusses the external auditor's responsibilities in regards to 302. In particular, it states:

> *The auditor's responsibility as it relates to management's quarterly certifications on internal control over financial reporting is different from the auditor's responsibility as it relates to management's annual assessment of internal control over financial reporting. The auditor should perform limited procedures quarterly to provide a basis for determining whether he or she has become aware of any material modifications that, in the auditor's judgment, should be made to the disclosures about changes in internal control over financial reporting in order for the certifications to be accurate and to comply with the requirements of Section 302 of the Act.*

> *To fulfill this responsibility, the auditor should perform, on a quarterly basis, the following procedures:*
>
> - *Inquire of management about significant changes in the design or operation of internal control over financial reporting as it relates to the preparation of annual as well as interim financial information that could have occurred subsequent to the preceding annual audit or prior review of interim financial information;*
> - *Evaluate the implications of misstatements identified by the auditor as part of the auditor's required review of interim financial information (See AU sec. 722, Interim Financial Information) as it relates to effective internal control over financial reporting; and*
> - *Determine, through a combination of observation and inquiry, whether any change in internal control over financial reporting has materially affected, or is reasonably likely to materially affect, the company's internal control over financial reporting.*

Fraud Considerations in an Audit of Internal Control Over Financial Reporting

The introduction to PCAOB Auditing Standard No. 2 provides specific reference to fraud considerations:

> *Strong internal controls also provide better opportunities to detect and deter fraud. For example, many frauds resulting in financial statement restatement relied upon the ability of management to exploit weaknesses in internal control. To the extent that internal control reporting can help restore investor confidence by improving the effectiveness of internal controls (and reducing the incidence of fraud), assessments of internal controls over financial reporting should emphasize controls that prevent or detect errors as well as fraud.*
>
> *For this reason, the proposed standard specifically addresses and emphasizes the importance of controls over possible fraud. It requires the auditor to test controls specifically intended to prevent or detect fraud likely to result in the material misstatement of the financial statements.*

PCAOB Auditing Standard No. 2 addresses fraud considerations and, in particular, it states that:

> *…Part of management's responsibility when designing a company's internal control over financial reporting is to design and implement programs and controls to prevent, deter, and detect fraud.*

The Foundation for Reliable Financial Reporting

IT professionals understand the critical role that IT plays in the operations of an organization. Indeed, it is difficult to imagine a successful organization existing in the 21st century without some level of reliance on IT systems.

In today's environment, financial reporting processes are driven by IT systems. Such systems, whether enterprise resource planning (ERP) or otherwise, are deeply integrated in the initiating, authorizing, recording, processing and reporting of financial transactions. As such, they are inextricably linked to the overall financial reporting process and need to be assessed, along with other important processes, for compliance with the Sarbanes-Oxley Act.

To emphasize this point, PCAOB Auditing Standard No. 2 discusses the relationship of IT and its importance in testing the design and operational effectiveness of internal control. In particular, it states:

> *…Controls should be tested, including controls over relevant assertions related to all significant accounts and disclosures in the financial statements. Generally, such controls include [among others]:*
>
> - *Controls, including information technology general controls, on which other controls are dependent.*

PCAOB Auditing Standard No. 2 continues by describing the process that auditors should follow in determining the appropriate assertions or objectives to support management's assessment:

> *To identify relevant assertions, the auditor should determine the source of likely potential misstatements in each significant account. In determining whether a particular assertion is relevant to a significant account balance or disclosure, the auditor should evaluate [among others]:*
>
> - *The nature and complexity of the systems, including the use of information technology by which the company processes and controls information supporting the assertion.*

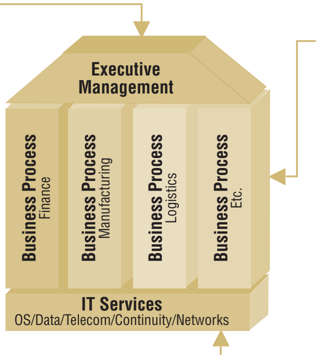
PCAOB Auditing Standard No. 2 also specifically addresses information technology in period-end financial reporting:

> *As part of understanding and evaluating the period-end financial reporting process, the auditor should evaluate [among others]:*
>
> - *The extent of information technology involvement in each period-end financial reporting process element;*

At least three common elements exist within all organizations—enterprise management, business process and shared service.

Figure 3—Common Elements of Organizations

Company-level Controls
Company-level controls over the IT control environment set the tone for the organization. Examples include:
- Operating style
- Enterprise policies
- Governance
- Collaboration
- Information sharing



Application Controls
Controls embedded in business process applications, such as large ERP systems and smaller best-of-breed systems, are commonly referred to as application controls. Examples include:
- Completeness
- Accuracy
- Validity
- Authorization
- Segregation of duties

General Controls
Controls embedded in IT services form general controls. Examples include:
- Program development
- Program changes
- Computer operations
- Access to programs and data

Executive Management	Business Process	IT Services
Executive management establishes and incorporates strategy into business activities. At the enterprise or entity level, business objectives are set, policies are established, and decisions are made on how to deploy and manage the resources of the organization. From an IT perspective, policies and other enterprisewide guidelines are set and communicated throughout the organization.	Business processes are the organization's mechanism of creating and delivering value to its stakeholders. Inputs, processing and outputs are functions of business processes. Increasingly, business processes are being automated and integrated with complex and highly efficient IT systems.	Shared services are those that are required by more than one department or process and are often delivered as a common service. From an IT perspective, services such as security, telecommunications and storage are necessary for any department or business unit and are often managed by a central IT function.

Figure 3 demonstrates how IT controls are embedded within each element of business. For instance, consider the following areas where IT enables the controls sought for reliable financial reporting:

- Information management and data classification
- Role-based user management (authentication, initiation and authorization of transactions)
- Real-time reporting
- Transaction thresholds and tolerance levels
- Data processing integrity and validation

More and more, IT systems are automating business process activities and providing functionality that enables as much or as little control as necessary. As such, compliance programs need to include system-based controls to keep up-to-date with contemporary financial systems.

Information Technology Controls—A Unique Challenge

The Sarbanes-Oxley Act makes corporate executives explicitly responsible for establishing, evaluating and monitoring the effectiveness of internal control over financial reporting. For most organizations, the role of IT will be crucial to achieving this objective. Whether through a unified ERP system or a disparate collection of operational and financial management software applications, IT is the foundation of an effective system of internal control over financial reporting.

Yet, this situation creates a unique challenge: many of the IT professionals being held accountable for the quality and integrity of information generated by their IT systems are not well versed in the intricacies of internal control. This is not to suggest that risk is not being managed by IT, but rather that it may not be formalized or structured in a way required by an organization's management or its auditors.

Organizations need representation from IT on their Sarbanes-Oxley teams to ensure that IT general controls and application controls exist and support the objectives of the compliance effort. Some of the key areas of responsibility for IT include:

- Understanding the organization's internal control program and its financial reporting process
- Mapping the IT systems that support internal control and the financial reporting process to the financial statements
- Identifying risks related to these IT systems
- Designing and implementing controls designed to mitigate the identified risks and monitoring them for continued effectiveness
- Documenting and testing IT controls
- Ensuring that IT controls are updated and changed, as necessary, to correspond with changes in internal control or financial reporting processes
- Monitoring IT controls for effective operation over time
- Participation by IT in the Sarbanes-Oxley project management office

The SEC regulations that affect the Sarbanes-Oxley Act are undeniably intricate, and implementation will be both time-consuming and costly. In proceeding with an IT control program, there are two important considerations that should be taken into account:

1. There is no need to reinvent the wheel; virtually all public companies have some semblance of IT control. While they may be informal and lacking sufficient documentation of the control and evidence of the control functioning, IT controls generally exist in areas such as security and change management.

2. Many organizations will be able to tailor existing IT control processes to comply with the provisions of the Sarbanes-Oxley Act. Frequently, it is the consistency and quality of control documentation and evidential matter that is lacking, but the general process is often in place, only requiring some modification.

Performing a thorough review of IT control processes and documenting them as the enterprise moves forward will be a time-consuming task. Without appropriate knowledge and guidance, organizations will run the risk of doing too much or too little. This risk is amplified when those responsible are not experienced in the design and assessment of IT controls or lack the necessary skill or management structure to identify and focus on the areas of most significant risk.

While some industries, such as financial services, are familiar with stringent regulatory and compliance requirements of public market environments, most are not. To meet the demands of the Sarbanes-Oxley Act, most organizations will require a change in culture. More likely than not, enhancements to IT systems and processes will be required, most notably in the design, documentation, retention of control evidence and evaluation of IT controls. Because the cost of noncompliance can be devastating to an organization, it is crucial to adopt a proactive approach and take on the challenge early.

Controls Over Information Technology Systems

With widespread reliance on IT systems, controls are needed over all such systems, large and small. IT controls commonly include controls over the IT environment, computer operations, access to programs and data, program development and program changes. These controls apply to all systems—from mainframe through client-server environments.

IT Control Environment

The control environment has become more important in PCAOB Auditing Standard No. 2. The standard states that:

> *…Because of the pervasive effect of the control environment on the reliability of financial reporting, the auditor's preliminary judgment about its effectiveness often influences the nature, timing, and extent of the tests of operating effectiveness considered necessary. Weaknesses in the control environment should cause the auditor to alter the nature, timing, or extent of tests of operating effectiveness that otherwise should have been performed in the absence of the weaknesses.*

The PCAOB has also indicated that an ineffective control environment should be regarded as at least a significant deficiency and as a strong indicator that a material weakness in internal control over financial reporting exists. These comments apply to the overall control environment, which includes the IT control environment.

The IT control environment includes the IT governance process, monitoring and reporting. The IT governance process includes the information systems strategic plan, the IT risk management process, compliance and regulatory management, IT policies, procedures and standards. Monitoring and reporting are required to ensure that IT is aligned with business requirements.

The IT governance structure should be designed to help ensure that IT adds value to the business and that IT risks are mitigated. This also includes an IT organization structure that supports adequate segregation of duties and promotes the achievement of the organization's objectives.

Computer Operations

These include controls over the definition, acquisition, installation, configuration, integration and maintenance of the IT infrastructure. Ongoing controls over operation address the day-to-day delivery of information services, including service level management, management of third-party services, system availability, customer relationship management, configuration and systems management, problem and incident management, operations management scheduling and facilities management.

The system software component of operations includes controls over the effective acquisition, implementation, configuration and maintenance of operating system software, database management systems, middleware software, communications software, security software and utilities that run the system and allow applications to function. System software also provides the incident tracking, system logging and monitoring functions. System software can report on uses of utilities, so that if someone accesses these powerful data-altering functions, at the least their use is recorded and reported for review.

Access to Programs and Data

Access controls over programs and data assume greater importance as internal and external connectivity to entity networks grows. Internal users may be halfway around the world or down the hall, and there may be thousands of external users accessing, or trying to access, entity systems. Effective access security controls can provide a reasonable level of assurance against inappropriate access and unauthorized use of systems. If well designed, they can intercept unethical hackers, malicious software and other intrusion attempts.

Adequate access control activities, such as secure passwords, Internet firewalls, data encryption and cryptographic keys, can be effective methods of preventing unauthorized access. User accounts and related access privilege controls restrict the applications or application functions only to authorized users that need them to do their jobs, supporting an appropriate division of duties. There should be frequent and timely review of the user profiles that permit or restrict access. Former or disgruntled employees can be a threat to a system; therefore, terminated employee passwords and user IDs should be revoked immediately. By preventing unauthorized use of, and changes to, the system, an entity protects its data and program integrity.

Program Development and Program Change

Application software development and maintenance has two principle components: the acquisition and implementation of new applications and the maintenance of existing applications.

The acquisition and implementation of new applications continue to be areas with a high degree of failure. Many implementations are considered to be outright failures, as they do not fully meet business requirements and expectations or are not implemented on time or within budget.

To reduce acquisition and implementation risks, some entities have a form of system development and quality assurance methodology. Standard software tools and IT architecture components often support this methodology. The methodology provides structure for the identification of automated solutions, system design and implementation, documentation requirements, testing, approvals, project management and oversight requirements, and project risk assessments.

Application maintenance addresses ongoing change management and the implementation of new releases of software. Appropriate controls over changes to the system should exist to help ensure that they are made properly. There is also a need to determine the extent of testing required for the new release of a system. For example, the implementation of a major new software release may require the evaluation of the enhancements to the system, extensive testing, user retraining and the rewriting of procedures. Controls may involve required authorization of change requests, review of the changes, approvals, documentation, testing and assessment of changes on other IT components and implementation protocols. The change management process also needs to be integrated with other IT processes, including incident management, problem management, availability management and infrastructure change control.

Relationship Between IT General Controls and Application Controls

As the IT organization becomes more focused on being aligned with the business, IT general controls and application controls are becoming more integrated. Traditionally, IT general controls were needed to ensure the function of application controls that depend on computer processes. While this continues to be true, IT general controls increasingly supplement application and business process controls. A number of application and business process control objectives, such as, system availability, may be achieved only through the operation of IT general controls.

The relationship between application controls and IT general controls is such that IT general controls are needed to support the functioning of application controls, and both are needed to ensure complete and accurate information processing.

IT general controls and IT application controls are becoming more important as the timing of error detection and the cost-efficiency of controls receive more attention. For example, in 1995, it may have been acceptable to wait several weeks for a manual reconciliation to detect an error. However, in 2004, in the world of 24/7 processing, this is increasingly not acceptable. An error may need to be detected within five minutes or less; therefore, the manual control can no longer be the key control.

When management realizes the cost of compliance with the Sarbanes-Oxley Act, there will be an increasing focus on automated controls. Why document and test a daily manual control for 30 to 50 occurrences when an automated control, supported by adequate security controls and program change controls, may need to be tested only several times? An increased focus on control efficiency is expected in 2005.

Compliance and IT Governance

There is no such thing as a risk-free environment, and compliance with the Sarbanes-Oxley Act does not create such an environment. However, the process that most organizations will follow to enhance their system of internal control to conform to the Sarbanes-Oxley Act is likely to provide lasting benefits. Good IT governance over planning and life cycle control objectives helps ensure more accurate and timely financial reporting.

The work required to meet the requirements of the Sarbanes-Oxley Act should not be regarded as a compliance process, but rather as an opportunity to establish strong governance models designed to ensure accountability and responsiveness to business requirements. Building a strong internal control program within IT can help to:

- Enhance overall IT governance
- Enhance the understanding of IT among executives
- Make better business decisions with higher-quality, more timely information

- Align project initiatives with business requirements
- Prevent loss of intellectual assets and the possibility of system breach
- Contribute to the compliance of other regulatory requirements, such as privacy
- Gain competitive advantage through more efficient and effective operations
- Optimize operations with an integrated approach to security, availability and processing integrity
- Enhance risk management competencies and prioritization of initiatives

Multilocation Considerations

Among the many factors that must be considered in complying with the Sarbanes-Oxley Act, some will uniquely impact multilocation organizations. For example, global organizations or non-US-based companies that are required to comply with the Sarbanes-Oxley Act need to examine their IT operations and determine if they are significant to the organization as a whole.

Significant business units can include financial business units or IT business units. The assessment of whether an IT business unit is significant can be impacted by the materiality of transactions processed by the IT business unit, the potential impact on financial reporting if an IT business unit fails and other qualitative risk factors. The issue is that there are financial materiality and significant risk considerations, quantitative and qualitative, and both aspects provide focus.

Examples of multilocation assessment considerations include:

- Where the financial business units within a territory are not significant individually, but if IT processing occurs in a central location, then the IT business unit may be significant, e.g., a US multinational's British financial business units that are not individually significant (although they would be significant on a consolidated basis) and most financial reporting IT processing performed by a single IT business unit
- Where the financial business unit is not significant in a particular territory, but the local IT business unit is responsible for regional IT processing, e.g., an IT business unit in Singapore that is responsible for IT processing throughout Asia-Pacific
- Where there is no financial business unit in a particular territory, but US-based IT responsibilities have been outsourced to that territory, e.g., a US insurance company that outsources IT processing and maintenance to an IT business unit based in India

Setting the Ground Rules

Until recently, assertions on control by an organization were mostly voluntary and based on a wide variety of internal control frameworks. As mentioned previously, to improve consistency and quality, the SEC mandated the use of a recognized internal control framework established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment, and made specific reference to COSO.[1]

COSO Defined

COSO is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal control and corporate governance. It was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector organization often referred to as the Treadway Commission. The sponsoring organizations include the American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), Financial Executives International (FEI), Institute of Internal Auditors (IIA) and Institute of Management Accountants (IMA). The sections that follow provide further insight into COSO as well as its implications for IT.

Adopting a Control Framework

For years, IT has played an important role in the operation of strategic and managerial information systems. Today, these systems are inseparable from an organization's ability to meet the demands of customers, suppliers and other important stakeholders. With widespread reliance on IT for financial and operational management systems, controls have long been recognized as necessary, particularly for significant information systems. PCAOB Auditing Standard No. 2 states that:

> *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 proposed 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.*

It will be important to demonstrate how IT controls support the COSO framework. An organization should have IT control competency in all COSO components. COSO identifies five essential components of effective internal control. They are:

- Control environment
- Risk assessment

[1] *www.coso.org*

- Control activities
- Information and communication
- Monitoring

Each of the five is described briefly in the following sections. Following that description are high-level IT considerations as they relate to each specific component. More detailed IT control objectives are included at the end of this document to provide considerations for compliance with the Sarbanes-Oxley Act.

Control Environment

Control environment creates the foundation for effective internal control, establishes the "tone at the top" and represents the apex of the corporate governance structure. The issues raised in the control environment component apply throughout an organization. The control environment primarily addresses the company level.

However, IT frequently has characteristics that may require additional emphasis on business alignment, roles and responsibilities, policies and procedures, and technical competence. The following list describes some considerations related to the control environment and IT:

- IT is often mistakenly regarded as a separate organization of the business and thus a separate control environment.
- IT is complex, not only with regard to its technical components but also as to how those components integrate into the organization's overall system of internal control.
- IT can introduce additional or increased risks that require new or enhanced control activities to mitigate successfully.
- IT requires specialized skills that may be in short supply.
- IT may require reliance on third parties where significant processes or IT components are outsourced.
- Ownership of IT controls may be unclear, especially for application controls.

Risk Assessment

Risk assessment involves the identification and analysis by management of relevant risks to achieve predetermined objectives, which form the basis for determining control activities. It is likely that internal control risks could be more pervasive in the IT organization than in other areas of the organization. Risk assessment may occur at the company level (for the overall organization) or at the activity level (for a specific process or business unit).

At the company level, the following may be expected:

- An IT planning subcommittee of the company's overall Sarbanes-Oxley steering committee. Among its responsibilities may be the following:

- – Oversight of the development of the IT internal control strategic plan, its effective and timely execution/implementation, and its integration with the overall Sarbanes-Oxley compliance plan
- – Assessment of IT risks, e.g., IT management, data security, program change and development

At the activity level, the following may be expected:

- Formal risk assessments built throughout the systems development methodology
- Risk assessments built into the infrastructure operation and change process
- Risk assessments built into the program change process

Control Activities

Control activities are the policies, procedures and practices that are put into place to ensure that business objectives are achieved and risk mitigation strategies are carried out. Control activities are developed to specifically address each control objective to mitigate the risks identified.

Without reliable information systems and effective IT control activities, public companies would not be able to generate accurate financial reports. COSO recognizes this relationship and identifies two broad groupings of information system control activities: general controls and application controls.

General controls, which are designed to ensure that the financial information generated from an organization's application systems can be relied upon, include the following types:

- Data center operation controls—Controls such as job setup and scheduling, operator actions, and data backup and recovery procedures
- System software controls—Controls over the effective acquisition, implementation and maintenance of system software, database management, telecommunications software, security software and utilities
- Access security controls—Controls that prevent inappropriate and unauthorized use of the system
- Application system development and maintenance controls—Controls over development methodology, including system design and implementation, that outline specific phases, documentation requirements, change management, approvals and checkpoints to control the development or maintenance of the project

Application controls are embedded within software programs to prevent or detect unauthorized transactions. When combined with other controls, as necessary, application controls ensure the completeness, accuracy, authorization and validity of processing transactions. Some examples of application controls include:

- Balancing control activities—Detect data entry errors by reconciling amounts captured either manually or automatically to a control total. For example, a company automatically balances the total number of transactions processed and passed from its online order entry system to the number of transactions received in its billing system.
- Check digits—Calculate to validate data. A company's part numbers contain a check digit to detect and correct inaccurate ordering from its suppliers. Universal product codes include a check digit to verify the product and the vendor.
- Predefined data listings—Provide the user with predefined lists of acceptable data. For example, a company's intranet site might include drop-down lists of products available for purchase.
- Data reasonableness tests—Compare data captured to a present or learned pattern of reasonableness. For example, an order to a supplier by a home renovation retail store for an unusually large number of board feet of lumber may trigger a review.
- Logic tests—Include the use of range limits or value/alphanumeric tests. For example, credit card numbers have a predefined format.

General controls are needed to support the functioning of application controls, and both are needed to help ensure accurate information processing and the integrity of the resulting information used to manage, govern and report on the organization. As automated application controls increasingly replace manual controls, general controls are becoming more important.

Information and Communication

COSO states that information is needed at all levels of an organization to run the business and achieve the entity's control objectives. However, the identification, management and communication of relevant information represent an ever-increasing challenge to the IT department. The determination of which information is required to achieve control objectives, and the communication of this information in a form and time frame that allow people to carry out their duties, support the other four components of the COSO framework.

The IT organization processes most financial reporting information. However, its scope is usually much broader. The IT department may also assist in implementing mechanisms to identify and communicate significant events, such as e-mail systems or executive decision support systems.

COSO also notes that the quality of information includes ascertaining whether the information is:

- Appropriate—Is it the right information?
- Timely—Is it available when required and reported in the right period of time?

- Current—Is it the latest available?
- Accurate—Are the data correct?
- Accessible—Can authorized individuals gain access to it as necessary?

At the company level, the following may be expected:

- Development and communication of corporate policies
- Development and communication of reporting requirements, including deadlines, reconciliations, and the format and content of monthly, quarterly and annual management reports
- Consolidation and communication of financial information

At the activity level, the following may be expected:

- Development and communication of standards to achieve corporate policy objectives
- Identification and timely communication of information to assist in achieving business objectives
- Identification and timely reporting of security violations

Monitoring

Monitoring, which covers the oversight of internal control by management through continuous and point-in-time assessment processes, is becoming increasingly important to IT management. There are two types of monitoring activities: continuous monitoring and separate evaluations.

IT performance and effectiveness are increasingly monitored using performance measures that indicate if an underlying control is operating effectively. Consider the following examples:

- Defect identification and management—Establishing metrics and analyzing the trends of actual results against metrics can provide a basis for understanding the underlying reasons for processing failures. Correcting these causes can improve system accuracy, completeness of processing and system availability.
- Security monitoring—Building an effective IT security infrastructure reduces the risk of unauthorized access. Improving security can reduce the risk of processing unauthorized transactions and generating inaccurate reports, and can ensure a reduction of the unavailability of key systems if applications and IT infrastructure components have been compromised.

An IT organization also has many different types of separate evaluations, including:

- Internal audits
- External audits
- Regulatory examinations
- Attack and penetration studies
- Independent performance and capacity analyses
- IT effectiveness reviews

- Control self-assessments
- Independent security reviews
- Project implementation reviews

At the company level, the following may be expected:

- Centralized continuous monitoring of computer operations
- Centralized monitoring of security
- IT internal audit reviews (While the audit may occur at the activity level, the reporting of audit results to the audit committee is at the company level.)

At the activity level, the following may be expected:

- Defect identification and management
- Local monitoring of computer operations or security
- Supervision of local IT personnel

Assessing the Readiness of IT

The Sarbanes-Oxley Act now requires all qualifying SEC-registered organizations to document, evaluate, monitor and report on internal control over financial reporting and disclosure controls and procedures, which include IT controls. The first step in this process is to assess the overall IT organization's Sarbanes-Oxley financial reporting controls readiness by considering the questions illustrated in **figure 4**. (For guidance on the assessment of the IT control environment, refer to the company-level questionnaire in appendix B.)

Figure 4—Sarbanes-Oxley IT Diagnostic Questions

1. Does the Sarbanes-Oxley steering committee understand the risks inherent in IT systems and their impact on compliance with section 404?
2. Have business process owners defined their requirements for financial reporting control?
3. Has IT management implemented suitable IT controls to meet these business requirements?
4. Does the CIO have an advanced knowledge of the types of IT controls necessary to support reliable financial processing?
5. Are policies governing security, availability and processing integrity established, documented and communicated to all members of the IT organization?
6. Are the roles and responsibilities for all those involved in processing financial IT systems related to section 404 documented and understood by all members of the department?
7. Do members of the IT department and all those involved in processing financial IT systems understand their roles, do they possess the requisite skills to perform their job responsibilities relating to internal control, and are they supported with appropriate skill development?
8. Is the IT department's risk assessment process integrated with the company's overall risk assessment process for financial reporting?
9. Does the IT department document, evaluate and remediate IT controls related to financial reporting on an annual basis?
10. Does the IT department have a formal process in place to identify and respond to IT control deficiencies?
11. Is the effectiveness of IT controls monitored and followed up on a regular basis?

The responses to these questions will help determine: (1) if the IT department and all those involved in processing financial IT systems are integrated with the overall Sarbanes-Oxley section 404 implementation plan, (2) if the IT department has documented and evaluated IT controls and (3) if executive management—including the CIO—appreciates the impact that the IT department has on Sarbanes-Oxley section 404 compliance.

Establishing IT Control Guidelines for Sarbanes-Oxley

While the importance of IT controls is embedded in the COSO internal control framework, IT management requires more examples to help identify, document and evaluate IT controls.

Several IT internal control frameworks exist. However, the IT control objectives known as COBIT are considered particularly useful and are an open framework, which aligns with the spirit of the Sarbanes-Oxley Act requirement that any framework used be open and generally acceptable. COBIT is an IT governance model that provides both company-level and activity-level objectives along with associated controls. Using the COBIT framework, an organization can design a system of IT controls to comply with section 404.

While COBIT provides controls that address operational and compliance objectives, those related more directly to financial reporting were used to develop this document. Consideration was also given to other IT control guidelines, including ISO17799 and the Information Technology Infrastructure Library (ITIL).

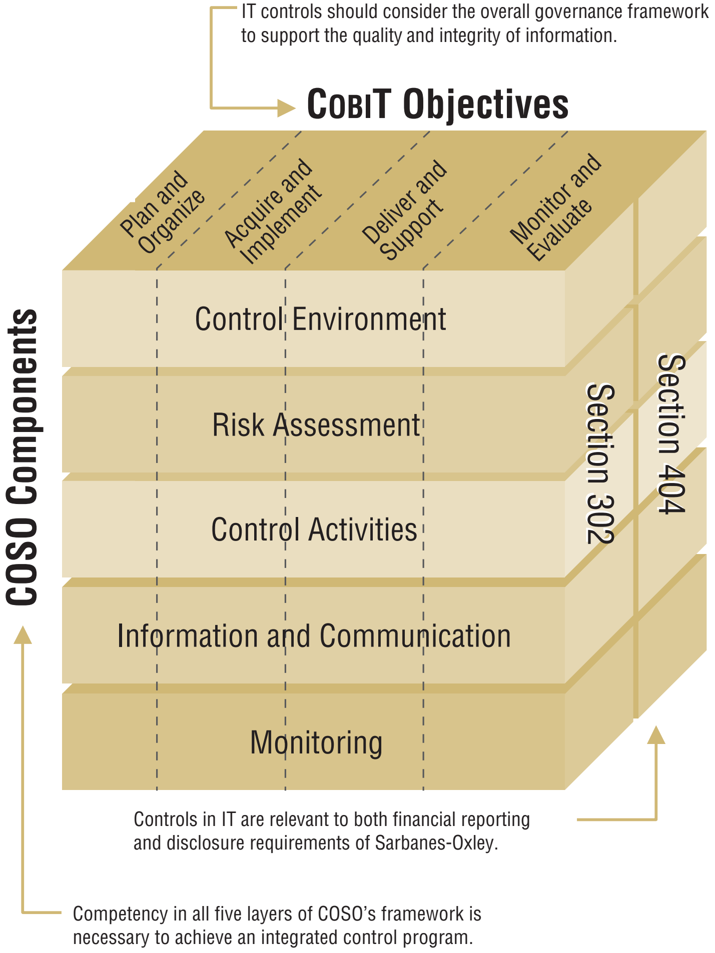
Note: Each organization should carefully consider the appropriate IT control objectives for its own circumstances. The organization may not include all control objectives discussed in this document, or may include others not discussed in this document.

Accordingly, each organization should tailor an IT control approach suitable to its size and complexity. In doing so, it is expected that changes will be made to the controls included in this document to reflect the specific circumstances of each organization. This document should not be a basis for audit reliance, and as such, it is advisable that organizations discuss with their external auditors to obtain their perspective on IT control objectives that should be addressed.

In the development of this IT control template, each control objective was challenged to ensure its relevance and importance to the requirements of the Sarbanes-Oxley Act. This process of evaluation resulted in some COBIT control objectives being excluded or combined into a single objective for applicability to financial reporting purposes. Furthermore, each IT control objective has been reconciled to COSO to support alignment with an organization's overall Sarbanes-Oxley program. (See appendix A—IT Control Objectives for Sarbanes-Oxley.)

While COSO identifies five components of internal control, illustrated in **figure 5**, that need to be in place and integrated to achieve financial reporting and disclosure objectives, COBIT provides similar detailed guidance for IT. The five components of COSO—beginning with identifying the control environment and culminating in the monitoring of internal controls—can be visualized as the horizontal layers of a three-dimensional cube, with the COBIT objective domains—from Plan and Organize through Monitor and Evaluate—applying to each individually and in aggregate.

Figure 5—Internal Control Components


IT controls should consider the overall governance framework to support the quality and integrity of information.
COBIT Objectives
Plan and Organize
Acquire and Implement
Deliver and Support
Monitor and Evaluate
COSO Components
Control Environment
Risk Assessment
Control Activities
Information and Communication
Monitoring
Section 302
Section 404
Controls in IT are relevant to both financial reporting and disclosure requirements of Sarbanes-Oxley.
Competency in all five layers of COSO's framework is necessary to achieve an integrated control program.

Closing the Gap

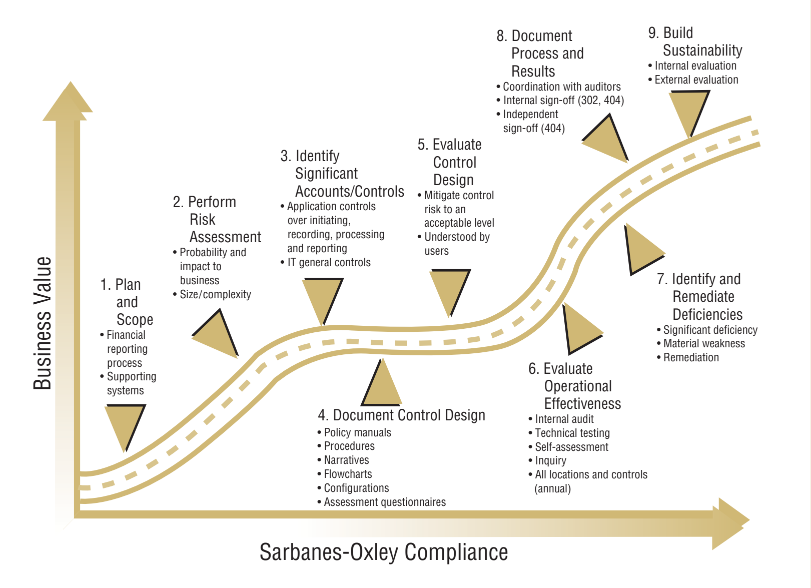
The following section provides a compliance road map that is tailored to the specific objectives and responsibilities of IT departments.

Road Map for Compliance

Understanding how Sarbanes-Oxley applies to an organization—based on its business characteristics—can aid in the development of the internal control program. Many factors come into play, and larger companies will face challenges distinct from those of smaller enterprises. Also, the extent to which a strong internal control framework is already in place will have significant bearing on activities.

The compliance road map, illustrated in **figure 6**, provides direction for IT professionals on meeting the challenges of the Sarbanes-Oxley Act. Compliance with the Act from an IT controls standpoint is not a stand-alone process. It must be integrated within the overall business-led compliance process. Since IT general controls require technical knowledge, they are usually the responsibility of the IT service provider to define and implement. However, even these should be based on business (financial reporting) requirements, signed off by the business, and not left to the IT provider. This is especially true when IT is outsourced. For IT application controls, the business, not IT, should define the control requirements, especially for financial systems that are often complex in nature from a business process perspective.

Figure 6—Compliance Road Map



1. Plan and Scope
• Financial reporting process
• Supporting systems
2. Perform Risk Assessment
• Probability and impact to business
• Size/complexity
3. Identify Significant Accounts/Controls
• Application controls over initiating, recording, processing and reporting
• IT general controls
4. Document Control Design
• Policy manuals
• Procedures
• Narratives
• Flowcharts
• Configurations
• Assessment questionnaires
5. Evaluate Control Design
• Mitigate control risk to an acceptable level
• Understood by users
6. Evaluate Operational Effectiveness
• Internal audit
• Technical testing
• Self-assessment
• Inquiry
• All locations and controls (annual)
7. Identify and Remediate Deficiencies
• Significant deficiency
• Material weakness
• Remediation
8. Document Process and Results
• Coordination with auditors
• Internal sign-off (302, 404)
• Independent sign-off (404)
9. Build Sustainability
• Internal evaluation
• External evaluation
Business Value
Sarbanes-Oxley Compliance

Plan and Scope

Scoping the project is one of the most important activities in the entire program. While it is true that general controls cut across geographic regions and business processes, not all IT processes are relevant.

In this project initiating phase, organizations should form an IT control subcommittee that is integrated into, and reports to, the overall Sarbanes-Oxley steering committee. Smaller organizations may be able to redeploy, on a part-time basis, existing staff; however, larger organizations may need dedicated full-time personnel.

As a critical first step, organizations must understand how the financial reporting process works and identify where technology is critical in the support of this process. This will identify key systems and subsystems that need to be included in the scope of the project. Typically, systems will be considered in scope if they participate in the initiation, recording, processing and reporting of financial information.

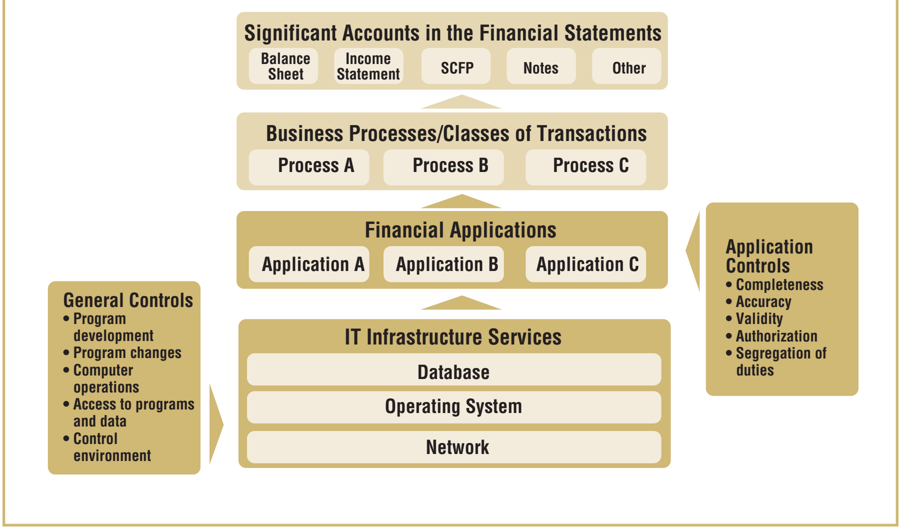
In considering which controls to include in the program, organizations should recognize that IT controls may have a direct or indirect impact on the financial reporting process. For example, IT application controls that ensure completeness of transactions can be directly related to financial assertions. However, access controls that exist within these applications or within their supporting systems, such as databases, networks and operating systems, are equally important, but do not directly align to a financial assertion. Consider the diagram in **figure 7** as a tool for scoping the IT control portion of the program. (Note: In **figure 7**, SCFP stands for statement of change in financial position.)

This diagram is particularly useful as it focuses the attention on the significant accounts involved in the financial reporting process. The IT systems involved in the financial reporting process are depicted within the bottom half of **figure 7**. As can be seen, application controls are generally aligned with a business process that, in turn, gives rise to financial reports. While there may be many IT systems operating within an organization, only those that are associated with a significant account or related business process need to be considered for compliance purposes.

The scope of the program generally includes the following processes and controls:

- Controls over initiating, recording, processing and reporting significant accounts and disclosures and related assertions embodied in the financial statements
- Controls over the selection and application of accounting policies that are in conformity with generally accepted accounting principles
- Antifraud programs and controls

Figure 7—IT Controls



- Controls, including IT general controls, on which other controls are dependent
- Controls over significant nonroutine and nonsystematic transactions, such as accounts involving judgments and estimates
- Controls over the period-end financial reporting process, including controls over procedures used to enter transaction totals into the general ledger; to initiate, record and process journal entries in the general ledger; and to record recurring and nonrecurring adjustments to the financial statements (e.g., consolidating adjustments, report combinations and reclassifications)

Factors that should be considered when determining whether systems need to be reviewed and tested as part of a Sarbanes-Oxley compliance program include whether they process large volumes of transactions, process large dollar-value items, are used to process complex transactions or support highly sensitive financial data repositories.

The location of IT systems also needs to be considered when performing the planning and scoping process. Although a location or business unit may not be significant from a financial standpoint, it may still be an important location. For example, a business unit could be responsible for critical online processing and, from an IT perspective, dependent on local systems for continuous operation. The nature of these operations could have a material impact on the organization and potentially expose it to a risk of material misstatement even though the relative financial significance is not material. In such an event, consideration of IT controls at this location would be appropriate.

When determining which locations or business units to include in the scope of the Sarbanes-Oxley program, organizations should consider the following:
- The extent of dependence on IT at the various locations or business units
- The degree of consistency in processes and procedures with other locations or business units. Where processes and procedures are unique, organizations may need to consider these locations separately and ensure that overall control objectives are met.
- The organization's assessment of risk related to the location or business unit

Perform Risk Assessment

In the planning and scoping phase of the overall Sarbanes-Oxley project, organizations should have determined the IT locations, systems and applications that are being relied upon to provide accurate financial information.

The next step in the road map is to perform risk assessments on the selected components. Risk assessment enables organizations to understand how events can inhibit the achievement of business objectives. The purpose of the risk assessment is to help determine the inherent and residual risks to establish the level of documentation and the extent of testing that needs to be performed.

Risk assessment requires two perspectives: impact and probability. Impact reflects the effect of events, while probability or likelihood reflects the potential for events to occur.

Some of the factors to be included when considering impact would be:
- Security failure on the reporting of financial information
- Implementation of an unapproved change
- Lack of availability of the system/application
- Failure to maintain the system/application
- Failure in the integrity (calculation accuracy, completeness, etc.) of information managed by the system/application

Some of the factors to be included when considering probability would be:
- Volume of transactions running through the system/application
- Complexity of the technology and the application
- Volume and complexity of changes made
- Age of the system/application
- Past history of issues related to the system/application
- Custom in-house programming vs. off-the-shelf packages

In performing the IT risk assessments, many companies utilize risk rating criteria to assign a risk level to the different IT locations, systems and applications. Some companies use a structured numbering scorecard based upon mathematical calculations while other companies use a summarized categorization of high, medium or low. The assignment of risks usually has a subjective component.

It is anticipated that the level of risk would have an impact on the extent and nature of expected controls as well as the type and extent of testing. For example, it would be anticipated that the higher risk areas would require more extensive testing to validate that adequate controls are in place.

Consideration must also be given to the relative financial and operational significance of various IT processing locations or business units. In some cases, the outsourcing or centralization of general IT controls may be significant to the business. In this way, compliance teams should understand the probability and impact of failures at each significant location and their potential impact to the overall organization.

Identify Significant Accounts/Controls

COSO identifies two broad groupings of information system control activities:

- Application controls, which apply to the business processes they support and are designed within the application to prevent/detect unauthorized transactions. When combined with manual controls, as necessary, application controls are used to help ensure completeness, accuracy, authorization and validity of processing transactions.
- General controls, which apply to all information systems, support secure and continuous operation

For application controls, organizations should first identify significant accounts that could have a material impact on the financial reporting and disclosure process. Once the significant accounts have been identified, application controls relevant to such accounts should be identified and documented.

For general controls, organizations should assess those controls that support the quality and integrity of information and that are designed to mitigate the identified risks.

Appendix C provides details of the specific control objectives that should be considered for both general and application controls. A detailed company-level questionnaire is also presented in appendix B. Since company-level controls are primarily related to the control environment and risk assessment components of COSO, and their existence sets the tone for the effectiveness of all other controls, assessing company-level controls is a key objective for this phase. The questionnaire includes such elements as:

- “Tone at the top”

- Integrity, ethical values and competence
- IT management's philosophy and operating style
- Delegation of authority and responsibility for IT management
- IT policies and procedures
- The quality and skill of people involved with the organization
- The direction provided by senior management

Document Control Design

Documentation is a unique aspect to the Sarbanes-Oxley compliance process that will likely pose a significant challenge for organizations. While most companies have controls in place, few have documentation to provide sufficient evidence of their design and operation. The PCAOB has noted that:

> *…The more clearly management documents its internal control over financial reporting, the process used to assess the effectiveness of the internal control, and the results of that process, the easier it will be for the auditor to understand the internal control, confirm that understanding, evaluate management's assessment, and plan and perform the audit of internal control over financial reporting.*

While PCAOB Auditing Standard No. 2 does not specifically define management's documentation requirements, it does suggest that the auditor should evaluate whether such documentation includes the following:

> - *The design of controls over all relevant assertions related to all significant accounts and disclosures in the financial statements. The documentation should include the five components of internal control over financial reporting…including the control environment and company-level controls.* (ITGI note: Many organizations' documentation addresses only the control activities component.)
> - *Information about how significant transactions are initiated, authorized, recorded, processed and reported*
> - *Sufficient information about the flow of transactions to identify the points at which material misstatements due to error or fraud could occur*
> - *Controls designed to prevent or detect fraud, including who performs the controls and the related segregation of duties*
> - *Controls over the period-end financial reporting process*
> - *Controls over safeguarding of assets*
> - *The results of management's testing and evaluation*
>
> *Documentation might take many forms, such as paper, electronic files, or other media, and can include a variety of information, including policy manuals, process models, flowcharts, job descriptions, documents, and forms. The form and extent of documentation will vary depending on the size, nature, and complexity of the company.*

> *Inadequate documentation of the design of controls over relevant assertions related to significant accounts and disclosures is a deficiency in the company's internal control over financial reporting.*

It is suggested that management discuss the proposed extent and detail of the control documentation with the external auditors early in the process to reduce the risk that the external auditor will consider the control documentation deficient.

Understanding control theory and the concepts that define IT control design will be an important competency of IT organizations in the future. Put simply, IT control design defines the approach an organization follows to reduce IT risk—the risk that IT prevents the business from achieving its objectives—to an acceptable level. Once the control is properly designed, its implementation and continued effectiveness become the focus. The existence of controls and their effectiveness are discussed in subsequent phases.

Equally important in this phase is the documentation that supports an organization's control program. Documentation should be prepared—both at the entity level as well as the activity level—regarding the objectives that the controls are designed to achieve to support the organization's internal control over financial reporting and disclosure controls and procedures. It is advisable that an organization document its approach to IT control, including the assignment of authority and responsibility for IT controls as well as their design and operation.

Evaluate Control Design

In this phase, an IT organization must step back and evaluate the ability of its control program to reduce IT risk to an acceptable level. More specifically, it requires that control attributes, including preventive, detective, automated and manual, be considered when designing an approach to effectively address risks. For example, if a change management risk is identified that would result in unauthorized programs being migrated into the production environment, a properly designed control would prevent this from occurring. In this example, a detective control that identifies unauthorized programs in production after the fact may not be appropriate.

The importance of control design in the overall IT control environment cannot be understated. PCAOB Auditing Standard No. 2 points out the importance of IT controls and reinforces the fact that such controls are necessary to support the overall internal control environment. In particular, it states that the effectiveness of a company's overall system of internal control is dependent on, "The effectiveness of other controls (for example, the control environment or information technology general controls)."

Accordingly, to help in this process of evaluating control design, consider the IT control design and effectiveness model in **figure 8**. Depending on how the organization measures up, it may be necessary to spend some time enhancing the design and effectiveness of the control program.

Figure 8—Stages of Control Reliability

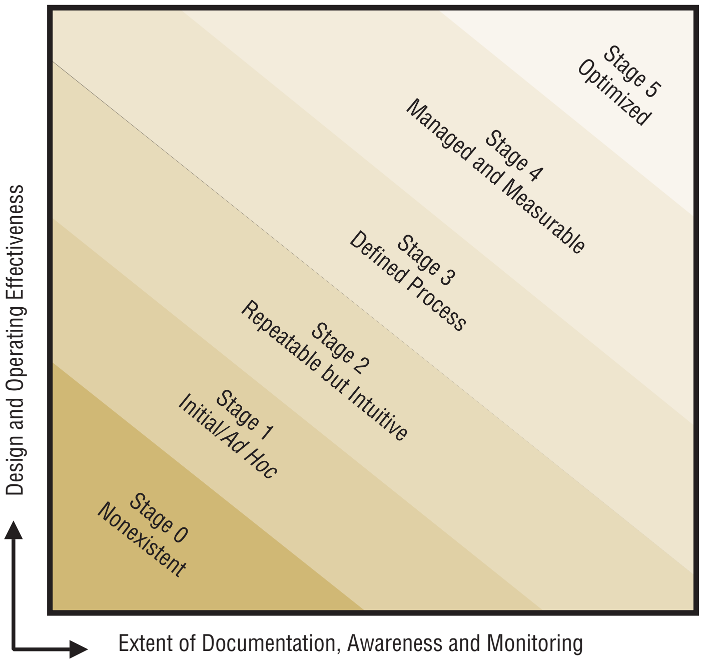


Figure 8 demonstrates the stages of control reliability that may exist within organizations. For the purposes of establishing internal control, some organizations may be willing to accept IT controls that fall somewhere short of stage 3. However, given the Sarbanes-Oxley Act's requirements for independent attestation of controls by external audit, controls will more than likely require the attributes and characteristics of stage 3 or higher for key control activities.

The table presented in **figure 9** provides insight into the various characteristics of each stage as well as the related implications. IT organizations must realize that there is little definition or guidance regarding the attributes or characteristics necessary to comply with the Sarbanes-Oxley Act. The SEC has indicated that no particular form of documentation is approved or required, and the extent of documentation may vary, depending upon the size and complexity of the organization.

Figure 9—Control Quality

	Stage 0—Nonexistent	Stage 1—Initial/*Ad Hoc*	Stage 2—Repeatable but Intuitive	Stage 3—Defined Process	Stage 4—Managed and Measurable	Stage 5—Optimized
Characteristics	At this level, there is a complete lack of any recognizable control process or the existence of any related procedures. The organization has not even acknowledged there is an issue to be addressed; therefore, no communication about the issue is generated.	There is some evidence the organization recognizes that controls and related procedures are important and need to be addressed. However, controls and related policies and procedures are not in place and documented. An event and disclosure process does not exist. Employees are not aware of their responsibility for control activities. The operating effectiveness of control activities is not evaluated on a regular basis. Control deficiencies are not identified.	Controls and related policies and procedures are in place but not always fully documented. An event and disclosure process is in place but not documented. Employees may not be aware of their responsibility for control activities. The operating effectiveness of control activities is not adequately evaluated on a regular basis and the process is not documented. Control deficiencies may be identified but are not remedied in a timely manner.	Controls and related policies and procedures are in place and adequately documented. An event and disclosure process is in place and adequately documented. Employees are aware of their responsibility for control activities. The operating effectiveness of control activities is evaluated on a periodic basis (e.g., quarterly); however, the process is not fully documented. Control deficiencies are identified and remedied in a timely manner.	Controls and related policies and procedures are in place and adequately documented, and employees are aware of their responsibility for control activities. An event and disclosure process is in place, adequately documented and monitored, but not always reevaluated to reflect major process or organizational changes. The operating effectiveness of control activities is evaluated on a periodic basis (e.g., weekly), and the process is adequately documented. There is limited, primarily tactical, use of technology to document processes, control objectives and activities.	Stage 5 meets all of the characteristics of stage 4. An enterprisewide control and risk management program exists such that controls and procedures are well documented and continuously reevaluated to reflect major process or organizational changes. A self-assessment process is used to evaluate the design and effectiveness of controls. Technology is leveraged to its fullest extent to document processes, control objectives and activities, identify gaps, and evaluate the effectiveness of controls.
Implications	The organization has a total inability to be in compliance at even the minimum level.	Insufficient controls, policies, procedures and documentation exist to even support management's assertion. The level of effort to document, test and remedy controls is very significant.	Although controls, policies and procedures are in place, insufficient documentation exists to support management's certification and assertion. The level of effort to document, test and remedy controls is significant.	Sufficient documentation exists to support management's certification and assertion. The level of effort to document, test and remedy controls may be significant depending on the organization's circumstances.	Sufficient documentation exists to support management's certification and assertion. The level of effort to document, test and remedy controls may be less significant depending on the organization's circumstances.	Implications of stage 4 remain. Improved decision-making is enabled because of high-quality, timely information. Internal resources are used effectively and efficiently. Information is timely and reliable.

Evaluate Operational Effectiveness

Once control design has been assessed, as appropriate, its implementation and continuing effectiveness must be confirmed. During this stage, initial and ongoing tests—conducted by individuals responsible for the controls and the internal control program management team—should be performed to check on the operating effectiveness of the control activities.

Ordinarily, organizations should test controls upon which other significant controls depend more extensively (e.g., general controls as opposed to application controls) and with higher frequency. In making a judgment about the extent of testing that is appropriate, organizations should consider how the IT control impacts financial and disclosure reporting processes.

Some organizations use external service organizations to perform outsourced services. These services are still part of an organization's overall operations and responsibility and, consequently, need to be considered in the overall IT internal control program.

PCAOB Auditing Standard No. 2 specifically addresses the service auditor's reports. It states:

> *The use of a service organization does not reduce management's responsibility to maintain effective internal control over financial reporting. Rather, management should evaluate controls at the service organization, as well as related controls at the company, when making its assessment about internal control over financial reporting.*

In such circumstances, organizations should review the activities of the service organization in arriving at a conclusion on the reliability of its internal control. Documentation of service organization control activities will be required for the attestation activities of the independent auditor, so an assessment is required of the service organization to determine the sufficiency and appropriateness of evidence supporting these controls.

Traditionally, audit opinions commonly known as SAS 70 reports (Section 5900 in Canada) have been performed for service organizations. If these audit reports do not include tests of controls, results of the tests and the service auditor's opinion on operating effectiveness, they may not be deemed sufficient for purposes of Sarbanes-Oxley compliance. In such cases, organizations may wish to consult with their external auditors and understand the specific requirements. Particular attention should be paid to the period covered by the SAS 70 and ensuring that the controls in the SAS 70 cover the environment, platforms and applications utilized by the company.

In evaluating whether such a service auditor's report provides sufficient evidence, management and the auditor should consider the following factors:

- The time period covered by the tests of controls and its relation to the date of management's assessment
- The scope of the examination and applications covered, the controls tested, and the way in which tested controls relate to the company's controls
- The results of those tests of controls and the service auditor's opinion on the operating effectiveness of the controls

In addition:

- Management should make inquiries concerning the service auditor's reputation, competence and independence.
- When a significant period of time has elapsed between the time period covered by the tests of controls in the service auditor's report and the date of management's assessment, additional procedures should be performed.

Identify and Remediate Deficiencies

Deficiencies in an entity's internal control range from inconsequential shortcomings to significant deficiencies to material weaknesses (see sidebar, What Is the Difference Between a Deficiency and a Material Weakness?). Determining whether a deficiency is significant or material requires professional judgment and the consideration of various factors.

In making the judgment as to which IT control deficiencies are significant, independent auditors consider various factors, such as the size of operations, complexity and diversity of activities, organizational structure and the likelihood that the IT control deficiency could result in a misstatement of the organization's financial records. In particular, application controls that are directly supportive of financial assertions (existence, completeness, valuation) are more likely to result in material weaknesses.

To prepare, IT organizations should engage individuals with experience performing IT control

What Is the Difference Between a Deficiency and a Material Weakness?

An ***internal control deficiency*** may consist of a design or operating deficiency. A design deficiency exists when a necessary control is missing or an existing control is not properly designed, so that even when the control is operating as designed the control objective is not always met. An operating deficiency exists when a properly designed control either is not operating as designed or the person performing a control does not possess the necessary authority or qualifications to perform the control effectively. Internal control deficiencies relevant to internal control over financial reporting could adversely affect the entity's ability to initiate, record, process and report financial data consistent with the assertions of management in the financial statements.

A ***significant deficiency*** is an internal control deficiency in a significant control or an aggregation of such deficiencies that could result in a misstatement of the financial statements that is more than inconsequential.

A ***material weakness*** is a significant deficiency or an aggregation of significant deficiencies that preclude the entity's internal control from providing reasonable assurance that material misstatements in the financial statements will be prevented or detected on a timely basis by employees in the normal course of performing their assigned functions. The inability to provide such reasonable assurance results from one or more significant deficiencies. The design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements caused by errors or fraud in amounts that would be material in relation to the financial statements may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. Therefore, the existence of a material weakness precludes the responsible party from concluding that internal control is effective and the practitioner from issuing an unqualified opinion that internal control is effective.

Note that management is not permitted to conclude that the company's internal control over financial reporting is effective, if there are one or more material weaknesses in the company's internal control over financial reporting.

audits to identify the weaknesses in IT internal control programs. Once a reliable control state has been reached, a sustainability model should be implemented to ensure operating effectiveness over time.

Document Process and Results

During the evaluation phase, results of tests performed should be recorded, as they will form the basis for management assertion and auditor attestation. Again, there is no prescribed format; the goal is to provide a comprehensive, easily understood summary of control effectiveness that is inclusive of all testing activities performed. This documentation should culminate in a management report that can be shared with senior executives and demonstrates the overall reliability, quality and integrity of IT systems. The documentation should also provide a summary of the activities and procedures performed, including significant judgments and decisions made, to demonstrate the process management followed to arrive at its controls. Doing so will help facilitate the CEO's and CFO's enterprisewide certifications of control.

Build Sustainability

The final phase ensures that internal controls are sustainable. At this point, IT management should be in a position to sign off on the IT internal control program effectiveness. Control assessment and management competencies must become part of the IT department's organization and culture and must sustain themselves over the long term. Control is not an event; it is a process that requires continuous support and evaluation to stay current.

How Compliance Should Be Documented

To date, most organizations have struggled with the question of how much documentation is necessary to support their internal control program, and in what form it should be retained. In responding to this query, it is important to consider the communications from the SEC as well as those that will likely guide independent auditors in their certification efforts.

Documentation may take various forms, including entity policy manuals, IT policy and procedures, narratives, flowcharts, decision tables, procedural write-ups or completed questionnaires. No single particular form of documentation is mandated and the extent of documentation may vary, depending upon the size and complexity of the organization.

For most organizations, documentation should be, at a minimum, prepared for the following:

- Company level
  - Statement of control and approach to confirming the controls existence and continued effectiveness over time

- Activity level
  - Description of the processes and related subprocesses (It may be in narrative form; however, it may be more effective to illustrate as a flowchart.)
  - Description of the risk associated with the process or subprocess, including an analysis of its impact and probability of occurrence. Consideration should be given to the size and complexity of the process or subprocess and its impact on the organization's financial reporting process.
  - Statement of the control objective designed to reduce the risk of the process or subprocess to an acceptable level and a description of its alignment to the COSO framework
  - Description of the control activity(ies) designed and performed to satisfy the control objective related to the process or subprocess
  - Description of the approach followed to confirm (test) the existence and operational effectiveness of the control activities
  - Conclusions reached about the effectiveness of controls, as a result of testing

Lessons Learned

Parallels can be drawn between the effect of the Sarbanes-Oxley Act of 2002 on public companies and the impact of the US Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) on the banking industry. Both statutes introduced regulations to remedy perceived market failures, and each enacted significant new reporting requirements. There are several lessons public companies can learn from the FDICIA example:

- Accept that the environment has changed. Companies must recognize that they operate in a new environment—one that demands more effort and accountability.
- Promote understanding of internal control within the organization. Companies may be tempted to show superficial compliance with the Sarbanes-Oxley Act, but such an approach may backfire if controls fail because form was stressed over substance.
- Factor into the business model the cost of developing an internal control program. Good internal control is not a one-time expense; rather, it changes the cost of doing business.

Past events ushered in a new era in the history of business, characterized by a firm resolve to increase corporate responsibility. The Sarbanes-Oxley Act was created to restore investor confidence in public markets. Accountability, disclosure and reporting, good corporate governance, and ethical business practices are no longer optional niceties—they are the law.

To this end, IT professionals, especially those in executive positions, need to be well versed in internal control theory and practice to meet the requirements of the Act. CIOs must now take on the challenges of (1) enhancing their knowledge of internal control, (2) understanding their company's overall Sarbanes-Oxley compliance plan, (3) developing a compliance plan to specifically address IT controls and (4) integrating this plan into the overall Sarbanes-Oxley compliance plan. Unlike previous event-driven control activities (e.g., Y2K), Sarbanes-Oxley activity will continue as a routine part of doing business. IT is very important to internal control over financial reporting. Management's assessment as required by section 404 of the Sarbanes-Oxley Act is a complex and time-consuming project. Organizations need to develop an ongoing process to monitor compliance, as the full impact of the Sarbanes-Oxley Act will not be known for several years.

Appendix A—IT Control Objectives for Sarbanes-Oxley

The stage has been set for the importance of IT to prepare for Sarbanes-Oxley compliance, so the focus now turns to the specific control objectives that will form the basis of an IT control program.

Figure 10 illustrates the IT processes of COBIT and maps their relationship to the appropriate COSO component. It is immediately evident that many COBIT IT processes have relationships with more than one COSO component. This is expected given the nature of general IT controls as they form the basis for achieving reliable information systems. This multiple relationship attribute further demonstrates why IT controls are the basis for all others and are essential for a reliable internal control program.

COBIT is a comprehensive framework for managing risk and control of IT, comprising four domains, 34 IT processes and 318 detailed control objectives. COBIT includes controls that address operational and compliance objectives, but only those related to financial reporting have been used to develop this document.

While focus has been provided on what is required for financial reporting, the control objectives and considerations set forth in this document may exceed what is necessary for organizations seeking to comply with the requirements of the Sarbanes-Oxley Act. The suggested internal control framework (COSO) to be used for compliance with the Sarbanes-Oxley Act, as recommended by the SEC, addresses the topic of IT controls, but does not dictate requirements for such control objectives and related control activities. Similarly, PCAOB Auditing Standard No. 2 states the importance of IT controls, but does not specify which in particular must be included. Such decisions remain the discretion of each organization. Accordingly, organizations should assess the nature and extent of IT controls necessary to support their internal control program on a case-by-case basis.

The reader may find the following materials particularly useful. This guide was not prepared to suggest a one-size-fits-all approach; instead, it recommends that each organization tailor the control objective template to fit its specific circumstances. For example, if systems development is considered to be of low risk, an organization may choose to amend or delete some or all of the suggested control objectives. An organization should also consult with its external auditors to help ensure that all attestation-critical control objectives are addressed.

An important part of this publication is to provide guidance on the specific IT control objectives that should be considered for compliance with COSO and, ultimately, the Sarbanes-Oxley Act. Accordingly, the following section provides this information as well as a perspective on the importance of the control segment and how it relates to COSO and financial disclosure controls.

As always, IT organizations should consider the nature and extent of their operations in determining which of the control objectives, illustrative controls and tests of controls need to be included in their internal control program.

Figure 10—CobiT Areas/COSO Components

			COSO Component				
Company Level	Activity Level	CobiT Area	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
		Plan and Organize (IT Environment)					
●		IT strategic planning	●	●		●	●
●		Information architecture			●	●	
		Determine technological direction					
●		IT organization and relationships	●			●	
		Manage the IT investment					
●		Communication of management aims and direction	●			●	●
●		Management of human resources	●			●	
●		Compliance with external requirements				●	●
●		Assessment of risks		●			
		Manage projects					
●		Management of quality	●		●	●	●
		Acquire and Implement (Program Development and Program Change)					
		Identify automated solutions					
	●	Acquire or develop application software			●		
	●	Acquire technology infrastructure			●		
	●	Develop and maintain policies and procedures			●	●	
	●	Install and test application software and technology infrastructure			●		
	●	Manage changes			●		●
		Deliver and Support (Computer Operations and Access to Programs and Data)					
	●	Define and manage service levels	●		●		●
	●	Manage third-party services	●	●	●		●
●		Manage performance and capacity			●		●
		Ensure continuous service					
	●	Ensure systems security			●	●	●
		Identify and allocate costs					
●		Educate and train users	●			●	
		Assist and advise customers					
	●	Manage the configuration			●	●	
	●	Manage problems and incidents			●	●	●
	●	Manage data			●	●	
●		Manage facilities		●			
	●	Manage operations			●	●	
		Monitor and Evaluate (IT Environment)					
●		Monitoring				●	●
●		Adequacy of internal controls					●
●		Independent assurance	●				●
●		Internal audit					●

Appendix B—Company-level Questionnaire

The following questionnaire provides a company-level assessment of an organization's IT control environment. This questionnaire includes CobiT control objectives found in the Plan and Organize and Monitor and Evaluate domains and a few from the Deliver and Support domain. As most organizations are using the COSO control framework for their internal control program, this questionnaire has been structured in the same order as COSO.

Control Environment

The control environment creates the foundation for effective internal control, establishes the "tone at the top," and represents the apex of the corporate governance structure. The issues raised in the control environment component apply throughout an IT organization.

Points to Consider	Responses	Comments
IT Strategic Planning		
1. Has management prepared strategic plans for IT that align business objectives with IT strategies? Does the planning approach include mechanisms to solicit input from relevant internal and external stakeholders affected by the IT strategic plans?	□ Yes □ No	Comments
2. Does management obtain feedback from business process owners and users regarding the quality and usefulness of its IT plans for use in the ongoing risk assessment process?	□ Yes □ No	Comments
3. Does an IT planning or steering committee exist to oversee the IT function and its activities? Does committee membership include representatives from senior management, user management and the IT function?	□ Yes □ No	Comments
4. Are IT strategies and ongoing operations formally communicated to senior management and the board of directors, e.g., through periodic meetings of an IT steering committee?	□ Yes □ No	Comments
5. Does the IT organization ensure that IT plans are communicated to business process owners and other relevant parties across the organization?	□ Yes □ No	Comments
6. Does IT management communicate its activities, challenges and risks on a regular basis with the CEO and CFO? Is this information also shared with the board of directors?	□ Yes □ No	Comments
7. Does the IT organization monitor its progress against the strategic plan and react accordingly to meet established objectives?	□ Yes □ No	Comments
IT Organization and Relationships		
8. Do IT managers have adequate knowledge and experience to fulfill their responsibilities?	□ Yes □ No	Comments
9. Have key systems and data been inventoried and their owners identified?	□ Yes □ No	Comments

Points to Consider	Responses	Comments
IT Organization and Relationships (cont.)		
10. Are roles and responsibilities of the IT organization defined, documented and understood?	□ Yes □ No	Comments
11. Do IT personnel have sufficient authority to exercise the role and responsibility assigned to them?	□ Yes □ No	Comments
12. Do IT staff understand and accept their responsibility regarding internal control?	□ Yes □ No	Comments
13. Have data integrity ownership and responsibilities been communicated to appropriate data/business owners and have they accepted these responsibilities?	□ Yes □ No	Comments
14. Is the IT organizational structure sufficient to provide for necessary information flow to manage its activities?	□ Yes □ No	Comments
15. Has IT management implemented a division of roles and responsibilities (segregation of duties) that reasonably prevents a single individual from subverting a critical process?	□ Yes □ No	Comments
16. Are IT staff evaluations performed regularly (e.g., to ensure that the IT function has a sufficient number of competent IT staff necessary to achieve objectives)?	□ Yes □ No	Comments
17. Are contracted staff and other contract personnel subject to policies and procedures created to control their activities by the IT function, and to assure the protection of the organization's information assets?	□ Yes □ No	Comments
18. Are significant IT events or failures, e.g., security breaches, major system failures or regulatory failures, reported to senior management or the board?	□ Yes □ No	Comments
Management of Human Resources		
19. Are controls in place to support appropriate and timely responses to job changes and job terminations so that internal controls and security are not impaired by such occurrences?	□ Yes □ No	Comments
20. Does the IT organization subscribe to a philosophy of continuous learning, providing necessary training and skill development to its members?	□ Yes □ No	Comments
21. Has the IT organization adopted and promoted the company's culture of integrity management, including ethics, business practices and human resources evaluations?	□ Yes □ No	Comments
Educate and Train Users		
22. Has the entity established procedures for identifying and documenting the training needs of all personnel using information services in support of the long-range plan?	□ Yes □ No	Comments
23. Does IT management provide education and ongoing training programs that include ethical conduct, system security practices, confidentiality standards, integrity standards and security responsibilities of all staff?	□ Yes □ No	Comments

Information and Communication

COSO states that information is needed at all levels of an organization to run the business and achieve the company's control objectives. However, the identification, management and communication of relevant information represents an ever-increasing challenge to the IT department. The determination of which information is required to achieve control objectives and the communication of this information in a form and time frame that allow people to carry out their duties support the other four components of the COSO framework.

Points to Consider	Responses	Comments
Information Architecture		
24. Has IT management defined information capture, processing and reporting controls—including completeness, accuracy, validity and authorization—to support the quality and integrity of information used for financial and disclosure purposes?	□ Yes □ No	Comments
25. Has IT management defined information classification standards in accordance with corporate security and privacy policies?	□ Yes □ No	Comments
26. Has IT management defined, implemented and maintained security levels for each of the data classifications? Do these security levels represent the appropriate (minimum) set of security and control measures for each of the classifications? Are they reevaluated periodically and modified accordingly?	□ Yes □ No	Comments
Communication of Management Aims and Directions		
27. Has IT management formulated, developed and documented policies and procedures governing the IT organization's activities?	□ Yes □ No	Comments
28. Has IT management communicated policies and procedures governing the IT organization's activities?	□ Yes □ No	Comments
29. Does IT management periodically review its policies, procedures and standards to reflect changing business conditions?	□ Yes □ No	Comments
30. Does IT management have processes in place to investigate compliance deviations and introduce remedial action?	□ Yes □ No	Comments
31. Does IT management have a process in place to assess compliance with its policies, procedures and standards?	□ Yes □ No	Comments
32. Does IT management understand its roles and responsibilities related to the Sarbanes-Oxley Act?	□ Yes □ No	Comments

Risk Assessment

Risk assessment involves the identification and analysis by management of relevant risks to achieve predetermined objectives, which form the basis for determining control activities. It is likely that internal control risks could be more pervasive in the IT organization than in other areas of the company. Risk assessment may occur at the company level (for the overall organization) or at the activity level (for a specific process or business unit).

Points to Consider	Responses	Comments
Assessment of Risks		
33. Does the IT organization have an entity- and activity-level risk assessment framework that is used periodically to assess information risk to achieving business objectives? Does it consider the probability and likelihood of threats?	□ Yes □ No	Comments
34. Does the IT organization's risk assessment framework measure the impact of risks according to qualitative and quantitative criteria, using inputs from different areas including, but not limited to, management brainstorming, strategic planning, past audits and other assessments?	□ Yes □ No	Comments
35. Is the IT organization's risk assessment framework designed to support cost-effective controls to mitigate exposure to risks on a continuing basis, including risk avoidance, mitigation or acceptance?	□ Yes □ No	Comments
36. Is a comprehensive security assessment performed for critical systems and locations based on their relative priority and importance to the organization?	□ Yes □ No	Comments
37. Where risks are considered acceptable, is there formal documentation and acceptance of residual risk with related offsets, including adequate insurance coverage, contractually negotiated liabilities and self-insurance?	□ Yes □ No	Comments
38. Is the IT organization committed to active and continuous risk assessment processes as an important tool in providing information on the design and implementation of internal controls, in the definition of the IT strategic plan, and in the monitoring and evaluation mechanisms?	□ Yes □ No	Comments
39. Is access to the data center restricted to authorized personnel, requiring appropriate identification and authentication?	□ Yes □ No	Comments
40. Has a business impact assessment been performed that considers the impact of systems failure on the financial reporting process?	□ Yes □ No	Comments
Manage Facilities		
41. Are data center facilities equipped with adequate environmental controls to maintain systems and data, including fire suppression, uninterrupted power service (UPS), air conditioning and elevated floors?	□ Yes □ No	Comments

Monitoring

Monitoring, which covers the oversight of internal control by management through continuous and point-in-time assessment processes, is becoming increasingly important to IT management. There are two types of monitoring activities: continuous monitoring and separate evaluations.

Points to Consider	Responses	Comments
Compliance With External Requirements		
42. Does the organization monitor changes in external requirements for legal, regulatory or other external requirements related to IT practices and controls?	□ Yes □ No	Comments
43. Are control activities in place and followed to ensure compliance with external requirements, such as regulatory and legal rules?	□ Yes □ No	Comments
44. Are internal events considered in a timely manner to support continuous compliance with legal and regulatory requirements?	□ Yes □ No	Comments
Management of Quality		
45. Is documentation created and maintained for all significant IT processes, controls and activities?	□ Yes □ No	Comments
46. Does a plan exist to maintain the overall quality assurance of IT activities based on the organizational and IT plans?	□ Yes □ No	Comments
47. Are documentation standards in place, have they been communicated to all IT staff, and are they supported with training?	□ Yes □ No	Comments
48. Does a quality plan exist for significant IT functions (e.g., system development and deployment) and does it provide a consistent approach to address both general and project-specific quality ssurance activities?	□ Yes □ No	Comments
49. Does the quality plan prescribe the type(s) of quality assurance activities (such as reviews, audits, inspections) to be performed to achieve the objectives of the quality plan?	□ Yes □ No	Comments
50. Does the quality assurance process include a review of adherence to IT policies, procedures and standards?	□ Yes □ No	Comments
51. Have data integrity ownership and responsibilities been communicated to the appropriate data owners and have they accepted these responsibilities?	□ Yes □ No	Comments
Manage Performance and Capacity		
52. Does IT management monitor the performance and capacity levels of the systems and network?	□ Yes □ No	Comments
53. Does IT management have a process in place to respond to suboptimal performance and capacity measures in a timely manner?	□ Yes □ No	Comments
54. Is performance and capacity planning included in system design and implementation activities?	□ Yes □ No	Comments
Monitoring		
55. Have performance indicators (e.g., benchmarks) from both internal and external sources been defined, and are data being collected and reported regarding achievement of these benchmarks?	□ Yes □ No	Comments

Points to Consider	Responses	Comments
Monitoring (cont.)		
56. Has IT management established appropriate metrics to effectively manage the day-to-day activities of the IT department?	□ Yes □ No	Comments
57. Does IT management monitor IT's delivery of services to identify shortfalls and does IT respond with actionable plans to improve?	□ Yes □ No	Comments
Adequacy of Internal Control		
58. Does IT management monitor the effectiveness of internal controls in the normal course of operations through management and supervisory activities, comparisons and benchmarks?	□ Yes □ No	Comments
59. Are serious deviations in the operation of internal control, including major security, availability and processing integrity events, reported to senior management?	□ Yes □ No	Comments
60. Are internal control assessments performed periodically, using self-assessments or independent audits, to examine whether or not internal controls are operating satisfactorily?	□ Yes □ No	Comments
Independent Assurance		
61. Does IT management obtain independent reviews prior to implementing significant IT systems that are directly linked to the organization's financial reporting environment?	□ Yes □ No	Comments
62. Does IT management obtain independent internal control reviews of third-party service providers (e.g., by obtaining and reviewing copies of SAS 70, SysTrust or other independent audit reports)?	□ Yes □ No	Comments
63. Is documentation retained in a manner that can be used by the independent auditor or examiner as a basis for reliance?	□ Yes □ No	Comments
Internal Audit		
64. Does the organization have an IT internal audit department that is responsible for reviewing IT activities and controls?	□ Yes □ No	Comments
65. Is the audit plan based upon a risk assessment that includes IT? Does it cover the full range of IT audits, e.g., general and application controls, systems development life cycle?	□ Yes □ No	Comments
66. Are procedures in place to follow up on IT control issues in a timely manner?	□ Yes □ No	Comments

Appendix C—IT Control Objectives

IT General Controls—Program Development and Program Change

This domain considers procedures for acquiring and implementing new programs and systems, as well as changes in, and maintenance of, existing systems to make sure that the life cycle is continued for these systems. To realize the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process.

COBIT control processes that should be considered for COSO internal control models include:
- Acquire or develop application system software
- Acquire technology infrastructure
- Develop and maintain policies and procedures
- Install and test application software and technology infrastructure
- Manage changes

Each of these control processes is outlined in **figures 11** through **15**.

Figure 11—Acquire or Develop Application Software

Control Guidance

Control Objective—Controls provide reasonable assurance that application and system software is acquired or developed that effectively supports financial reporting requirements.

Rationale—Acquiring and maintaining software includes the design, acquisition/building and deployment of systems that support the achievement of business objectives. This process includes major changes to existing systems. This is where controls are designed and implemented to support initiating, recording, processing and reporting financial information and disclosure. Deficiencies in this area may have a significant impact on financial reporting and disclosure. For instance, without sufficient controls over application interfaces, financial information may not be complete or accurate.

Illustrative Controls	Illustrative Tests of Controls
The organization's system development life cycle methodology (SDLC) includes security, availability and processing integrity requirements of the organization.	Obtain a copy of the organization's SDLC methodology. Review the methodology to determine that it addresses security, availability and processing integrity requirements. Consider whether there are appropriate steps to ensure that these requirements are considered throughout the development or acquisition life cycle, e.g., security and availability and processing integrity should be considered during the requirements phase.
The organization's SDLC policies and procedures consider the development and acquisition of new systems and major changes to existing systems.	Review the organization's SDLC methodology to determine if it considers both the development and acquisition of new systems and major changes to existing systems.
The SDLC methodology ensures that information systems are designed to include application controls that support complete, accurate, authorized and valid transaction processing.	Review the methodology to determine if it addresses application controls. Consider whether there are appropriate steps to ensure that application controls are considered throughout the development or acquisition life cycle, e.g., application controls should be included in the conceptual design and detailed design phases.
The organization has an acquisition and planning process that aligns with its overall strategic direction.	Review the SDLC methodology to ensure that the organization's overall strategic direction is considered, e.g., an IT steering committee must review and approve projects to ensure that a proposed project aligns with strategic business requirements and that it will utilize approved technologies.
IT management ensures that users are appropriately involved in the design of applications, selection of packaged software and the testing thereof, to ensure a reliable environment.	Review the SDLC to determine if users are appropriately involved in the design of applications, selection of packaged software and testing.

Figure 11—Acquire or Develop Application Software *(cont.)*

Control Guidance

Illustrative Controls	Illustrative Tests of Controls
Post-implementation reviews are performed to verify controls are operating effectively.	Determine if post-implementation reviews are performed on new systems and significant changes reported.
The organization acquires/develops systems software in accordance with its acquisition, development and planning process.	Select a sample of projects that resulted in new financial systems being implemented. Review the documentation and deliverables from these projects to determine if they have been completed in accordance with the acquisition, development and planning process.

Figure 12—Acquire Technology Infrastructure

Control Guidance

Control Objective—Controls provide reasonable assurance that technology infrastructure is acquired so that it provides the appropriate platforms to support financial reporting applications.

Rationale—The process of acquiring and maintaining technology infrastructure includes the design, acquisition/building and deployment of systems that support applications and communications. Infrastructure components, including servers, networks and databases, are critical for secure and reliable information processing. Without an adequate infrastructure there is an increased risk that financial reporting applications will not be able to pass data between applications, financial reporting applications will not operate, and critical infrastructure failures will not be detected in a timely manner.

Illustrative Controls	Illustrative Tests of Controls
Documented procedures exist and are followed to ensure that infrastructure systems, including network devices and software, are acquired based on the requirements of the financial applications they are intended to support.	Select a sample of technology infrastructure implementations. Review the documentation and deliverables from these projects to determine if infrastructure requirements were considered at the appropriate time during the acquisition process.

Figure 13—Develop and Maintain Policies and Procedures

Control Guidance

Control Objective—Controls provide reasonable assurance that policies and procedures that define required acquisition and maintenance processes have been developed and are maintained, and that they define the documentation needed to support the proper use of the applications and the technological solutions put in place.

Rationale—Policies and procedures include the SDLC methodology, the process for acquiring, developing and maintaining applications, as well as required documentation. For some organizations they include service level agreements, operational practices and training materials. Policies and procedures support an organization's commitment to perform business process activities in a consistent and objective manner.

Illustrative Controls	Illustrative Tests of Controls
The organization's SDLC methodology and associated policies and procedures are regularly reviewed, updated and approved by management.	Confirm that the organization's policies and procedures are regularly reviewed and updated as changes in the environment dictate. When policies and procedures are changed, determine if management approves such changes. Select a sample of projects and determine that user reference and support manuals and systems documentation and operations documentation were prepared. Consider whether drafts of these manuals were incorporated in user acceptance testing. Determine whether any changes to proposed controls resulted in documentation updates.
The organization ensures that its systems and applications are developed in accordance with its supported, documented policies and procedures.	Review a sample of application documentation (including user manuals) to determine if they comply with the policies and procedures that have been documented by the organization.

Figure 14—Install and Test Application Software and Technology Infrastructure

Control Guidance

Control Objective—Controls provide reasonable assurance that the systems are appropriately tested and validated prior to being placed into production processes and associated controls operate as intended and support financial reporting requirements.

Rationale—Installation testing and validating relate to the migration of new systems into production. Before such systems are installed, appropriate testing and validation must be performed to ensure that systems are operating as designed. Without adequate testing, systems may not function as intended and may provide invalid information, which could result in unreliable financial information and reports.

Illustrative Controls	Illustrative Tests of Controls
A testing strategy is developed and followed for all significant changes in applications and infrastructure technology, which addresses unit-, system-, integration- and user acceptance-level testing to help ensure that deployed systems operate as intended.	Select a sample of system development projects and significant system upgrades (including technology upgrades). Determine if a formal testing strategy was prepared and followed. Consider whether this strategy considered potential development and implementation risks and addressed all the necessary components to address these risks, e.g., if the completeness and accuracy of system interfaces were essential to the production of complete and accurate reporting, these interfaces were included in the testing strategy. (Note: controls over the final move to production are addressed in the Manage Changes **figure 15**.)
Load and stress testing is performed according to a test plan and established testing standards.	Select a sample of system development projects and significant system upgrades that are significant for financial reporting. Where it was considered that capacity and performance were of potential concern, review the approach to load and stress testing. Consider whether a structured approach was taken to load and stress testing and that the approach taken adequately modeled the anticipated volumes, including types of transactions being processed and the impact on performance of other services that would be running concurrently.

Figure 14—Install and Test Application Software and Technology Infrastructure *(cont.)*

Control Guidance

Illustrative Controls	Illustrative Tests of Controls
Interfaces with other systems are tested to confirm that data transmissions are complete, accurate and valid.	Select a sample of system development projects and significant system upgrades that are significant for financial reporting. Determine if interfaces with other systems were tested to confirm that data transmissions are complete, e.g., record totals are accurate and valid. Consider whether the extent of testing was sufficient and included recovery in the event of incomplete data transmissions.
The conversion of data is tested between its origin and its destination to confirm that it is complete, accurate and valid.	Obtain a sample of system development projects and significant system upgrades that are significant for financial reporting. Determine if a conversion strategy was documented. Consider whether it included strategies to “scrub” the data in the old system before conversion or to “run down” data in the old system before conversion. Review the conversion testing plan. Consider whether the following were considered: data transformations, input of data not available in the old system, edits, completeness controls and timing of conversions. Determine if the conversion was included in acceptance testing and was approved by user management.

Figure 15—Manage Changes

Control Guidance

Control Objective—Controls provide reasonable assurance that system changes of financial reporting significance are authorized and appropriately tested before being moved to production.

Rationale—Managing changes addresses how an organization modifies system functionality to help the business meet its financial reporting objectives. Deficiencies in this area could significantly impact financial reporting. For instance, changes to the programs that allocate financial data to accounts require appropriate approvals and testing prior to the change to ensure classification and reporting integrity.

Illustrative Controls	Illustrative Tests of Controls
Requests for program changes, system changes and maintenance (including changes to system software) are standardized, documented and subject to formal change management procedures	Determine that a documented change management process exists and is maintained to reflect the current process. Consider if change management procedures exist for all changes to the production environment, including program changes, system maintenance and infrastructure changes. Evaluate the process used to control and monitor change requests. Consider whether change requests are properly initiated, approved and tracked. Determine whether program change is performed in a segregated, controlled environment. Select a sample of changes made to applications/systems to determine whether they were adequately tested and approved before being placed into a production environment. Establish if the following are included in the approval process: operations, security, IT infrastructure management and IT management. Evaluate procedures designed to ensure only authorized/ approved changes are moved into production. Trace the sample of changes back to the change request log and supporting documentation. Confirm that these procedures address the timely implementation of patches to system software. Select a sample to determine compliance with the documented procedures.

Figure 15—Manage Changes *(cont.)*

Control Guidance	
Illustrative Controls	**Illustrative Tests of Controls**
Emergency change requests are documented and subject to formal change management procedures.	Determine if a process exists to control and supervise emergency changes. Determine if an audit trail exists of all emergency activity and that it is independently reviewed. Determine that procedures require that emergency changes be supported by appropriate documentation. Establish that backout procedures are developed for emergency changes. Evaluate procedures ensuring that all emergency changes are tested and subject to standard approval procedures after they have been made. Review a sample of changes that are recorded as "emergency" changes, and determine if they contain the needed approval and the needed access was terminated after a set period of time. Establish that the sample of changes was well documented.
Controls are in place to restrict migration of programs to production only by authorized individuals.	Evaluate the approvals required before a program is moved to production. Consider approvals from system owners, development staff and computer operations. Confirm that there is appropriate segregation of duties between the staff responsible for moving a program into production and development staff. Obtain and test evidence to support this assertion.
IT management ensures that the setup and implementation of system software do not jeopardize the security of the data and programs being stored on the system.	Determine that a risk assessment of the potential impact of changes to system software is performed. Review procedures to test changes to system software in a development environment before they are applied to production. Verify that backout procedures exist.

IT General Controls—Computer Operations and Access to Programs and Data

This domain considers procedures for the actual delivery of required services, which range from traditional operations to security and access management. To deliver services, the necessary support processes must be set up.

COBIT control processes that should be considered for COSO internal control models include:

- Define and manage service levels
- Manage third-party services
- Ensure systems security
- Manage the configuration
- Manage problems and incidents
- Manage data
- Manage operations

Each of these control processes is outlined in **figures 16** through **22**.

Figure 16—Define and Manage Service Levels

<table>
<tr><th colspan="2">Control Guidance</th></tr>
<tr><td colspan="2"><b>Control Objective—Controls provide reasonable assurance that service levels are defined and managed in a manner that satisfies financial reporting system requirements and provides a common understanding of performance levels with which the quality of services will be measured.</b></td></tr>
<tr><td colspan="2"><b>Rationale</b>—The process of defining and managing service levels addresses how an organization meets the functional and operational expectations of its users and, ultimately, the objectives of the business. Roles and responsibilities are defined and an accountability and measurement model is used to ensure services are delivered as required. Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, if systems are poorly managed or system functionality is not delivered as required, financial information may not be processed as intended.</td></tr>
<tr><th>Illustrative Controls</th><th>Illustrative Tests of Controls</th></tr>
<tr><td>Service levels are defined and managed to support financial reporting system requirements.</td><td>Obtain a sample of service level agreements and review their content for clear definition of service descriptions and expectations of users.
Discuss with members of the organization responsible for service level management and test evidence to determine whether service levels are actively managed.
Obtain and test evidence that service levels are being actively managed in accordance with service level agreements.
Discuss with users whether financial reporting systems are being supported and delivered in accordance with their expectations and service level agreements.</td></tr>
</table>

Figure 16—Define and Manage Service Levels *(cont.)*

Control Guidance

Illustrative Controls	Illustrative Tests of Controls
A framework is defined to establish key performance indicators to manage service level agreements, both internally and externally.	Obtain service level performance reports and confirm that they include key performance indicators. Review the performance results, identify performance issues and assess how service level managers are addressing these issues.

Figure 17—Manage Third-party Services

Control Guidance

Control Objective—Controls provide reasonable assurance that third-party services are secure, accurate and available, support processing integrity and defined appropriately in performance contracts.

Rationale—Managing third-party services includes the use of outsourced service providers to support financial applications and related systems. Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, insufficient controls over processing accuracy by a third-party service provider may result in inaccurate financial results.

Illustrative Controls	Illustrative Tests of Controls
A designated individual is responsible for regular monitoring and reporting on the achievement of the third-party service level performance criteria.	Determine if the management of third-party services has been assigned to appropriate individuals.
Selection of vendors for outsourced services is performed in accordance with the organization’s vendor management policy.	Obtain the organization’s vendor management policy and discuss with those responsible for third-party service management if they follow such standards. Obtain and test evidence that the selection of vendors for outsourced services is performed in accordance with the organization’s vendor management policy.
IT management determines that, before selection, potential third parties are properly qualified through an assessment of their capability to deliver the required service and a review of their financial viability.	Obtain the criteria and business case used for selection of third-party service providers. Assess whether these criteria include a consideration of the third party’s financial stability, skill and knowledge of the systems under management, and controls over security, availability and processing integrity.

Figure 17—Manage Third-party Services *(cont.)*

Control Guidance

Illustrative Controls	Illustrative Tests of Controls
Third-party service contracts address the risks, security controls and procedures for information systems and networks in the contract between the parties.	Select a sample of third-party service contracts and determine if they include controls to support security, availability and processing integrity in accordance with the company's policies and procedures.
Procedures exist and are followed to ensure that a formal contract is defined and agreed for all third-party services before work is initiated, including definition of internal control requirements and acceptance of the organization's policies and procedures.	Review a sample of contracts and determine whether: • There is a definition of services to be performed. • The responsibilities for the controls over financial reporting systems have been adequately defined. • The third party has accepted compliance with the organization's policies and procedures, e.g., security policies and procedures. • The contracts were reviewed and signed by appropriate parties before work commenced. • The controls over financial reporting systems and subsystems described in the contract agree with those required by the organization. Review gaps, if any, and consider further analysis to determine the impact on financial reporting.
A regular review of security, availability and processing integrity is performed for service level agreements and related contracts with third-party service providers.	Inquire whether third-party service providers perform independent reviews of security, availability and processing integrity, e.g., service auditor report. Obtain a sample of the most recent review and determine if there are any control deficiencies that would impact financial reporting.

Figure 18—Ensure Systems Security

Control Guidance

Control Objective—Controls provide reasonable assurance that financial reporting systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.

Rationale—Managing systems security includes both physical and logical controls that prevent unauthorized access. These controls typically support authorization, authentication, nonrepudiation, data classification and security monitoring. Deficiencies in this area could significantly impact financial reporting. For instance, insufficient controls over transaction authorization may result in inaccurate financial reporting.

Illustrative Controls	Illustrative Tests of Controls
An information security policy exists and has been approved by an appropriate level of executive management.	Obtain a copy of the organization's security policy and evaluate the effectiveness. Points to be taken into consideration include: • Is there an overall statement of the importance of security to the organization? • Have specific policy objectives been defined? • Have employee and contractor security responsibilities been addressed? • Has the policy been approved by an appropriate level of senior management to demonstrate management's commitment to security? • Is there a process to communicate the policy to all levels of management and employees?
A framework of security standards has been developed that supports the objectives of the security policy.	Obtain a copy of the security standards. Determine whether the standards framework effectively meets the objectives of the security policy. Consider whether the following topics, which are often addressed by security standards, have been appropriately covered: • Security organization • Asset classification and control • Personnel security • Software security policy • Physical and environmental security • Workstation security • Computing environment management • Network environment management • System access control • Business continuity planning • Compliance • System development and maintenance Determine if there are processes in place to communicate and maintain these standards.

Figure 18—Ensure Systems Security *(cont.)*

Control Guidance	
Illustrative Controls	**Illustrative Tests of Controls**
An IT security plan exists that is aligned with overall IT strategic plans.	Obtain a copy of security plans or strategies for financial reporting systems and subsystems and assess their adequacy in relation to the overall company plan.
The IT security plan is updated to reflect changes in the IT environment as well as security requirements of specific systems.	Confirm that the security plan reflects the unique security requirements of financial reporting systems and subsystems.
Procedures exist and are followed to authenticate all users to the system to support the validity of transactions. subsystems.	Assess the authentication mechanisms used to validate user credentials for financial reporting systems and validate that user sessions time-out after a predetermined period of time.
Procedures exist and are followed to maintain the effectiveness of authentication and access mechanisms (e.g., regular password changes).	Review security practices to confirm that authentication controls (passwords, IDs, two-factor, etc.) are used appropriately and are subject to common confidentiality requirements (IDs and passwords not shared, alphanumeric passwords used, etc.).
Procedures exist and are followed to ensure timely action relating to requesting, establishing, issuing, suspending and closing user accounts.	Confirm that procedures exist for the registration, change and deletion of users from financial reporting systems and subsystems on a timely basis and the procedures are followed. Validate that attempts to gain unauthorized access to financial reporting systems and subsystems are logged and are followed up on a timely basis. Select a sample of new users and determine if management approved their access and the access granted agrees with the access privileges that were approved. Select a sample of terminated employees and determine if their access has been removed, and was done in a timely manner. Select a sample of current users and review their access for appropriateness based upon their job functions.

Figure 18—Ensure Systems Security *(cont.)*

Control Guidance

Illustrative Controls	Illustrative Tests of Controls
A control process exists and is followed to periodically review and confirm access rights.	Inquire whether access controls are reviewed for financial reporting systems and subsystems on a periodic basis by management. Assess the adequacy of how exceptions are reexamined, and if the follow-up occurs in a timely manner.
Where appropriate, controls exist to ensure that neither party can deny transactions and controls are implemented to provide nonrepudiation of origin or receipt, proof of submission and receipt of transactions.	Determine how the organization establishes accountability for transaction initiation and approval. Test the use of accountability controls by observing a user attempting to enter an unauthorized transaction. Obtain a sample of transactions, and identify evidence of the accountability or origination of each.
Where network connectivity is used, appropriate controls, including firewalls, intrusion detection and vulnerability assessments, exist and are used to prevent unauthorized access.	Determine the sufficiency and appropriateness of perimeter security controls including firewalls and intrusion detection systems. Inquire whether management has performed an independent assessment of controls within the past year (e.g., ethical hacking, social engineering). Obtain a copy of this assessment and review the results, including the appropriateness of follow-up on identified weaknesses. Determine if antivirus systems are used to protect the integrity and security of financial reporting systems and subsystems. When appropriate, determine if encryption techniques are used to support the confidentiality of financial information sent from one system to another.

Figure 18—Ensure Systems Security *(cont.)*

Control Guidance	
Illustrative Controls	**Illustrative Tests of Controls**
IT security administration monitors and logs security activity, and identified security violations are reported to senior management.	Inquire whether a security office exists to monitor for security vulnerabilities and related threat events. Assess the nature and extent of such events over the past year and discuss with management how they have responded with controls to prevent unauthorized access or manipulation of financial systems and subsystems.
Controls relating to appropriate segregation of duties over requesting and granting access to systems and data exist and are followed.	Review the process to request and grant access to systems and data and confirm that the same person does not perform these functions.
Access to facilities is restricted to authorized personnel and requires appropriate identification and authentication.	Obtain polices and procedures as they relate to facility security, key and card reader access—and determine if those procedures account for proper identification and authentication. Observe the in and out traffic to the organization's facilities to establish that proper access is controlled. Select a sample of users and determine if their access is appropriate based upon their job responsibilities.

Figure 19—Manage the Configuration

Control Guidance

Control Objective—Controls provide reasonable assurance that all IT components, as they relate to security, processing and availability, are well protected, would prevent any unauthorized changes, and assist in the verification and recording of the current configuration.

Rationale—Configuration management ensures that security, availability and processing integrity controls are set up in the system and maintained through its life cycle. Insufficient configuration controls can lead to security and availability exposures that may permit unauthorized access to systems and data and impact financial reporting.

Illustrative Controls	Illustrative Tests of Controls
Only authorized software is permitted for use by employees using company IT assets.	Determine if procedures are in place to detect and prevent the use of unauthorized software. Obtain and review the company policy as it relates to software use to see that this is clearly articulated. Consider reviewing a sample of applications and computers to determine if they are in conformance with organization policy.
System infrastructure, including firewalls, routers, switches, network operating systems, servers and other related devices, is properly configured to prevent unauthorized access.	Determine if the organization's policies require the documentation of the current configuration, as well as the security configuration settings to be implemented. Review a sample of servers, firewalls, routers, etc., to consider if they have been configured in accordance with the organization's policy.
Application software and data storage systems are properly configured to provision access based on the individual's demonstrated need to view, add, change or delete data.	Conduct an evaluation of the frequency and timeliness of management's review of configuration records. Assess whether management has documented the configuration management procedures. Review a sample of configuration changes, additions or deletions, to consider if they have been properly approved based on a demonstrated need.
IT management has established procedures across the organization to protect information systems and technology from computer viruses.	Review the organization's procedures to detect computer viruses. Verify that the organization has installed and is using virus software on its networks and personal computers.
Periodic testing and assessment is performed to confirm that the software and network infrastructure is appropriately configured.	Review the software and network infrastructure to establish that it has been appropriately configured and maintained, according to the organization's documented process.

Figure 20—Manage Problems and Incidents

Control Guidance

Control Objective—Controls provide reasonable assurance that any problems and/or incidents are properly responded to, recorded, resolved or investigated for proper resolution.

Rationale—Managing problems and incidents addresses how an organization identifies, documents and responds to events that fall outside of normal operations. Deficiencies in this area could significantly impact financial reporting.

Illustrative Controls	Illustrative Tests of Controls
IT management has defined and implemented a problem management system to ensure that operational events that are not part of standard operation (incidents, problems and errors) are recorded, analyzed and resolved in a timely manner.	Determine if a problem management system exists, and how it is being used. Review how management has ocumented how the system is to be used. Review a sample of problem or incident reports, to consider if the issues were addressed (recorded, analyzed and resolved) in a timely manner.
The problem management system provides for adequate audit trail facilities, which allow tracing from incident to underlying cause.	Determine if the organization's procedures include audit trail facilities—tracking of the incidents. Review a sample of problems recorded on the problem management system to consider if a proper audit trail exists and is used.
A security incident response process exists to support timely response and investigation of unauthorized activities.	Verify that all unauthorized activities are responded to in a timely fashion, and there is a process to support proper disposition.

Figure 21—Manage Data

Control Guidance

Control Objective—Controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and valid throughout the update and storage process.

Rationale—Managing data includes the controls and procedures used to support information integrity, including its completeness, accuracy, authorization and validity. Controls are designed to support initiating, recording, processing and reporting financial information. Deficiencies in this area could significantly impact financial reporting. For instance, without appropriate authorization controls over the initiation of transactions, resulting financial information may not be reliable.

Illustrative Controls	Illustrative Tests of Controls
Policies and procedures exist for the handling, distribution and retention of data and reporting output.	Review the policies and procedures for the handling, distribution and retention of data and reporting output. Determine whether the policies and procedures are adequate for the protection of data and the timely distribution of all the correct financial reports (including electronic reports) to appropriate personnel. Obtain and test evidence that the controls over the protection of data and the timely distribution of financial reports (including electronic reports) to appropriate personnel are operating effectively.
Management protects sensitive information, logically and physically, in storage and during transmission against unauthorized access or modification.	Review the results of security testing. Determine if there are adequate controls to protect sensitive information, both logically and physically, in storage and during transmission against unauthorized access or modification.
Retention periods and storage terms are defined for documents, data, programs, reports and messages (incoming and outgoing), as well as the data (keys, certificates) used for their encryption and authentication.	Obtain the procedures dealing with distribution and retention of data. Confirm that the procedures define the retention periods and storage terms for documents, data, programs, reports and messages (incoming and outgoing), as well as the data (keys, certificates) used for their encryption and authentication. Confirm that the retention periods are in conformity with the Sarbanes-Oxley Act.

Figure 21—Manage Data *(cont.)*

Control Guidance	
Illustrative Controls	**Illustrative Tests of Controls**
	Confirm that the retention periods of previously archived material are in conformity with the Sarbanes-Oxley Act. Select a sample of archived material and test evidence that archived material is being archived in conformance with the requirements of the Sarbanes-Oxley Act.
Management has implemented a strategy for cyclical backup of data and programs.	Determine if the organization has procedures in place to back up data and programs based on IT and user requirements. Select a sample of data files and programs and determine if they are being backed up as required.
Procedures exist and are followed to periodically test the effectiveness of the restoration process and the quality of backup media.	Inquire whether the retention and storage of messages, documents, programs, etc., have been tested during the past year. Obtain and review the results of testing activities. Establish whether any deficiencies were noted and whether they have been reexamined. Obtain the organization's access security policy and discuss with those responsible whether they follow such standards and guidelines dealing with sensitive backup data.
Changes to data structures are authorized, made in accordance with design specifications and implemented in a timely manner.	Obtain a sample of data structure changes and determine whether they adhere to the design specifications and were implemented in the time frame required.

Figure 22—Manage Operations

Control Guidance

Control Objective—Controls provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing, error monitoring and system availability.

Rationale—Managing operations addresses how an organization maintains reliable application systems in support of the business to initiate, record, process and report financial information. Deficiencies in this area could significantly impact an entity's financial reporting. For instance, lapses in the continuity of application systems may prevent an organization from recording financial transactions and thereby undermine its integrity.

Illustrative Controls	Illustrative Tests of Controls
Management has established and documented standard procedures for IT operations, including scheduling, managing, monitoring and responding to security, availability and processing integrity events.	Determine if management has documented its procedures for IT operations, and operations are reviewed periodically to ensure compliance. Review a sample of events to confirm that response procedures are operating effectively. When used, review the job scheduling process and the procedures in place to monitor job completeness.
System event data are sufficiently retained to provide chronological information and logs to enable the review, examination and reconstruction of system and data processing.	Determine if sufficient chronological information is being recorded and stored in logs, and it is useable for reconstruction, if necessary. Obtain a sample of the log entries, to determine if they sufficiently allow for reconstruction.
System event data are designed to provide reasonable assurance as to the completeness and timeliness of system and data processing.	Inquire as to the type of information that is used by management to verify the completeness and timeliness of system and data processing. Review a sample of system processing event data to confirm the completeness and timeliness of processing.
End-user computing policies and procedures concerning security, availability and processing integrity exist and are followed.	Obtain a copy of the end-user computing policies and procedures and confirm that they address security, availability and processing integrity controls. Select a sample of users and inquire whether they are aware of this policy and if they are in compliance with it.

Figure 22—Manage Operations *(cont.)*

Control Guidance

Illustrative Controls	Illustrative Tests of Controls
End-user computing, including spreadsheets and other user-developed programs, are documented and regularly reviewed for processing integrity, including their ability to sort, summarize and report accurately.	Inquire as to management's knowledge of end-user programs in use across the company. Inquire as to the frequency and approaches followed to review end-user programs for processing integrity, and review a sample of these to confirm effectiveness. Review user-developed systems and test their ability to sort, summarize and report in accordance with management intentions.
User-developed systems and data are regularly backed up and stored in a secure area.	Inquire how end-user systems are backed up and where they are stored.
User-developed systems, such as spreadsheets and other end-user programs, are secured from unauthorized use.	Review the security used to protect unauthorized access to user-developed systems. Consider observing a user attempting to gain unauthorized access to user-developed systems. Inquire how management is able to detect unauthorized access and what follow-up procedures are performed to assess the impact of such access.
Access to user-developed systems is restricted to a limited number of users.	Select a sample of user-developed systems and determine who has access and if the access is appropriate.
Inputs, processing and outputs from user-developed systems are independently verified for completeness and accuracy.	Inquire how management verifies the accuracy and completeness of information processed and reported from user-developed systems. Inquire who reviews and approves outputs from user-developed systems prior to their submission for further processing or final reporting. Consider reperforming or reviewing the logic used in user-developed systems and conclude on its ability to process completely and accurately.

Application Controls—Business Cycles

Application controls apply to the business processes they support. They are controls designed within the application to prevent or detect unauthorized transactions. When combined with manual controls, as necessary, application controls ensure completeness, accuracy, authorization and validity of processing transactions.

For the most part, control objectives presented in the following figures can be enabled through the use of built-in application control functionality. This functionality is commonly found in integrated ERP environments, such as SAP, PeopleSoft, Oracle, JD Edwards and others. Where this functionality does not exist, these control objectives may require a combination of manual and automated control procedures to satisfy the control objective.

The control objectives presented below should not be considered an exhaustive list, but rather an example of controls that are commonly enabled by application systems. Organizations should consider what additional control objectives are required based on their particular industry and operating environment.

Figures 23-27 refer to controls that extend into applications and business processes that contribute to completeness, accuracy, validity and authorization controls.

Figure 23—Application Control Objectives for the Sales Cycle

Illustrative Control Objectives	Financial Statement Assertions
Orders are processed only within approved customer credit limits.	Valuation
Orders are approved by management as to prices and terms of sale.	Validity
Orders and cancellations of orders are input accurately.	Valuation
Order entry data are transferred completely and accurately to the shipping and invoicing activities.	Valuation Completeness
All orders received from customers are input and processed.	Completeness
Only valid orders are input and processed.	Validity
Invoices are generated using authorized terms and prices.	Valuation
Invoices are accurately calculated and recorded.	Valuation
Credit notes and adjustments to accounts receivable are accurately calculated and recorded.	Valuation
All goods shipped are invoiced.	Completeness

Figure 23—Application Control Objectives for the Sales Cycle *(cont.)*

Illustrative Control Objectives	Financial Statement Assertions
Credit notes for all goods returned and adjustments to accounts receivable are issued in accordance with organization policy.	Validity
Invoices relate to valid shipments.	Validity
All credit notes relate to a return of goods or other valid adjustments.	Completeness
All invoices issued are recorded.	Completeness
All credit notes issued are recorded.	Validity
Invoices are recorded in the appropriate period.	Valuation Occurrence
Credit notes issued are recorded in the appropriate period.	Valuation Occurrence
Cash receipts are recorded in the period in which they are received.	Valuation Occurrence
Cash receipts data are entered for processing accurately.	Valuation
All cash receipts data are entered for processing.	Validity
Cash receipts data are valid and are entered for processing only once.	Completeness
Cash discounts are accurately calculated and recorded.	Valuation
Timely collection of accounts receivable is monitored.	Valuation
The customer master file is maintained.	Completeness Validity
Only valid changes are made to the customer master file.	Completeness Validity
All valid changes to the customer master file are input and processed.	Completeness Validity
Changes to the customer master file are accurate.	Valuation
Changes to the customer master file are processed in a timely manner.	Completeness Validity
Customer master file data remain up-to-date.	Completeness Validity

Figure 24—Application Control Objectives for the Purchasing Cycle

Illustrative Control Objectives	Financial Statement Assertions
Purchase orders are placed only for approved requisitions.	Validity
Purchase orders are accurately entered.	Valuation
All purchase orders issued are input and processed.	Completeness
Amounts posted to accounts payable represent goods or services received.	Validity
Accounts payable amounts are accurately calculated and recorded.	Valuation
All amounts for goods or services received are input and processed to accounts payable.	Completeness
Amounts for goods or services received are recorded in the appropriate period.	Valuation Occurrence
Accounts payable are adjusted only for valid reasons.	Completeness Validity
Credit notes and other adjustments are accurately calculated and recorded.	Valuation
All valid credit notes and other adjustments related to accounts payable are input and processed.	Completeness Validity
Credit notes and other adjustments are recorded in the appropriate period.	Valuation Occurrence
Disbursements are made only for goods and services received.	Validity
Disbursements are distributed to the appropriate suppliers.	Validity
Disbursements are accurately calculated and recorded.	Valuation
All disbursements are recorded.	Completeness
Disbursements are recorded in the period in which they are issued.	Valuation Occurrence
Only valid changes are made to the supplier master file.	Completeness Validity
All valid changes to the supplier master file are input and processed.	Completeness Validity
Changes to the supplier master file are accurate.	Valuation
Changes to the supplier master file are processed in a timely manner.	Completeness Validity
Supplier master file data remain up-to-date.	Completeness Validity

Figure 25—Application Control Objectives for the Inventory Cycle

Illustrative Control Objectives	Financial Statement Assertions
Adjustments to inventory prices or quantities are recorded promptly and in the appropriate period.	Validity Completeness Valuation Occurrence
Adjustments to inventory prices or quantities are recorded accurately.	Valuation
Raw materials are received and accepted only if they have valid purchase orders.	Validity
Raw materials received are recorded accurately.	Valuation
All raw materials received are recorded.	Completeness
Receipts of raw materials are recorded promptly and in the appropriate period.	Valuation Occurrence
Defective raw materials are returned promptly to suppliers.	Validity
All transfers of raw materials to production are recorded accurately and in the appropriate period.	Valuation Occurrence Completeness
All direct and indirect expenses associated with production are recorded accurately and in the appropriate period.	Valuation Occurrence
All transfers of completed units of production to finished goods inventory are recorded completely and accurately in the appropriate period.	Valuation Completeness
Finished goods returned by customers are recorded completely and accurately in the appropriate period.	Valuation Completeness Occurrence
Finished goods received from production are recorded completely and accurately in the appropriate period.	Completeness Valuation Occurrence
All shipments are recorded.	Validity
Shipments are recorded accurately.	Valuation
Shipments are recorded promptly and in the appropriate period.	Valuation Occurrence
Inventory is reduced only when goods are shipped with approved customer orders.	Completeness Validity
Costs of shipped inventory are transferred from inventory to cost of sales.	Validity Valuation
Costs of shipped inventory are accurately recorded.	Valuation
Amounts posted to cost of sales represent those associated with shipped inventory.	Completeness Validity
Costs of shipped inventory are transferred from inventory to cost of sales promptly and in the appropriate period.	Valuation Occurrence

Figure 25—Application Control Objectives for the Inventory Cycle *(cont.)*

Illustrative Control Objectives	Financial Statement Assertions
Only valid changes are made to the inventory management master file.	Validity Completeness
All valid changes to the inventory management master file are input and processed.	Validity Completeness
Changes to the inventory management master file are accurate.	Valuation
Changes to the inventory management master file are promptly processed.	Validity Completeness
Inventory management master file data remain up-to-date.	Completeness Validity

Figure 26—Application Control Objectives for the Asset Management Cycle

Illustrative Control Objectives	Financial Statement Assertions
Fixed asset acquisitions are accurately recorded.	Valuation
Fixed asset acquisitions are recorded in the appropriate period.	Valuation Occurrence
All fixed asset acquisitions are recorded.	Completeness
Depreciation charges are accurately calculated and recorded.	Valuation
All depreciation charges are recorded in the appropriate period.	Validity Valuation Occurrence Completeness
All fixed asset disposals are recorded.	Validity
Fixed asset disposals are accurately calculated and recorded.	Valuation
Fixed asset disposals are recorded in the appropriate period.	Valuation Occurrence
Records of fixed asset maintenance activity are accurately maintained.	Completeness
Fixed asset maintenance activities records are updated in a timely manner.	Completeness
Only valid changes are made to the fixed asset register and/or master file.	Completeness Validity
All valid changes to the fixed asset register and/or master file are input and processed.	Completeness Validity
Changes to the fixed asset register and/or master file are accurate.	Valuation
Changes to the fixed asset register and/or master file are promptly processed.	Completeness Validity
Fixed asset register and/or master file data remain up-to-date.	Completeness Validity

Figure 27—Application Control Objectives for the Human Resource Cycle

Illustrative Control Objectives	Financial Statement Assertions
Additions to the payroll master files represent valid employees.	Validity
All new employees are added to the payroll master files.	Completeness
Terminated employees are removed from the payroll master files.	Validity
Employees are terminated only within statutory and union requirements.	Completeness
Deletions from the payroll master files represent valid terminations.	Completeness
All time worked is input.	Completeness
Time worked is accurately input and processed.	Valuation
Payroll is recorded in the appropriate period.	Valuation Occurrence
Payroll (including compensation and withholdings) is accurately calculated and recorded.	Valuation
Payroll is disbursed to appropriate employees.	Validity
Only valid changes are made to the payroll master files.	Validity Completeness
All valid changes to the payroll master files are input and processed.	Validity Completeness
Changes to the payroll master files are accurate.	Valuation
Changes to the payroll master files are processed in a timely manner.	Validity Completeness
Payroll master file data remain up-to-date.	Validity Completeness
Only valid changes are made to the payroll withholding tables.	Validity Completeness
All valid changes to the payroll withholding tables are input and processed.	Validity Completeness
Changes to the payroll withholding tables are accurate.	Valuation
Changes to the payroll withholding tables are promptly processed.	Validity Completeness
Payroll withholding table data remain up-to-date.	Validity Completeness