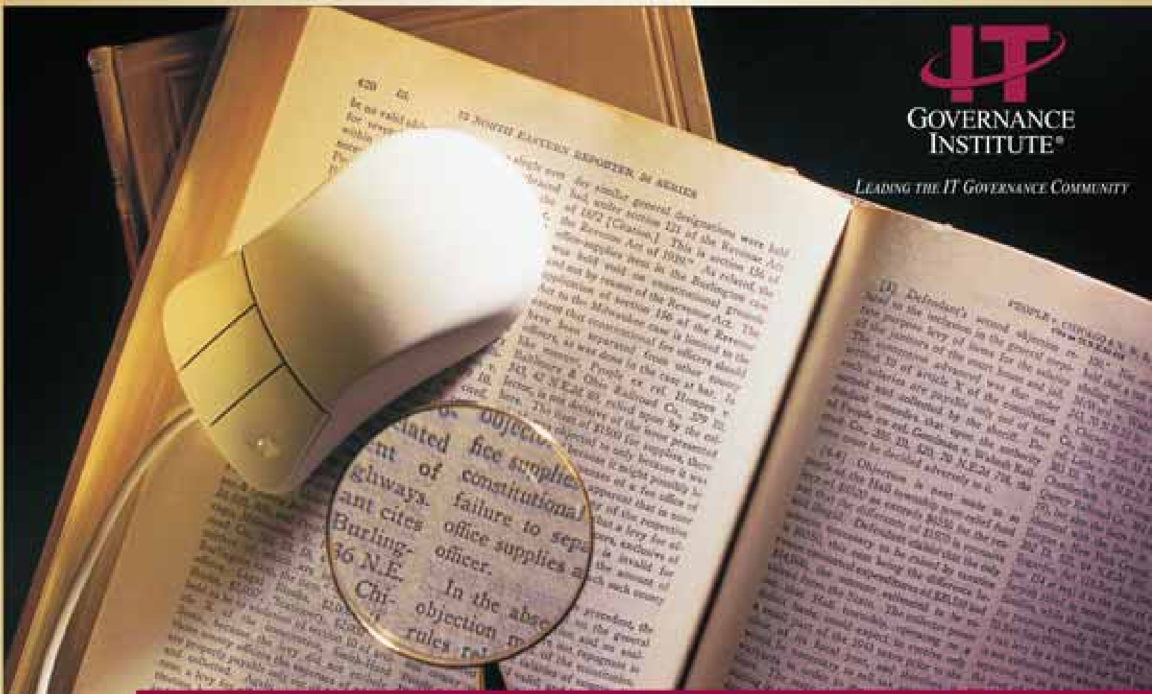


IT Governance Institute®
Leading the IT Governance Community

IT Control Objectives for Sarbanes-Oxley

The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting

2nd Edition

September 2006

IT Governance Institute®

The IT Governance Institute (ITGI™) (*www.itgi.org*) was established in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology. Effective IT governance helps ensure that IT supports business goals, optimizes business investment in IT, and appropriately manages IT-related risks and opportunities. ITGI offers electronic resources, original research and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

Disclosure

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: *research@itgi.org*
Web site: *www.itgi*. org

ISBN 1-933284-76-5
IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition
Printed in the United States of America

Disclaimer

The IT Governance Institute, ISACA® 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, US Securities and Exchange Commission (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, which is responsible for regulating public companies, or the US Public Company Accounting Oversight Board (PCAOB), which is responsible for regulating the public accounting profession. The issues that are dealt with in this publication will continue to evolve. 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, procedures, internal controls and procedures for financial reporting that:

- Are compliant with the internal control reporting requirements of the Sarbanes-Oxley Act (the Act)
- Make the organization's plans 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.

Acknowledgments

From the publisher
The IT Governance Institute wishes to recognize:

The principal contributors
Christopher Fox, ACA
Paul Zonneveld, CISA, CA

The following contributors
Gordon Bloom, CISA, RSM McGladrey Inc., USA
Michael Cangemi, CISA, CPA, Cangemi Company LLC, USA
Nancy Cohen, CPA, AICPA, USA
Roger Debreceny, Ph.D., FCPA, University of Hawaii, USA
Robert Frelinger, CISA, Sun Microsystems Inc., USA
Kenneth S. Gabriel, CPA, KPMG LLP, USA
Michael Garber, CIA, CPA, Motorola Inc., USA
John Gimpert, CPA, Deloitte & Touche LLP, USA
John Hainaut, Jefferson Wells, USA
Hussain Hasan, CISM, CISSP, RSM McGladrey Inc., USA
Edward Hill, CIA, CPA, Protiviti, USA
Tara Janos, BP Amoco, USA
Peter Koltun, Jefferson Wells, USA
Phillip Lageschulte, CPA, KPMG LLP, USA
Elsa K. Lee, CISA, CISM, CSQA, AdvanSoft International Inc., USA
Anthony Noble, CISA, CCP, Viacom Inc., USA
Heriot Prentice, MIIA, FIIA, QiCA, The Institute of Internal Auditors, USA
Debbie Sanneman, Motorola, USA
Sheryl Skolnik, CISA, CISM, CPA, BDO Seidman LLP, USA
Tracy Stewart, CISA, CISSP, CCP, CIA, Allstate Insurance Company, USA
Doug Underwood, CPA, McGladrey & Pullen, USA
Mickey Vaja, CISA, CCNA, CISSP, Grant Thornton LLP, USA
Kenneth Vander Wal, CISA, CPA, CSP, Ernst & Young LLP, USA
Timothy Van Ryzin, CISA, CISM, Harley-Davidson, USA
Jeffrey Ward, CISA, CPA, CITP, Stone Carlie & Company LLC, USA
Margaret Yocher, United Technologies-Carrier, USA
Paul Zonneveld, CISA, CA, Deloitte & Touche LLP, Canada

The ITGI Board of Trustees

Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, International President

Georges Ataya, CISA, CISM, CISSP, Solvay Business School, Belgium, Vice President

William C. Boni, CISM, Motorola, USA, Vice President

Lucio Augusto Molina Focazzio, CISA, Colombia, Vice President

Avinash Kadam, CISA, CISM, CBCP, CISSP, Miel e-Security Pvt. Ltd., India, Vice President

Jean-Louis Leignel, MAGE Conseil, France, Vice President

Howard Nicholson, CISA, City of Salisbury, Australia, Vice President

Frank Yam, CISA, CIA, CCP, CFE, CFSA, FFA, FHKCS, FHKIoD, Focus Strategic Group, Hong Kong, Vice President

Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President,

Robert S. Roussey, CPA, University of Southern California, USA, Past International President

Ronald Saull, CSP, The Great-West Life and IGM Financial, Canada, Trustee

The IT Governance Committee

William C. Boni, CISM, Motorola, USA, Chair

Max Blecher, Virtual Alliance, South Africa

Sushil Chatterji, Singapore

Tony Hayes, FCPA, Queensland Government, Australia

Anil Jogani, CISA, FCA, Tally Solutions Limited, UK

John W. Lainhart IV, CISA, CISM, IBM, USA

Romulo Lomparte, CISA, Banco de Credito BCP, Peru

Michael Schirmbrand, Ph.D., CISA, CISM, CPA, KPMG LLP, Austria

Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada

The CobiT Steering Committee

Roger Stephen Debreceny, Ph.D., FCPA, University of Hawaii, USA, Chair

Gary S. Baker, CA, Deloitte & Touche, Canada

Rafael Eduardo Fabius, CISA, Republica AFAP, S.A., Uruguay

Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland

Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium

Jimmy Heschl, CISA, CISM, KPMG, Austria

Debbie A. Lew, CISA, Ernst & Young LLP, USA

Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia

Dirk E. Steuperaert, CISA, PricewaterhouseCoopers LLC, Belgium

Robert Ernest Stroud, CA Inc., USA

The ITGI Advisory Panel

Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Chair
Roland Bader, F. Hoffmann-La Roche AG, Switzerland
Linda Betz, IBM Corporation, USA
Jean-Pierre Corniou, Renault, France
Rob Clyde, CISM, Symantec, USA
Richard Granger, NHS Connecting for Health, UK
Howard Schmidt, CISM, R&H Security Consulting LLC, USA
Alex Siow Yuen Khong, StarHub Ltd., Singapore
Amit Yoran, Yoran Associates, USA

The ITGI Affiliates and Sponsors

ISACA chapters
American Institute for Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association of Corporate Governance
Information Security Forum
The Information Systems Security Association
Institut de la Gouvernance des Systèmes d'Information
Institute of Management Accountants
ISACA
ITGI Japan
Solvay Business School
University of Antwerp Management School
Aldion Consulting Pte. Ltd.
CA
Hewlett-Packard
IBM
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Symantec Corporation
Wolcott Systems Group
World Pass IT Solutions

Table of Contents

Executive Summary

In April 2004, the IT Governance Institute issued *IT Control Objectives for Sarbanes-Oxley* to help companies assess and enhance their internal control systems. Since that time, the publication has been used by companies around the world as a tool for evaluating information technology controls in support of Sarbanes-Oxley compliance.

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 should result in 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 result in accountability and responsiveness to business requirements. Building a strong internal control program within IT can help to:

- Gain competitive advantage through more efficient and effective operations
- Enhance risk management competencies and prioritization of initiatives
- Enhance overall IT governance
- Enhance the understanding of IT among executives
- Optimize operations with an integrated approach to security, availability and processing integrity
- Enable better business decisions by providing higher-quality, more timely information
- Contribute to the compliance of other regulatory requirements, such as privacy
- Align project initiatives with business requirements
- Prevent loss of intellectual assets and the possibility of system breach

Enhancements to the Publication With the Second Edition

Many lessons have been learned with respect to financial reporting and IT controls since the publication was issued—most significantly, the need to take a top-down, risk-based approach in Sarbanes-Oxley compliance programs to help ensure that sufficient and appropriate attention is given to areas of highest risk.

As a result, ITGI has revised the publication to provide additional IT guidance on areas of greater importance to internal control over financial reporting, as well as to share lessons learned regarding IT compliance with Sarbanes-Oxley. The second edition was exposed publicly for a 60-day period, and comments received were addressed through revisions in this final publication.

While much has been learned since the initial release of the publication, the fundamental guidance provided in April 2004 is sound. The purpose of enhancing the publication is to share lessons learned from companies and provide additional guidance on how to improve the efficiency and effectiveness of compliance using a risk-based approach. A summary of enhancements to the publication follows:

- Enhanced focus on scoping and risk assessment—Guidance has been added to assist companies in applying a top-down, risk-based approach. In particular, guidance has been added to assist in performing an IT risk assessment for Sarbanes-Oxley.
- Prioritization of controls—Guidance has been added to assist companies in defining "relevant controls." Using this guidance, certain controls in appendix C, IT General Controls, have been identified as most relevant controls.
- Managing the human element of change—Insights into cultural and people management issues have been added to highlight the human factors that need to be considered when complying with Sarbanes-Oxley.
- Enhanced guidance on application controls—Guidance has been added to assist companies in identifying and addressing various types of application controls and providing a business case for using application controls.
- Approach for spreadsheets—Guidance has been added to assist companies in addressing spreadsheets, including best practices for controls.
- Simplification of the readiness road map—Changes have been made to the readiness road map to simplify the process.
- Cross-reference to COBIT® 4.0 processes
- Lessons learned—A summary of lessons learned has been added to share the compliance experiences of companies worldwide, including steps to consider in realizing benefits or avoiding common pitfalls.
- Issues in and approach for using SAS 70 examination reports
- Enhanced guidance on segregation of duties for significant applications

Considerations for Smaller Companies

In July 2006, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued *Guidance for Smaller Public Companies Reporting on Internal Control Over Financial Reporting*. The COSO publication highlighted the challenges faced by smaller companies in complying with regulations such as Sarbanes-Oxley and provided suggestions to address these challenges.

Smaller companies may also find it difficult to address the IT control considerations that are expected under Sarbanes-Oxley. Therefore, it is important not to take a one-size-fits-all strategy, but instead to take a risk-based approach and implement only those IT controls that are necessary and relevant in the circumstances. For instance, smaller companies often use relatively simple off-the-shelf (OTS) financial applications rather than large, customizable enterprise resource planning (ERP) systems. In such cases, the risk of financial statement errors resulting from the application is typically less than that of a larger, more complex system. Accordingly, the nature and extent of controls required for the smaller company should be less than those of the larger company. While there are always exceptions to the rule, smaller companies should carefully assess their risks and implement only the controls that are necessary. To assist in this regard, enhancements have been made to the risk assessment guidance provided in this publication.

Alignment With PCAOB and CobiT

In all, 12 IT control objectives, which align to the PCAOB Auditing Standard No. 2 and *Control Objectives for Information and related Technology* (CobiT®), were defined for Sarbanes-Oxley. **Figure 1** provides a high-level mapping of the IT control objectives for Sarbanes-Oxley described in this document, IT general controls identified by the PCAOB and the CobiT 4.0 processes.

Figure 1—Mapping to PCAOB and CobiT

	CobiT	PCAOB IT General Controls			
IT Control Objectives for Sarbanes-Oxley	Mapping to CobiT 4.0 Processes	Program Development	Program Changes	Computer Operations	Access to Programs and Data
1. Acquire and maintain application software.	AI2	●	●	●	●
2. Acquire and maintain technology infrastructure.	AI3	●	●	●	
3. Enable operations.	AI4	●	●	●	●
4. Install and accredit solutions and changes.	AI7	●	●	●	●
5. Manage changes.	AI6		●		●
6. Define and manage service levels.	DS1	●	●	●	●
7. Manage third-party services.	DS2	●	●	●	●
8. Ensure systems security.	DS5			●	●
9. Manage the configuration.	DS9			●	●
10. Manage problems and incidents.	DS8, DS10			●	
11. Manage data.	DS11			●	●
12. Manage the physical environment and operations.	DS12, DS13			●	●

Using This Publication

The information contained in this document provides useful guidance and tools for companies trying to prepare and sustain their IT organizations relative to Sarbanes-Oxley compliance. **However, each organization should carefully consider the appropriate IT control objectives necessary for its own circumstances. Organizations may choose not to include all the control objectives discussed in this document, and, similarly, they may choose to include others not discussed in this document.** In either case, it is expected that changes to the description of control objectives, illustrative controls and illustrative tests of controls provided in this document will be necessary to reflect the specific circumstances of each organization.

The Foundation for Reliable Financial Reporting

A Need for IT Control Guidance

In today's environment, financial reporting processes are driven by IT systems. Such systems, whether ERP or otherwise, are deeply integrated in initiating, authorizing, recording, processing and reporting 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.

Much has been written on the importance of the Sarbanes-Oxley Act and internal controls in general; however, little exists on the significant role that information technology plays in this area. For instance, the Sarbanes-Oxley Act requires organizations to select and implement a suitable internal control framework. COSO's *Internal Control—Integrated Framework* has become the most commonly used framework by companies complying with Sarbanes-Oxley; however, COSO does not provide a great deal of guidance to assist companies in the design and implementation of IT controls.

As a result, organizations need guidance to address IT components as they relate to the overall financial reporting compliance program. This document is intended to assist in this regard, using relevant SEC, PCAOB COSO, and CobiT content. See appendix B for further discussion about COSO and CobiT.

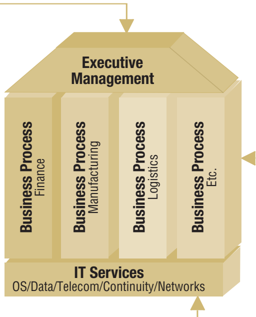
Where to Find IT Controls

In understanding where IT controls exist within the typical company, consideration of at least three elements should be given: executive management, business process and IT services.
Figure 2 illustrates the common elements of organizations.

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.	IT services form the foundation for operations and are provided across the organization, rather than segregated by business process or business unit. IT services commonly include network management, database management, operating system management, storage management, facilities management and security administration, and are often managed by a central IT function.

More and more, IT systems are automating business processes. In doing so, these systems often replace manual control activities with automated or IT-dependent control activities. As a result, compliance programs need to consider system-based controls to keep pace with changes in business processes and new system functionality.

Figure 2—Common Elements of Organizations


Executive Management
Business Process Finance
Business Process Manufacturing
Business Process Logistics
Business Process Etc.
IT Services
OS/Data/Telecom/Continuity/Networks

Entity-level Controls

Entity-level controls set the tone and culture of the organization. IT entity-level controls are part of a company's overall control environment.

Controls include:
- Strategies and plans
- Policies and procedures
- Risk assessment activities
- Training and education
- Quality assurance
- Internal audit

Application Controls

Controls embedded within business process applications directly support financial control objectives. Such controls can be found in most financial applications including large systems such as SAP and Oracle as well as smaller OTS systems such as ACCPAC.

Control objectives/assertions include:
- Completeness
- Accuracy
- Existence/authorization
- Presentation/disclosure

IT General Controls

Controls embedded within IT processes that provide a reliable operating environment and support the effective operation of application controls

Controls include:
- Program development
- Program changes
- Access to programs and data
- Computer operations

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 is 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 determine whether IT monitoring controls, general controls and application controls exist and support the objectives of the compliance effort. Some of the important areas of responsibility for IT include:

- Understanding the organization's internal control program and its financial reporting process
- Mapping the IT environment (IT services and processes) that supports 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 and systems-based 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
- Participating in the Sarbanes-Oxley project management office

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

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

Performing a thorough review of IT control processes and documenting them as the enterprise moves forward can be a time-consuming task. The review of application and IT processes will be driven by the risk of the business processes and environments. Without appropriate knowledge and guidance, organizations 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 are in the process of a change in culture. Enhancements to IT systems and processes have been required, most notably in the design, documentation, retention of control evidence and evaluation of IT controls.

PCAOB Guidance for IT Controls

PCAOB Auditing Standard No. 2 discusses the relationship of IT and internal control over financial reporting and emphasizes the importance of identifying IT controls and testing their design and operational effectiveness. 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;*

Controls Over IT Systems

With widespread reliance on IT systems, controls are needed over 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 systems that have been determined to be financially significant.

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, and IT policies, procedures and standards. Monitoring and reporting are required to align IT with business requirements.

The IT governance structure should be designed so that IT adds value to the business and 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 operations 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 if someone accesses these powerful data-altering functions, at least that individual's 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 designed well, 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 have two principal components: the acquisition and implementation of new applications and the maintenance of existing applications.

The acquisition and implementation process for new applications tends to result in 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 so that all changes 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 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.

Managing the Human Element of Change

Implementing controls for Sarbanes-Oxley, where few existed before, has become a significant challenge for most organizations. In many cases, the finance organization within a company has been familiar with the need for controls and related documentation because they have been part of financial audits for years. However, IT organizations are less accustomed to these issues and, therefore, implementing controls that operate effectively over time has proven to be a difficult task.

To successfully implement and sustain controls, IT organizations first need to understand that compliance with Sarbanes-Oxley will likely involve change in current practices. Similarly, IT organizations should recognize that change is more than a process—it has significant cultural and personal undertones that need to be taken into consideration to be successful. Therefore, companies must have a strategy for change that reflects the cultural preferences and capability of its people. Change does not just happen—it has to be managed.

Committing to Change

The first step in managing change is obtaining commitment. In seeking this commitment, an organization needs to define what it wants to change and what it should look like after it has changed. Building a vision for the future state allows for commitment to take place. Companies also need to understand how change can be effected within their organizations. For instance, is change best accomplished through a top-down or bottom-up approach? Understanding these issues is important to obtaining commitment.

Assessing the Current State

Successful change management starts with an honest assessment of the current state. The current state refers to the readiness of the organization to embrace change. Consider the following factors in assessing the current state:

- Culture—The probability of successful change is most likely to be affected by an organization's culture. That is, if an organization is accustomed to a flexible, entrepreneurial style, then change is already part of its culture and will be met with acceptance. If the culture is stoic or rigid, then change will be more difficult.
- Extent of change—The more significant the change, the less likely that success will result. Organizations need to assess the extent of change they are trying to accomplish and be realistic with their goals.
- Impact on people—With every change, there are people who perceive it positively and negatively and it is important to understand how people will be impacted. Those who see change positively are often "change agents" and those who see it negatively are often "obstacles", so identifying the change agents early and engaging them in the process will be a key success factor. Similarly, if there is a high proportion of obstacles, organizations may need to rethink how change can be introduced into the organization.

- Bench strength—The ability of an organization to adapt to change is often proportionate to its skills and experience. If change requires significant retraining or modification in skill set, then, to be successful, training investments need to be made.

Overcoming the Obstacles

As part of the process of assessing its current state, an organization identifies the relevant obstacles to change. It then needs to implement a strategy to overcome them. For instance, evolving an organization toward Sarbanes-Oxley compliance requires the design and implementation of controls, which some may perceive as impediments to "getting the job done." However, if designed and communicated properly, these controls can be implemented to enhance business process efficiency and effectiveness, resulting in improved business performance.

In overcoming the obstacles, there are important lessons to be learned from companies that have already been through this process, as follows:

1. Communicate—Effective communication is more than just providing regular updates. Organizations are naturally resistant to change, and people need to understand the purpose of change and the benefits of it. Some suggestions in this regard are:
   – Understand the "pain points". Figure out what could negatively impact an individual or the organization as a whole and make sure the communication clearly describes how the change will reduce the pain. There are many pain points within Sarbanes-Oxley, the most significant of which is failing to meet the requirements of the Sarbanes-Oxley Act. Once people understand how this affects them, they will be much more willing to embrace the changes associated with compliance.
   – Determine the best medium for communicating. Newsletters, e-mail, workshops and lunch-and-learns are all good examples of communication, and in most cases more than one type is required to get the message across. Sarbanes-Oxley projects are long and complicated, so regular communication is important.
   – Obtain feedback. It is just as important to collect and analyze feedback as it is to communicate. Feedback allows organizations to show flexibility and adaptability, demonstrating that they are listening. One of the biggest reasons change is not successful is because organizations do not listen. There are many ways to meet the requirements of Sarbanes-Oxley, and companies would be surprised to see the excitement that is generated when people's feedback is sought and implemented.
2. Train—If companies want to evolve, it is important to give people the skills they need to get there. Training requirements should be identified for each affected employee, and plans should be implemented to deliver this training. The requirements of Sarbanes-Oxley are complicated and the wide variety of opinions on what constitutes the right amount of work suggests that training and education are essential for a successful project.

For instance, training is particularly important in understanding how general computer controls relate to application controls, as well as many other areas addressed in this publication.

3. Motivate—Change is most successful when incentives are used. Incentives provide a productive and goal-oriented approach for making change happen, and the result is often a win-win for the company and its people. For instance, consider building Sarbanes-Oxley compliance objectives into the performance evaluation process of every employee, and be as specific as possible in defining these objectives so they are relevant to the roles and responsibilities of each individual.

Setting the Ground Rules

COSO Defined

Historically, assertions on control by an organization have been mostly voluntary and based on a wide variety of internal control frameworks. 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. Specifically, the SEC referred to COSO.[1]

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 and its implications for IT.

Applying COSO to IT

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. To emphasize this point, refer to the guidance provided in PCAOB Auditing Standard No. 2:

> *Known as the COSO report, it provides a suitable and available framework for purposes of management's assessment. For that reason, the performance and reporting directions in this standard are based on the COSO framework. Other suitable frameworks have been published in other countries and may be developed in the future. Such other suitable frameworks may be used in an audit of internal control over financial reporting. Although different frameworks may not contain exactly the same elements as COSO, they should have elements that encompass, in general, all the themes in COSO.*

[1] Committee of Sponsoring Organizations of the Treadway Commission, *www.coso.org*

For Sarbanes-Oxley compliance efforts, it is important to demonstrate how IT controls support the COSO framework. An organization should have IT control competency in all five of the components COSO identifies as essential for effective internal control. They are:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

Each of the five is described briefly in the following subsections. Following the description are high-level IT considerations as they relate to the specific component. More detailed IT control objectives are included in the appendices as 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 entity 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 in 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 management's identification and analysis of relevant risks to achieving 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 entity level (for the overall organization) or at the activity level (for a specific process or business unit).

At the entity 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 so 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 so 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 across all layers of systems, operating system, database and application
- 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 configured appropriately, or used in combination with other manual controls, application controls support the completeness, accuracy, authorization and existence of processing transactions. Additional guidance regarding application controls is provided in appendix D.

General controls are needed to support the functioning of application controls, and both are needed to support 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 entity 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.

Increasingly, IT performance and effectiveness are being continuously 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 those 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 should result in a reduction of the unavailability of relevant systems if applications and IT infrastructure components have been compromised.

At the entity 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 entity 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

IT Compliance Road Map

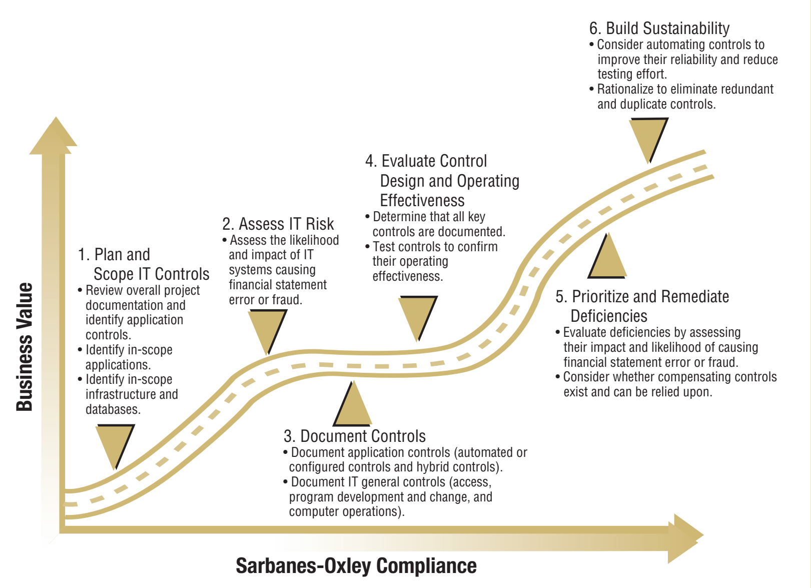
The following section provides a compliance road map that is tailored to the specific objectives and responsibilities of IT departments. The road map has been simplified from the version included in the initial publication, to make the implementation process easier to manage and to focus efforts on activities that are most important to Sarbanes-Oxley 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.

Sarbanes-Oxley Compliance

The compliance road map, illustrated in **figure 3**, provides direction for IT professionals on meeting the challenges of the Sarbanes-Oxley Act. The first two steps of the road map—plan and scope IT controls and assess IT risk—should be conducted in tandem.

Figure 3—IT Compliance Road Map


6. Build Sustainability
• Consider automating controls to improve their reliability and reduce testing effort.
• Rationalize to eliminate redundant and duplicate controls.
4. Evaluate Control Design and Operating Effectiveness
• Determine that all key controls are documented.
• Test controls to confirm their operating effectiveness.
2. Assess IT Risk
• Assess the likelihood and impact of IT systems causing financial statement error or fraud.
1. Plan and Scope IT Controls
• Review overall project documentation and identify application controls.
• Identify in-scope applications.
• Identify in-scope infrastructure and databases.
Business Value
5. Prioritize and Remediate Deficiencies
• Evaluate deficiencies by assessing their impact and likelihood of causing financial statement error or fraud.
• Consider whether compensating controls exist and can be relied upon.
3. Document Controls
• Document application controls (automated or configured controls and hybrid controls).
• Document IT general controls (access, program development and change, and computer operations).
Sarbanes-Oxley Compliance

1. Plan and Scope IT Controls

Like all significant projects, careful attention should be given to properly scoping and planning the IT compliance program. Scoping is the process of understanding which IT applications and related subsystems should be included in the project and which applications and subsystems can be excluded, working with and using the findings of the financial/business team. The inclusion and exclusion of systems will be based on the results of the overall financial risk assessment process of the organization, which is led by the financial/business compliance team. In other words, only those applications and related subsystems that support business and relevant controls over financial reporting should be included in scope. Conversely, planning is the process of developing a time schedule of activities whereby tasks are assigned to people and progress can be monitored.

Assign Accountability and Responsibility

An important first step in the IT control compliance program is to form an IT control subcommittee. The subcommittee should be integrated into, and report to, the overall Sarbanes-Oxley steering committee. It should oversee the IT Sarbanes-Oxley compliance process, facilitate communication and integration with the overall Sarbanes-Oxley project, and facilitate the role of the independent auditors in the Sarbanes-Oxley IT process. Smaller organizations may be able to redeploy, on a part-time basis, existing staff; however, larger organizations may need dedicated full-time personnel. The subcommittee should assign an IT controls lead who is responsible for the project and is given appropriate authority and accountability for completing the project.

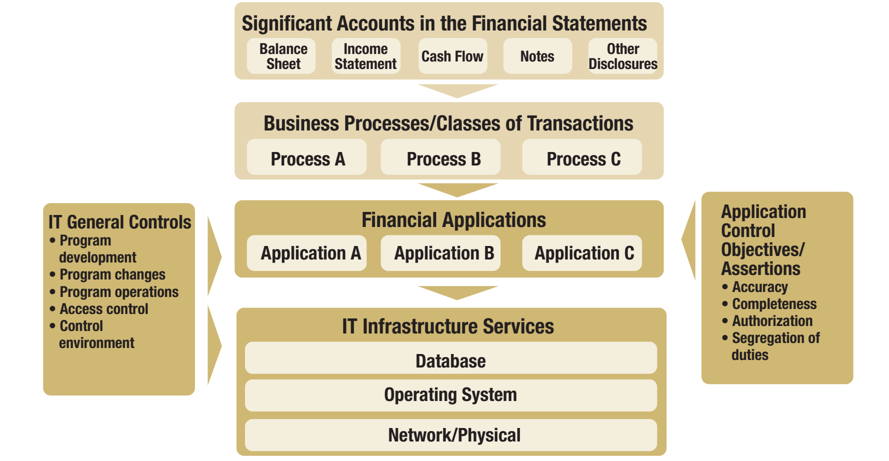
Inventory Relevant Applications and Related Subsystems

Working with the financial/business controls team, an inventory of in-scope applications (Sarbanes-Oxley applications and related subsystems) should be developed by identifying the applications that support relevant application controls, as shown in **figure 4**. Typically, applications that support online authorizations, complex calculations or valuations, or are responsible for maintaining the integrity of significant account balances, such as inventory, fixed assets or loan balances, should be identified in this phase. Appendix D, Application Controls, provides guidance on the definition of application controls and examples of where they may exist within a company when working with the financial/business controls team.

By having an inventory of applications, as well as the IT processes that manage and drive the applications, the IT control project team will be able to identify all applications that need to be considered and identify all subsystems that support the applications, including databases, servers, operating systems and networks (see appendix E, Sample Application and Technology Layers Inventory, for an example of an inventory spreadsheet of relevant applications and subsystems).

This step in the project will also help the IT organization gain an understanding of how the financial reporting process works and identify where technology is critical in the support of the process.

Figure 4—Scoping the IT Control Project—Top Down



The inventory of applications and related subsystems should be used for preliminary planning purposes, and will be assessed for risk in the following phase to determine the nature and extent of controls and testing required.

Review Financial Process Documentation and Identify Application Controls
Organizations have many business processes and controls; however, compliance with Sarbanes-Oxley is limited to those processes and controls that support financial reporting. Consequently, it is important that the IT compliance team participate in the identification of application controls. There are two common approaches to do this—organizations can either have the IT controls team support the financial/business controls team in the identification of application controls, or organizations can have the financial/business controls team identify all controls first, and then the IT controls team can review them to identify which of these controls is dependent on IT. It does not matter which approach is used, as long as organizations properly identify which controls have IT dependencies. In doing so, organizations are able to properly plan the IT controls project, limiting scope to application controls that support financial reporting objectives.

Develop a Preliminary Project Plan and Obtain Approval
Using the inventory of in-scope applications and subsystems, a preliminary project plan of activities should be developed using the six phases described in **figure 3**. The project plan will be modified and refined later, but it is important to get an overall view of the project's size and approach. In developing the plan, the time required for each phase can be estimated using the project estimating tool in appendix F.

Once the plan is developed, it is important to discuss with the financial/business controls compliance team the in-scope applications and appropriateness of the project's scope. Once this is complete, it is time to obtain approval to proceed with the project. Obtaining formal approval is very important given the significance of the project and the impact it will have on various members of the organization. Formal approval will solidify the sponsors of the project and allow one to obtain buy-in from all relevant stakeholders and staff members that need to participate.

Determine Responsibility for Application Controls

One of the common areas of confusion for IT control projects has been "who is responsible for application controls?" The lack of clarification of this responsibility has led to significant duplication of effort, unnecessary testing of duplicative relevant controls and the risk that a relevant control may not be tested because both the financial and IT teams have assumed that the other team is addressing the issue. It is suggested that business owners are responsible for business-process-specific application controls. The responsibility of the IT organization is to assist the process owners in identifying and testing these controls, while ensuring that the general application controls (access restrictions, change controls, backup recovery, etc.) are in place and reliable.

Consider Multilocation Issues

Among the many factors that should be considered in scoping the IT control project are companies with decentralized operations or companies with operations that span geographical boundaries. Such companies need to determine if their IT operations in each geographical location operate within a single control environment or multiple control environments. Single control environments typically have one leadership structure, while multilocation environments typically have multiple leadership structures. Generally speaking, multilocation environments, when significant, have to be treated separately and, therefore, result in a larger project and more work.

Consider Whether Applications Can Be Eliminated From Scope

The fact that an application is included in scope indicates that it supports a relevant application or hybrid control required for Sarbanes-Oxley compliance. In most cases, the application and its related subsystems will have to be assessed. However, if the application supports a very limited number of application controls (e.g., just one control), then consideration could be given to eliminating the application control (and therefore the application itself) and either identifying a relevant manual control or increasing reliance on existing manual controls to reduce overall effort. While this is rare, it is a consideration for companies that have many applications that support very few controls. Care should be taken to ensure that inadvertent reliance does not occur in these situations (e.g., relying on a system-generated report). This is a decision/issue on which the organization's overall Sarbanes-Oxley steering committee needs to be focused. This is not an IT dependent issue.

Identify Dependencies on Third-party Service Organizations (Outsourcing)
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. Therefore, 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 Statement on Auditing Standards (SAS) 70 reports 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 independent auditors and understand the specific requirements. Particular attention should be paid to the period covered by the SAS 70 and to whether the controls in the SAS 70 cover the environment, platforms and applications utilized by the company as well as the testing results and overall opinion. Appendix L, Issues in Using SAS 70 Examination Reports, contains a more in-depth discussion on evaluating the sufficiency of a SAS 70 report.

2. Assess IT Risk
At this point, organizations need to assess risks within the IT processes and layers that support the applications in scope. One of the most significant lessons learned through the initial years of Sarbanes-Oxley compliance projects is that the project needs to be risk-based. Not all IT systems or processes pose a high risk to the financial statements and, therefore, not all IT systems or processes need to be included or evaluated to the same extent. In performing a risk assessment, consideration needs to be given to inherent risk rather than residual risk (the risk left over after considering the impact of controls). A number of tools have been provided in appendix F, Project Estimating Tool, to assist in the risk assessment process.

Assess the Inherent Risk of Applications and Related Subsystems

Assessing inherent risk of applications and their related subsystems, such as databases, operating systems, networks and physical environments, is necessary to determine the nature and extent of controls needed to manage such risks. It is also necessary to understand application and related subsystem inherent risk to properly plan and perform testing of operating effectiveness of such controls.

In performing an inherent risk assessment, consideration should be given to a number of risk factors; however, the final assessment is judgmental. The purpose of considering common risk factors is to provide companies with relevant information so that a fair and reasonable risk assessment can be made. In performing the risk assessment, both the probability and impact of the risk event should be taken into consideration. For example, without access controls, there is a risk that someone could access the primary financial application and enter false transactions into the system. Without controls, the likelihood of this happening is not entirely remote and the impact of entering false transactions is significant. As a result, this risk is considered significant and controls are required to reduce the risk. It is important to note that the objective is to reduce risk to a reasonable level, rather than eliminate risk altogether.

The following factors are commonly used in performing the risk assessment, but companies should determine if others need to be added based on their unique circumstances (see appendix G, Inherent Risk Assessment and Control Prioritization Grid, for additional guidance):

- Nature of technology (complex or simple)
- Nature of people (experienced or inexperienced)
- Nature of processes (centralized or decentralized)
- Past experience
- Significance to the financial reports

Once a risk assessment has been performed, its results can assist in determining the nature and extent of controls and testing required. Appendix C, IT General Controls, provides guidance on the recommended IT controls that should be considered for applications and related subsystems (collectively referred to as the “technology layers”). As noted in the matrix provided in appendix G, the risk assessment will allow for the exclusion of certain IT control processes simply because the probability or impact of events related to that technology layer is not sufficient to warrant any work. Regardless of the outcome, documentation of the decisions made and rationale for such decisions should be maintained for discussion with management or the external auditors.

Refine Scope and Update the Project Plan
Once a risk assessment has been performed, the IT controls team should be in a position to refine the project scope and update which applications and related subsystems may be excluded from scope. The risk assessment process and related conclusions should be clearly documented, particularly where systems are excluded from scope. Similarly, the project plan should be updated where changes to scope and the extent of effort is modified to reflect a risk-based approach.

3. Document Controls

Documenting controls illustrates to management how risks associated with reliable financial reporting have been addressed and enables management to make informed decisions regarding the acceptability of the remaining level of risk. For example, if financial applications are heavily relied upon for complex calculations, then there is a risk that unauthorized changes could result in material errors in the financial statements. As a result, it is critical to identify and document controls that prevent this from occurring or detect its occurrence.

Identify IT Entity-level Controls
Entity-level controls are reflected in the operating style of an organization. They include policies, procedures and other high-level practices that set the tone for the organization. Entity-level controls are a fundamental component of the COSO model and should take into consideration IT operations that support financial reporting. Identification of IT entity-level controls should be integrated into the overall entity-level assessment performed for the company. The existence of strong IT entity-level controls, such as well-defined and communicated policies and procedures, often suggests a more reliable IT operating environment. Similarly, organizations with weak IT entity-level controls are more likely to experience difficulty in consistently performing control activities, such as change management and access control. As a result, the relative strength or weakness of entity-level controls will impact the nature, extent and timing of testing activities.

Identify Application Controls
Identification of application controls that support financial reporting is a critical step in the process. Once all application controls have been identified, their supporting IT general controls can be identified as well. Most often, application controls are included in the business process documentation. Ideally, IT specialists document a process with a controls specialist and together they may identify the relevant controls for the process. However, in many cases, the process documentation has already been created. Therefore, someone has to review this documentation and identify the application controls. Appendix D, Application Controls, provides additional guidance on the identification of application controls.

Identifying automated controls may seem trivial, but in many cases, it is not. Two types of application controls are commonly used by companies and need to be documented:

- Automated controls—Performed by computers and binary in nature, they function as designed and are not subject to intermittent error. Examples include input edit checks to validate order quantities, or configured controls in automated purchasing systems to allow orders only up to preconfigured limits.
- IT-dependent manual controls (hybrid)—These are essentially manual controls that are dependent on IT systems.

IT application controls are becoming more important as the timing of error detection and the cost efficiency of controls receive more attention. For example, whereas years ago it may have been acceptable to wait several weeks for a manual reconciliation to detect an error or fraud, such a delay is becoming increasingly less acceptable. Therefore, manual controls unsupported by an automated process may no longer be tolerable. Further guidance, including examples of application controls, is provided in appendix D, Application Controls.

Hybrid controls, in particular, have not been well documented by many companies despite the emphasis provided by the PCAOB in its November 2004 guidance:

> *Application controls also may be manual controls that are dependent on IT (for example, the review by an inventory manager of an exception report when the exception report is generated by IT). Although IT general control deficiencies do not result in financial statement misstatements directly, an associated ineffective application control may lead to misstatements. Therefore, the significance of an IT general control deficiency should be evaluated in relation to its effect on application controls, that is, whether the associated application controls are ineffective.*

Identify IT General Controls

The relationship between application controls and IT general controls is such that IT general controls are needed to support the reliability of application controls. For example, ensuring database security is often considered a requirement for reliable financial reporting. Without security at the database level, companies would be exposed to unauthorized changes to financial data.

The challenge with IT general controls is that they rarely impact the financial statements directly. Rather, the PCAOB describes IT general controls as having a “pervasive” effect over all internal controls. That is, if a relevant IT general control fails (e.g., a control restricting access to programs and data), it has a pervasive impact on all systems that rely on it, including financial applications. As a result, without being assured that only authorized users have access to financial applications, companies are unable to conclude that only authorized users initiated and approved transactions.

Identify Which Controls Are Relevant Controls

Financial risks are not all equal in likelihood and materiality. Similarly, financial controls are also not the same in their effectiveness in mitigating identified risks. Furthermore, management is not required to evaluate all control activities related to a risk. As a result, companies should endeavor to limit their documentation of controls to relevant controls.

The question most companies ask is “what is a relevant control?” Unfortunately, there is no authoritative definition for relevant controls, despite the fact that the term is used ubiquitously. While they may sound elusive, relevant controls are those that companies choose to rely on to meet a control objective—they are the controls that provide the most assurance to the control owners that the financial control objective was met.

When judging whether a control is relevant, companies should consider the following:

- Relevant controls commonly include policies, procedures, practices and an organization structure that are essential for management to mitigate significant risks and achieve the related control objective.
- Relevant controls often support more than one control objective. For instance, access controls support the existence of financial transactions, valuation of financial accounts, segregation of duties, and more. In most cases, a combination of relevant controls is an effective way to achieve a particular objective or series of objectives. Placing too much reliance on a single control could create a single point of failure for the compliance program.
- Controls that directly address significant risks (or directly achieve objectives) are often relevant. For example, the risk of unauthorized access is a significant risk for most companies; therefore, security controls that prevent or detect unauthorized access are relevant.
- Preventive controls are typically more effective than detective controls. For example, preventing a fraud from occurring is far better than simply detecting it after the fact. Therefore, preventive fraud controls are often considered relevant.
- Automated controls are more reliable than manual controls. For example, automated controls that force periodic password changes by users are more reliable than generic policies that have no enforcement. Manual processes are also subject to human error.

In appendix C, IT General Controls, a listing of IT general controls has been provided as a illustrative guide for preparing IT organizations for Sarbanes-Oxley compliance. Within these lists, certain controls are highlighted as “most relevant” controls, indicating that they are the most commonly used in designing a reliable and robust IT general control environment.

Consider IT-based Antifraud Controls

The importance of antifraud controls under Sarbanes-Oxley is something that cannot be overstated. Fraud is the principal reason for introducing Sarbanes-Oxley in the first place, so sufficient and appropriate attention should be given to this issue.

Information technology plays a significant role in the prevention and detection of fraud, as many antifraud controls rely on IT systems. The following examples of IT-based antifraud controls should be considered for inclusion for a company's compliance program:

- Application-enforced segregation of duties—Most systems have the ability to define what privileges are assigned to users within the application. As a result, the system enforces appropriate approvals for transaction processing and prevents users from initiating and authorizing their own transactions.
- Access controls—Most systems have privileged users who can access sensitive information, such as payroll data, allowing them to add fictitious employees and thereby commit fraud. Limiting such access to a few people and making sure that the financial reporting team does not have this access is important to establishing internal control over financial reporting.

Control Documentation

Under the Sarbanes-Oxley Act, companies are required to document controls over financial reporting and perform an assessment of their design and operating effectiveness. Documentation may take various forms, including entity policy manuals, IT policies and procedures, narratives, flowcharts, decision tables, procedural write-ups, or completed questionnaires. No single particular form of documentation is mandated by Sarbanes-Oxley, and the extent of documentation may vary, depending upon the size and complexity of the organization.

For most organizations, documentation of IT controls should include the following:

- Entity level
  - Assessment of entity-level controls including evidence to support the responses and opinions of management
- Activity level
  - Description of the processes and related subprocesses (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. This should include the type of controls (preventive or detective) and the frequency they are performed.
- 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

4. Evaluate Control Design and Operating Effectiveness

Evaluate Control Design

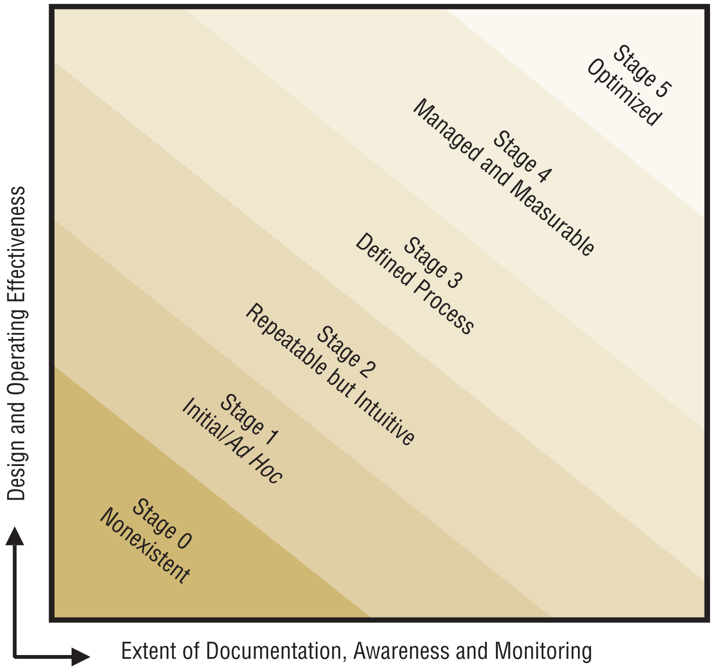
Control design causes an IT organization to step back and evaluate the ability of its control program to reduce IT risk to an acceptable level. More specifically, it forces management to evaluate the appropriateness of control attributes, including preventive, detective, automated and manual, when concluding on control design. 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 will prevent this from occurring. In this example, a detective control that identifies unauthorized programs in production after the fact may not be appropriate.

Control design in the overall IT control environment cannot be overstated. 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 IT general controls). Accordingly, the evaluation of control design is an essential step in evaluating the IT control environment.

To help in this process, consider the IT control design and effectiveness model in **figure 5**. 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 5 demonstrates the stages of control reliability that may exist within organizations. For the purposes of establishing internal control, it is important to note that the higher stages provide a more reliable control environment and the lower stages are less reliable. While there is no specific stage required by Sarbanes-Oxley other than a requirement for controls to be documented and tested, organizations should carefully consider at which stage (maturity) they are currently and whether this presents a risk to compliance.

Figure 5—Stages of Control Reliability



The table presented in **figure 6** provides insight into the various characteristics of each stage as well as the related implications. IT organizations should 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.

As discussed earlier, to provide a basis to support management's assertion regarding the adequacy of control design, management needs to document its evaluation of control design. Management's documentation of its evaluation of control design should be sufficiently detailed for the external auditor to review the design, perform a walk-through and test the effectiveness of a control. The external auditor should be able to understand management's evaluation of control design with sufficient detail to reperform the test of design. Generally, it is not sufficient to provide policies and manuals without providing a reconciliation to the design evaluation process.

Figure 6—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 that there is an issue to be addressed; therefore, no communication about the issue is generated.	There is some evidence that 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 and is adequately documented and monitored, but it is 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.
Sarbanes-Oxley Implications	The organization has a total inability to be in compliance at even the minimum level.	Insufficient controls, policies, procedures and documentation exist to 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 design and effectiveness should be tested. 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 test the design and operating effectiveness of the control activities.

Although there are many factors that go into selecting sample sizes (e.g., other controls being tested, expected error rate), **figure 7** represents a common (minimum) sample selection methodology used by companies and auditors to test the operating effectiveness of controls. For IT general controls, the sample size selected will correspond with the frequency of control operation.

Figure 7—Guidance for Sample Size Selection[2, 3]

Nature of Control	Frequency of Performance	Minimum Sample Size
Manual	Many times per day	25
Manual	Daily	25
Manual	Weekly	5
Manual	Monthly	2
Manual	Quarterly	2
Manual	Annually	1
Automated	Test one application of each programmed control activity (assumes IT general controls are effective).	
IT general controls	Follow the guidance above for manual and programmed aspects of IT general controls.	

Management needs to document its tests of operating effectiveness and conclusions on whether the relevant controls evaluated by management are operating as designed. Similar to management's documentation of its evaluation of control design, management needs to document its evaluation of operational effectiveness in sufficient detail for external auditors to reperform the operational effectiveness tests performed by management.

In addition to the information documented in the control design evaluation, the documentation of operational effectiveness may include the following information:

- Nature, timing and extent of test steps performed
- Results from testing
- Individual who performed the test and the date performed
- Sample size and test population
- Reference/location of supporting documentation

[2] Further guidance can be found in SAS 39 Audit Sampling.

[3] Assumes control operating efficiency

- Conclusion on operational effectiveness
- Exceptions identified and related remediation plans and/or compensating controls

Consider the Nature of Evidence Required
Auditing Standard No. 2 describes different forms of evidence that can be obtained in testing the design and operating effectiveness of controls. In principle, registrants are expected to obtain a mix of inquiries of appropriate personnel, inspection of relevant documentation, observation of the company's operations, and reperformance of the application of the control. Forms of evidence include:

a) Inquiry—Inquiry is a procedure that consists of seeking information of knowledgeable persons throughout the company. For most organizations, inquiry is used extensively and is often complemented by performing other procedures.
b) Inspection of Documentation—Because inquiry alone does not provide sufficient evidence to support the design or operating effectiveness of a control, additional tests should be performed. To obtain sufficient evidence about the operating effectiveness of the control, organizations should corroborate inquiries by performing other procedures, such as inspecting reports or other documentation used in performance of the control.
c) Observation—In circumstances in which documentary evidence of controls or the performance of controls does not exist and is not expected to exist, organizations should corroborate inquiries of appropriate personnel with observation of company activities.
d) Reperformance—In circumstances where the quality of evidence regarding the design or effective operation of controls might not be sufficiently persuasive, organizations may choose to reperform the control and independently run the exception report and investigate exceptions. For example, the signature on an exception report may not be sufficient to demonstrate that all exceptions have been investigated. If this is the case, organizations may chose to reperform the control and, independently run the exception report and investigate exceptions.

Consider the Timing of Control Testing
Organizations should perform tests of controls over a period of time that is adequate to determine whether, as of the date specified in management's report, the controls necessary for achieving the objectives of the control criteria are operating effectively. The period of time over which organizations performs tests of controls varies with the nature of the controls being tested and with the frequency with which specific controls operate and specific policies are applied. Some controls operate continuously (for example, approval of user access requests), while others operate only at certain times (for example, periodic review of user access lists). Generally speaking, organizations should perform testing at the time controls are operating.

Roll-forward Testing

For many organizations, testing of IT controls is performed at an interim date (prior to year end). When organizations test controls at an interim date, they should determine what additional evidence to obtain concerning the operation of the control for the remaining period. In making that determination, organizations should consider:

- The specific controls tested prior to the "as of" date and the results of those tests
- The degree to which evidence about the operating effectiveness of those controls was obtained
- The length of the remaining period
- The possibility that there have been any significant changes in internal control over financial reporting subsequent to the interim date

5. Prioritize and Remediate Deficiencies

Consider Guidance From the SEC and PCAOB

In November 2004, the PCAOB issued guidance suggesting that IT general control deficiencies in the absence of an application control deficiency could be classified as only a control deficiency. However, the PCAOB goes on to describe three conditions under which an IT general control deficiency could result in more than a deficiency and could perhaps be a "material weakness." They are as follows:

- Application-level deficiencies—The significance of an IT general control deficiency should be evaluated in relation to its effect on application controls, that is, whether the associated application controls are ineffective. If the application deficiency is caused by the IT general control, then they are treated the same. For example, if an application-based tax calculation is materially wrong and was caused by poor change controls to tax tables, then the application-based control (calculation) and the general control (changes) could be classified as material weaknesses.
- Control environment deficiencies—After an IT general control deficiency has been evaluated in relation to its effect on application controls, it also should be evaluated when aggregated with other control deficiencies. Take, for example, management's decision not to correct an IT general control deficiency and its associated reflection on the control environment; when aggregated with other deficiencies affecting the control environment, it could lead to the conclusion that a significant deficiency or material weakness in the control environment exists.
- Failing to remediate a deficiency for an unreasonable period of time—Based on the directions in the PCAOB Auditing Standard No. 2, the auditor could determine that a prudent official in the conduct of his/her own affairs would conclude that the IT general control deficiency, by itself, was a significant deficiency. In this manner, an IT general control deficiency that has been communicated to management and the audit committee yet remains uncorrected after some reasonable period of time is a strong indicator of a material weakness.

Identify and Assess IT General Control Deficiencies
All deficiencies, including IT deficiencies, should be reviewed with the financial compliance team and evaluated as part of the overall internal control certification. IT control deficiencies should not be evaluated in isolation. Similarly, application controls that directly support the financial statement control objectives also need to be reviewed and evaluated with the financial compliance team.

The general guidance for evaluation of IT general control deficiencies provided in appendix H, Sample Control Documentation and Testing Template, provides an example of a deficiency evaluation decision tree to assist companies in their preliminary analysis of control deficiencies. However, this is only a preliminary analysis and additional review and conclusion need to be performed by the overall financial compliance team.

Generally speaking, there are two types of deficiencies that companies will have to address:

1. Design deficiencies—These are issues related to missing controls, inadequate controls, lack of supporting documentation or other flaws in control design that do not sufficiently mitigate the related risk.
2. Operating effectiveness deficiencies—These are issues relating to the consistency with which controls are operating, such as not performing a control as designed consistently throughout the year.

Consider the Aggregate Effect of Deficiencies
In some cases, individual control deficiencies may be considered insignificant, yet when combined with other similar deficiencies, the combined effect may be more significant. For example, an organization that does not perform a periodic review of user access lists to its financial application would normally be considered to have a control design deficiency. On its own, it may not be significant, especially if other compensating controls exist. However, if this organization also failed to properly authorize user access requests for the same application, then the aggregate effect of the two deficiencies may result in a significant deficiency or material weakness. In other words, the combined effect of control deficiencies related to user access requests and user access reviews could place into question the validity of users' access within the financial application and, therefore, place into question the validity of transactions within the system as well.

Remediate Control Deficiencies
The remediation phase of most projects is where significant effort and money is spent. In some cases, there may be short-term options for remediation that may not be expensive to implement and can be implemented quickly, but may cost more to operate. For instance, the manual process for adding, changing and deleting users in systems is time-consuming and slow. However, if a company needs a quick solution, the

manual approval and entry approach is often the most time-sensitive solution. However, a longer-term solution might include process automation that restricts user access provisioning without appropriate authorization. This approach will definitely cost more in the near term, but tends to be far more reliable and cost-effective in the long term.

6. Build Sustainability

At this point, IT management should be in a position to assess the IT internal control program effectiveness. Effective internal controls, control assessment and management competencies should become part of the IT department's organization and culture and sustain themselves over the long term. Control is not an event; it is a process that requires continuous support and evaluation to stay current. The ultimate objective is to convert the IT control project into a process. The following activities should be considered to achieve this:

- Performing a postimplementation review of the Sarbanes-Oxley project, identifying what went right and areas for improvement
- Reviewing recent SEC and PCAOB guidance and speeches to determine if changes in interpretation could impact the future approach
- Reviewing other independent material for suggestions and opportunities to improve the approach
- Meeting with peers in other organizations to discuss potential improvements to the process
- Assessing longer-term solutions to address Sarbanes-Oxley issues, such as automation of processes and implementation of program change control software
- Developing a preliminary plan and timetable for the following year, making it an ingrained process
- Building the Sarbanes-Oxley process into the wider IT governance initiatives

Rationalize Controls

Control rationalization (or elimination) is another initiative that should take place in the sustainment phase. Undoubtedly, there will be some controls that are documented that, over time, become less and less useful. Companies should periodically review their controls to identify which controls can be eliminated from the control listing. In doing so, consideration should be given to the impact of removing a control and any documentation prepared—explaining the rationale as to why the control was removed.

Automate Controls

In most cases, there are a significant number of manual controls that can be automated. The automated control examples provided in appendix D, Application Controls, are a great starting point for identifying where to transform manual controls into automated controls. Companies can review the examples in appendix D and the manual controls to determine which can be transformed into automated controls. In many cases, more detailed information will be needed depending on the applications available to a company and the nature of controls that are desired. Some organizations have more detailed control benchmarks that provide such details for a given application, such as SAP and Oracle.

Perform Application Benchmarking

The concept of application benchmarking was introduced by the PCAOB in its November 2004 guidance and is described more fully in appendix D. The idea is that, once an application is shown to be reliable through testing, it may not have to be tested every year. As a result, reductions in effort can be realized, making the compliance process more efficient and effective.

Appendix A—Sarbanes-Oxley Primer

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.

Background

The Sarbanes-Oxley Act was passed by the US Congress and signed into law by the President on 30 July 2002. Among other provisions, section 404 of the Act requires public companies registered with the SEC and their auditors to annually assess and report on the design and effectiveness of internal control over financial reporting.

Much has been written on the importance of the Act and internal controls in general; however, little exists on the significant role that information technology plays in this area. Most would agree that the reliability of financial reporting is heavily dependent on a well-controlled IT environment. Accordingly, there is a need for information that organizations can consider in addressing IT controls in a financial reporting context. While this document is primarily intended to assist SEC registrants in considering IT controls as part of their assessment activities, it can also be used to support compliance activities of companies that are registered in other jurisdictions and have implemented similar CEO/CFO certification requirements.

Many IT controls were considered in developing this document. However, a significant effort was made to limit the consideration of such controls to those directly related to internal control over financial reporting. As such, this document is deliberate in its exclusion of controls supporting operational and efficiency issues. It is, however, inevitable (and desirable) that operational and efficiency issues will be addressed over time and built into the control structures and processes that are developed. For further guidance in these areas, refer to the ITGI *Board Briefing on IT Governance, 2nd Edition*,[4] and the *IT Governance Implementation Guide*.[5]

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

[4] IT Governance Institute, *Board Briefing on IT Governance, 2nd Edition*, USA, 2003

[5] IT Governance Institute, *IT Governance Implementation Guide*, USA, 2003 (and to be released in a second edition late in 2006)

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.

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.*

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 and others responsible for the reliable operation of IT systems must take on the challenges of:

- Enhancing their knowledge of internal control
- Understanding their organization's overall Sarbanes-Oxley compliance plan
- Developing a compliance plan to specifically address IT controls
- Integrating this plan into the overall Sarbanes-Oxley compliance plan

Accordingly, the goal of this publication is to provide guidance to those responsible for the reliable operation of IT systems—including executive management, IT management, IT control professionals and assurance professionals—with regard to the following:

- Assessing the current state of the IT control environment
- Designing controls necessary to meet the requirements of Sarbanes-Oxley
- Developing an approach for testing and sustaining controls into the future
- Identifying exceptions and related remediation plans and adding compensating controls for exceptions identified

Auditing Internal Control Over Financial Reporting

In March 2004, the PCAOB approved Auditing Standard No. 2, titled "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements." The standard became effective in June 2004, upon approval by the SEC. This auditing standard establishes the requirements for performing an audit of internal control over financial reporting and provides some important direction on the scope and approach required of auditors.

The PCAOB Auditing Standard No. 2 includes specific requirements for auditors to understand the flow of transactions, including how transactions are initiated, authorized, recorded, processed and reported. In many cases, these transactions involve the use of financial applications that help record and process business information. The reliability of these applications is itself dependent on other systems, such as databases, networks and operating systems. Collectively, they define the IT systems that are involved in the financial reporting process and, as a result, need to be considered in the design and evaluation of internal control over financial reporting.

In the PCAOB Auditing Standard No. 2, information technology is described as having a "pervasive" effect on internal control over financial reporting. In essence, the auditing standard recognizes the importance of IT controls to the overall control environment and requires companies to understand how IT is used in the financial reporting process and how controls are designed and implemented to manage risks. In particular, the auditing standard highlights four IT controls that need to be considered for Sarbanes-Oxley: program development, program changes, computer operations, and access to programs and data.

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 to those sections can be found in **figure 8**.

Figure 8—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 officers ("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.	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 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

*Annual for foreign private issuers

Figure 8—Sarbanes-Oxley Requirements Primer *(cont.)*

	302	404
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.	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.
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

For the latest on requirements for section 404 requirements, refer to the SEC's website.

**Foreign filers begin on 15 July 2007 and nonaccelerated filers (<US $75 million) can defer to 15 December 2007. Furthermore, nonaccelerated filers have until 15 December 2008 to provide an auditors attestation report on internal control, as required by Section 404 (B).

Disclosure Controls and Procedures

Disclosure controls and procedures refer to the processes in place designed to help 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 be authorized, complete and accurate, and 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 its annual filing. Section 404 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.*

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 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.*
>
> *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 are effective.*

Auditor Focus Under Sarbanes-Oxley

Section 404 requires a company's independent auditor to attest to management's assessment of its internal control over financial reporting. Not only should organizations determine if appropriate controls (including IT controls) are in place, they should also provide their independent auditors with documentation—evidence of the design and operating effectiveness of 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 section 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 independent auditors to determine the period of time a control is required to be operating before the attestation date.

PCAOB Auditing Standard No. 2 discusses the external auditor's responsibilities in regard to section 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.*

Appendix B—COSO and CobiT

As presented earlier in the document, COSO divides internal control into five components. **Figure 9** shows that all of these 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 9—Cross-reference of COSO and CobiT Control Components

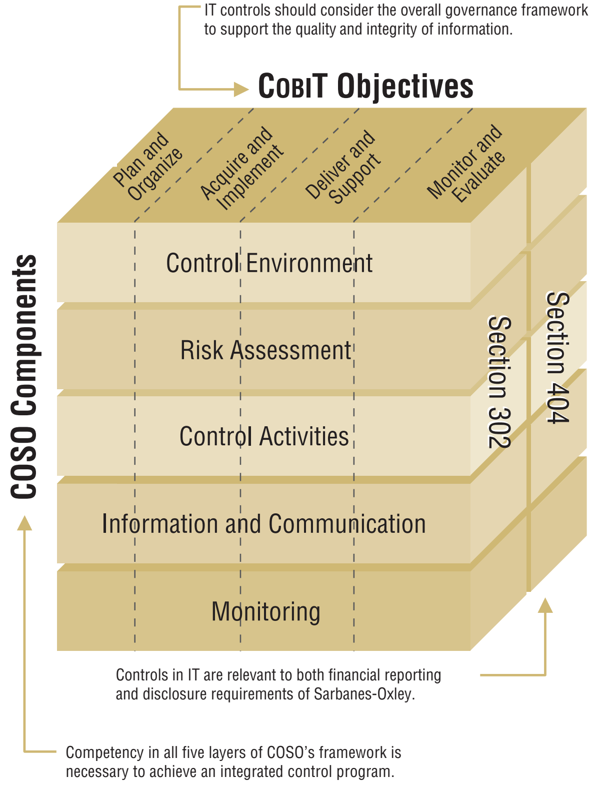

IT controls should consider the overall governance framework to support the quality and integrity of information.
CobiT Objectives
Plan and Organize
Acquire and Implement
Deliver and Support
Monitor and Evaluate
COSO Components
Control Environment
Risk Assessment
Control Activities
Information and Communication
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.

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 relying on application controls. 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 management of the governance of risk and control of IT, comprising four domains, 34 IT processes and 215 control objectives. CobiT includes controls that address all aspects of IT governance, but **only** those significant to financial reporting have been used to develop this document. It is a freely available framework, which aligns with the spirit of the Sarbanes-Oxley Act requirement that any framework used be easy to access and generally acceptable. CobiT provides both entity-level and activity-level objectives along with associated controls, and is widely used by organizations as a supplement to COSO.

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. 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.

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 IT professionals with guidance on the specific control objectives that should be considered along side COSO and, ultimately, compliance with the Sarbanes-Oxley Act. Accordingly, appendix C provides this information. 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.

In the development of this illustrative guidance, each control objective was challenged to ensure its relevance and importance to the financial reporting 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. Refer to **figure 10** to see this reconciliation.

Figure 10—COBIT Areas/COSO Components

Entity Level	Activity Level	COBIT IT Processes	COSO Component				
			Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
Plan and Organize (IT Environment)							
●		Define IT strategic planning.		●		●	●
		Define the information architecture.					
		Determine technological direction.					
●		Define the IT processes, organization and relationships.	●			●	●
		Manage the IT investment.					
●		Communicate management aims and direction.	●			●	
●		Manage IT human resources.	●			●	
●		Manage quality.	●		●	●	●
●		Assess and manage IT risks.		●			
		Manage projects.					
Acquire and Implement (Program Development and Program Change)							
		Identify automated solutions.					
	●	Acquire and maintain application software.			●		
	●	Acquire and maintain technology infrastructure.			●		
	●	Enable operation and use.			●	●	
		Procure IT resources.					
	●	Manage changes.		●	●		●
	●	Install and accredit solutions and 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.	●			●	
	●	Manage service desk and incidents.			●	●	●
	●	Manage the configuration.			●	●	
	●	Manage problems.			●	●	●
	●	Manage data.			●	●	
	●	Manage the physical environment.			●	●	
	●	Manage operations.			●	●	
Monitor and Evaluate (IT Environment)							
●		Monitor and evaluate IT performance.			●	●	●
●		Monitor and evaluate internal control.	●				●
●		Ensure regulatory compliance.			●	●	●
●		Provide IT governance.	●				●

Appendix C—IT General Controls

The Sarbanes-Oxley Act requires that organizations select and implement a suitable internal control framework. COSO's *Internal Control—Integrated Framework* has become the most commonly used framework by companies complying with Sarbanes-Oxley. While COSO makes reference to the importance of IT relative to the overall control environment, it does not provide detailed guidance for companies needing to design and implement specific IT controls for their environment.

In developing this publication, the IT control objectives, illustrative controls and tests of controls were derived using CobiT, see appendix B. Consideration was also given to ISO 17799, *The Code of Practice for Information Security Management*, and the Information Technology Infrastructure Library (ITIL) for service management. While all of these control frameworks address operational and financial objectives, **only** guidance considered significant to the control of financial reporting was selected and tailored for use in this publication.

Entity-level IT Controls

Generally speaking, IT general controls include objectives at the entity level and activity level. This publication addresses both; however, the entity-level objectives are presented as "points to consider" since the purpose of entity-level controls is to gain an understanding of the culture and operating style of the organization. Furthermore, entity-level controls are less likely to have specific activities; therefore, trying to define controls and tests for each area of the entity-level is beyond the scope of this document. As a result, this publication provides considerations that, when reviewed in aggregate, provide an overall assessment of the design and effectiveness of entity-level controls.

In using these points to consider, companies should be careful not to simply answer "yes" or "no." The purpose of the questions is to initiate a dialog that will yield examples of how the controls are performed and can be evidenced with documentation or through corroborative inquiry.

Figures 11 through **14** provide considerations for the entity-level assessment of an organization's IT control environment. As most organizations are using the COSO control framework for their internal control program, the figures have been structured in the same order as COSO and address points that could be considered in determining whether an entity-level objective has been achieved.

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.

Figure 11—Control Environment Considerations

Points to Consider	COBIT 4.0 Reference	Response/ Evidence
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?	PO1.4	
2. Does the IT organization communicate its IT plans to business process owners and other relevant parties across the organization?	PO1.2 PO6.5	
3. 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?	PO1.2 PO6.5	
4. Does the IT organization monitor its progress against the strategic plan and react accordingly to meet established objectives?	PO1.3 ME1.2	
IT Processes, Organization and Relationships		
5. Do IT managers have adequate knowledge and experience to fulfill their responsibilities?	PO7.2 PO7.4	
6. Have relevant systems and data been inventoried and their owners identified?	PO4.9	
7. Are roles and responsibilities of the IT organization defined, documented and understood?	PO4.6	
8. Do IT personnel understand and accept their responsibility regarding internal control?	PO4.6 PO6.1 ME2.2	
9. Have data integrity ownership and responsibilities been communicated to appropriate data/business owners and have they accepted these responsibilities?	PO4.9 PO6.5	
10. Has IT management implemented a division of roles and responsibilities (segregation of duties) that reasonably prevents a single individual from subverting a critical process?	PO4.11	
Manage IT Human Resources		
11. Has the IT organization adopted and promoted the company's culture of integrity management, including ethics, business practices and human resources evaluations?	PO6.1 PO7.7	
Educate and Train Users		
12. 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?	PO7.4 DS7.1	

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 important information represent an ever-increasing challenge to the IT department. The determination of this information is required to achieve control objectives.

The communication of this information in a form and time frame that allow people to carry out their duties supports the other four components of the COSO framework.

Figure 12—Information and Communication Considerations

Points to Consider	CobiT 4.0 Reference	Response/ Evidence
Communicate Management Aims and Directions		
13. Does IT management periodically review its policies, procedures and standards to reflect changing business conditions?	PO6.3	
14. Does IT management have a process in place to assess compliance with its policies, procedures and standards?	ME2	
15. Does IT management understand its roles and responsibilities related to the Sarbanes-Oxley Act?	ME3.1 ME3.2	

Risk Assessment

Risk assessment involves the identification and analysis by management of significant risks to achieving 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 entity level (for the overall organization) or at the activity level (for a specific process or business unit).

Figure 13—Risk Assessment Considerations

Points to Consider	CobiT 4.0 Reference	Response/ Evidence
Assess and Manage IT Risks		
16. Does the IT organization have an entity- and activity-level risk assessment framework that is used periodically to assess information risk to achieving financial reporting objectives? Does it consider the probability and likelihood of threats?	PO9.1	
17. 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?	PO9.2 PO9.3 PO9.4 ME4.5	
18. 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? Where risks have not been accepted, does management have an action plan to implement risk response?	PO9.5 PO9.6	

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.

Figure 14—Monitoring Considerations

Points to Consider	COBIT 4.0 Reference	Response/ Evidence
Manage Quality		
19. Is documentation created and maintained for significant IT processes, controls and activities?	PO8.2	
20. 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 assurance activities?	PO8.1 PO8.6	
Monitor and Evaluate Performance		
21. Has IT management established appropriate metrics to effectively manage the day-to-day activities of the IT department?	ME1.2 ME1.4	
22. Does IT management monitor IT's delivery of services to identify shortfalls and does IT respond with actionable plans to improve?	ME1.2 ME1.4	
Monitor and Evaluate Internal Control		
23. Does IT management obtain independent reviews of its operations, including policies, procedures, overall IT systems and processes, and do they assess adherence to those policies and procedures?	ME1.6 ME2.1 ME2.5	
24. Does the organization have an IT internal audit that is responsible for reviewing IT activities and controls, including general and application controls? Is there a follow-up process for residual actions? Is there a mechanism to allow monitoring of internal control of third-party service providers?	ME2.5 ME2.6 ME2.7	

Activity-level IT Controls

Providing information to enable management's reporting to regulators, investors and stakeholders is a life cycle of collecting complete and accurate information and reporting it on a timely basis. As one might expect, this life cycle is highly dependent on information systems, such as applications, databases and other tools used to enhance the efficiency and effectiveness of data processing.

The balance of this appendix is dedicated to providing guidance on IT controls that are specifically designed to support financial reporting objectives. As noted earlier, these controls are not intended to be an exhaustive list nor are they completely representative of what may be considered by the external auditor. However, they do provide a starting point as companies determine which IT controls are necessary for their environment. Consideration should also be given to IT controls that may not be included in the following tables, but which an organization considers relevant nonetheless.

In **figures 15** through **27**, certain illustrative controls are highlighted with a ✭ indicating that the control is a most relevant control. The most relevant internal controls applicable to financial statement assertions can be defined to include activities that prevent or detect and correct a significant misstatement in the financial reporting or other required disclosures, including those over recording amounts into the general ledger and recording journal entries (standard, nonstandard and consolidation). The most relevant controls may be manual or automated, and preventive or detective in nature. This definition has been applied to the controls in **figures 15** to **27** to identify those that are commonly required to comply with Sarbanes-Oxley. Note that in the titles of **figures 15** to **27**, COBIT control objectives are listed in parentheses.

As noted previously, this guidance is not intended to be authoritative. Professional judgment, as always, needs to be applied when determining the necessary controls that should be included in the compliance program, including some which may not be highlighted as most relevant controls in this document.

Figure 15—Acquire and Maintain Application Software (AI2)

Control Guidance

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

Rationale—The process of 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	COBIT 4.0 References
The organization has a system development life cycle (SDLC) methodology, which includes security 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 and processing integrity requirements. Consider whether there are appropriate steps to determine if these requirements are considered throughout the development or acquisition life cycle, e.g., security and processing integrity are considered during the requirements phase.	PO8.3 AI2.3 AI2.4

Figure 15—Acquire and Maintain Application Software (AI2) *(cont.)*

Control Guidance

Illustrative Controls	Illustrative Tests of Controls	CobiT 4.0 References
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.	PO6.3 AI2 AI6.2
The SDLC methodology includes requirements that information systems be designed to include application controls that support complete, accurate, authorized and valid transaction processing. ✩	Review the SDLC methodology to determine if it addresses application controls. Consider whether there are appropriate steps so 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.	AI1 AI2.3 AC
The organization has an acquisition and planning process that aligns with its overall strategic direction.	Review the SDLC methodology to determine if the organization's overall strategic direction is considered, e.g., an IT steering committee should review and approve projects so that a proposed project aligns with strategic business requirements and will utilize approved technologies.	PO4.3 AI3.1
To maintain a reliable environment, IT management involves users in the design of applications, selection of packaged software and the testing thereof. ✩	Review the SDLC methodology to determine if users are appropriately involved in the design of applications, selection of packaged software and testing.	AI1 AI2.1 AI2.2 AI7.2
Postimplementation reviews are performed to verify that controls are operating effectively.	Determine if postimplementation reviews are performed on new systems and significant changes reported.	AI7.12
The organization acquires/develops application 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 processes.	AI2

Figure 16—Acquire and Maintain Technology Infrastructure (AI3)

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	COBIT 4.0 References
Documented procedures exist and are followed so 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.	AI3

Figure 17—Enable Operations (PO6, PO8, AI6, DS13)

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 and the process for acquiring, developing and maintaining applications as well as required documentation. For some organizations, the policies and procedures 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	COBIT 4.0 References
The organization has policies and procedures regarding program development, program change, access to programs and data, and computer operations, which are periodically reviewed, updated and approved by management. ☆	Confirm that the organization has policies and procedures that are reviewed and updated regularly for changes in the business. 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, 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.	PO6.1 PO6.3 PO8.1 PO8.2 PO8.3 AI6.1 DS13.1

Figure 17—Enable Operations (PO6, PO8, AI6, DS13) *(cont.)*

Control Guidance

Illustrative Controls	Illustrative Tests of Controls	CobiT 4.0 References
The organization develops, maintains and operates its systems and applications in accordance with its supported, documented policies and procedures. ☆	Obtain the policies and procedures and determine if the organization manages its IT environment in accordance with them.	PO6.1 PO6.3 PO8.1 PO8.2 PO8.3 AI6.1 DS13.1

Figure 18—Install and Accredit Solutions and Changes (AI7)

Control Guidance

Control Objective—Controls provide reasonable assurance that the systems are appropriately tested and validated prior to being placed into production processes and that 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 should be performed to determine if the 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	CobiT 4.0 References
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 so 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 are 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 **figure 19**—Manage Changes.)	AI7.2 AI7.4 AI7.6 AI7.7

Figure 18—Install and Accredit Solutions and Changes (AI7) *(cont.)*

Control Guidance

Illustrative Controls	Illustrative Tests of Controls	COBIT 4.0 References
Load and stress testing is performed according to a test plan and established testing standards.	Select a sample of system development projects and system upgrades that are significant for financial reporting. Where capacity and performance were considered of potential concern, review the approach to load and stress testing. Consider whether a structured approach was taken to load and stress testing and 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.	AI7.2
Interfaces with other systems are tested to confirm that data transmissions are complete, accurate and valid. ✯	Select a sample of system development projects and 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.	AI7.5
The conversion of data is tested between their origin and their destination to confirm that the data are complete, accurate and valid. ✯	Obtain a sample of system development projects and 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.	AI7.5

Figure 19—Manage Changes (AI6, AI7)

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 so that proper classification and reporting integrity is maintained.

Illustrative Controls	Illustrative Tests of Controls	CobiT 4.0 References
Requests for program changes, system changes and maintenance (including changes to system software) are standardized, logged, approved, 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 determine that 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.	AI6.1 AI6.2 AI6.4 AI6.5 AI7.3 AI7.8 AI7.9 AI7.10 AI7.11

Figure 19—Manage Changes (AI6, AI7) *(cont.)*

Control Guidance

Illustrative Controls	Illustrative Tests of Controls	COBIT 4.0 References
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 verify that it is independently reviewed. Determine that procedures require emergency changes to 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.	AI6.3 AI7.10
Controls are in place to restrict migration of programs to production by authorized individuals only. ✯	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.	AI7.8
IT management implements system software that does 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.	AI6.2 AI7.4 AI7.9

Figure 20—Define and Manage Service Levels (DS1)

Control Guidance

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 by which the quality of services will be measured.

Rationale—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 determine if 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.

Illustrative Controls	Illustrative Tests of Controls	CobiT 4.0 References
Service levels are defined and managed to support financial reporting system requirements.	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.	DS1.2 DS1.3 DS1.5 DS1.6
A framework is defined to establish appropriate 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.	DS1.1 DS1.3

Figure 21—Manage Third-party Services (DS2)

Control Guidance

Control Objective—Controls provide reasonable assurance that third-party services are secure, accurate and available; support processing integrity; and are 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	CobiT 4.0 References
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.	DS2.2
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.	PO1.4 PO6.3 DS2
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 and processing integrity.	DS2.3
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 and processing integrity in accordance with the company's policies and procedures.	DS2.3

Figure 21—Manage Third-party Services (DS2) *(cont.)*

Control Guidance

Illustrative Controls	Illustrative Tests of Controls	CobiT 4.0 References
Procedures exist and are followed that include requirements that for third-party services a formal contract be defined and agreed to 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.	DS2.3
A regular review of security and processing integrity is performed by third-party service providers (e.g., SAS 70, Canadian 5970 and ISA 402). ☆	Inquire whether third-party service providers perform independent reviews of security and processing integrity, e.g., a service auditor report. Obtain a sample of the most recent review and determine if there are any control deficiencies that would impact financial reporting.	ME2.6

Figure 22—Ensure Systems Security (DS5)

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	CobiT 4.0 References
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?	PO6.3 PO6.5 DS5.2
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 • Roles and responsibilities • Physical and environmental security • Operating system security • Network security • Application security • Database security Determine if there are processes in place to communicate and maintain these standards.	PO8.2 DS5.2

Figure 22—Ensure Systems Security (DS5) *(cont.)*

Control Guidance

Illustrative Controls	Illustrative Tests of Controls	COBIT 4.0 References
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.	DS5.2
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.	DS5.2
Procedures exist and are followed to authenticate all users of the system (both internal and external) to support the existence of transactions. ✯	Assess the authentication mechanisms used to validate user credentials for financial reporting systems and subsystems and validate that user sessions time-out after a predetermined period of time. Validate that no shared user profiles (including administrative profiles) are used.	DS5.3 AC
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.).	DS5.3 DS5.4
Procedures exist and are followed relating to timely action for requesting, establishing, issuing, suspending and closing user accounts. (Include procedures for authenticating transactions originating outside the organization.) ✯	Confirm that procedures for the registration, change and deletion of users from financial reporting systems and subsystems on a timely basis exist and are followed. 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 the removal was done in a timely manner. Select a sample of privileged and current users and review their access for appropriateness based upon their job functions.	DS5.4

Figure 22—Ensure Systems Security (DS5) *(cont.)*

Control Guidance		
Illustrative Controls	**Illustrative Tests of Controls**	**COBIT 4.0 References**
A control process exists and is followed to periodically review and confirm access rights. ☆	Inquire whether access controls for financial reporting systems and subsystems are reviewed by management on a periodic basis. Assess the adequacy of how exceptions are reexamined, and if the follow-up occurs in a timely manner.	DS5.4
Where appropriate, controls exist so 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.	DS11.6 AC AC
Appropriate controls, including firewalls, intrusion detection and vulnerability assessments, exist and are used to prevent unauthorized access via public networks.	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.	DS5.10

Figure 22—Ensure Systems Security (DS5) *(cont.)*

Control Guidance

Illustrative Controls	Illustrative Tests of Controls	CobiT 4.0 References
IT security administration monitors and logs security activity at the operating system, application and database levels and identified security violations are reported to senior management. ✯	Inquire whether a security office exists to monitor for security vulnerabilities at the application and database levels 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. Validate that attempts to gain unauthorized access to financial reporting systems and subsystems are logged and followed up on a timely basis.	DS5.5
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.	DS5.3 DS5.4
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.	DS12.2 DS12.3

Figure 23—Manage the Configuration (DS9)

Control Guidance

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

Rationale—Configuration management includes procedures such that security and processing integrity controls are set up in the system and maintained through its life cycle. Insufficient configuration controls can lead to security exposures that may permit unauthorized access to systems and data and impact financial reporting. An additional potential risk is corruption to data integrity caused by poor control of the configuration when making system changes or by the introduction of unauthorized system components.

Illustrative Controls	Illustrative Tests of Controls	CobiT 4.0 References
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 it is clearly articulated. Consider reviewing a sample of applications and computers to determine if they are in conformance with organization policy.	DS9.2
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.	DS5.3 DS5.4 DS5.10
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.	DS5.4

Figure 23—Manage the Configuration (DS9) *(cont.)*

Control Guidance

Illustrative Controls	Illustrative Tests of Controls	COBIT 4.0 References
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.	DS5.9
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.	AI3.2 AI3.3

Figure 24—Manage Problems and Incidents (DS8, DS10)

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—The process of 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	COBIT 4.0 References
IT management has defined and implemented an incident and problem management system such that data integrity and access control incidents are recorded, analyzed, resolved in a timely manner and reported to management. ✯	Determine if an incident management system exists and how it is being used. Review how management has documented how the system is to be used. Review a sample of incident reports, to consider if the issues were addressed (recorded, analyzed and resolved) in a timely manner.	DS8
The problem management system provides for adequate audit trail facilities, which allow tracing from problem or incident to underlying cause.	Determine if the organization's procedures include audit trail facilities—tracking of the problems or incidents. Review a sample of problems recorded on the problem management system to consider if a proper audit trail exists and is used.	DS10.2
A security incident response process exists to support timely response and investigation of unauthorized activities.	Verify that unauthorized activities are responded to in a timely fashion, and there is a process to support proper disposition.	DS5.6 DS8.3 DS10.1 DS10.3

Figure 25—Manage Data (DS11)

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 existence. 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	CobiT 4.0 References
Policies and procedures exist for the distribution and retention of data and reporting output.	Review the policies and procedures for the 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 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.	DS11.1 DS11.2 DS11.6
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—logically and physically, in storage and during transmission—against unauthorized access or modification.	DS11.6
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. 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.	DS11.2

Figure 25—Manage Data (DS11) *(cont.)*

Control Guidance

Illustrative Controls	Illustrative Tests of Controls	COBIT 4.0 References
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.	DS11.5
The restoration of information is periodically tested. ✯	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.	DS11.5
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.	AI6

Figure 26—Manage Operations (DS13)

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 and error monitoring.

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**	**COBIT 4.0 References**
Management has established, documented and follows standard procedures for IT operations, including job scheduling and monitoring and responding to security and processing integrity events. ☆	Determine if management has documented its procedures for IT operations, and operations are reviewed periodically for 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.	DS13.1 DS13.2
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 usable for reconstruction, if necessary. Obtain a sample of the log entries, to determine if they sufficiently allow for reconstruction.	DS13.3
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 determine 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.	DS11.1 DS13.3

Figure 27—End-user Computing

Control Guidance

The following illustrative controls for end-user computing have been extracted from the control guidance in figures 15 to 26 and are presented to address the characteristics of a typical end-user computing environment. Appropriate CobiT processes apply to this environment.

Illustrative Controls	Illustrative Tests of Controls
End-user computing policies and procedures concerning security and processing integrity exist and are followed. ✯	Obtain a copy of the end-user computing policies and procedures and confirm that they address security 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.
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. Select a sample of user-developed systems and determine who has access and if the access is appropriate.

Figure 27—End-user Computing *(cont.)*

Control Guidance	
Illustrative Controls	**Illustrative Tests of Controls**
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 as to 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 their ability to process completely and accurately.

Appendix D—Application Controls

The Importance of Application Controls

In the realm of complex IT-dependent financial reporting environments, many organizations still have not focused enough attention on application controls when performing their certification work. The PCAOB has highlighted the importance of this area and organizations that do not properly consider these controls may be at risk of failing Sarbanes-Oxley compliance.

Very frequently, organizations assume that their financial reporting systems are reliable because they have never experienced a problem with them or they believe that testing at some point in the past is sufficiently reliable. In other instances, organizations take a "black box" approach and place all their reliance on manual controls, failing to consider the risks that exist within the system. The challenge in each instance is that undue reliance is being placed on the system—companies are relying on their systems without understanding how they support financial reporting objectives. This can be a significant oversight that could lead to a material weakness in internal control.

In response, many organizations are starting to review their relevant applications to understand how they support the financial reporting process. In doing so, they are developing application integrity documentation through a process called "baselining" or benchmarking.

Defining Application Controls

At the business process level, controls are applied to specific business activities to achieve financial objectives. Most business processes are automated and integrated with IT application systems, resulting in many of the controls at this level being automated as well. These controls are known as automated application controls.

Automated application controls apply only to the business processes they support. They are controls designed within the application to prevent or detect unauthorized transactions and support financial objectives including completeness, accuracy, authorization and existence of transactions. Before starting the identification and documentation of controls, careful consideration should be given to the type of controls that should be used.

In making the decision on which controls should be documented, it is important to understand the characteristics of each. Generally speaking, there are three types of controls:

- Manual controls—Performed without the assistance of applications or any other technology systems. Examples include supervisory controls; written authorizations, such as a signature on a check; or manual tasks, such as reconciling purchase orders to goods receipt statements. Manual controls are subject to the inherent risk of human error and, as a result, are often considered less reliable.

- Automated controls—Performed by computers and binary in nature, they always function as designed and are not subject to intermittent error. Examples include input edit checks that validate order quantities or configured controls in automated purchasing systems that allow orders only up to preconfigured limits. Examples include:
  - Balancing control activities—Controls that 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—A calculation to validate data. For example, 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—Controls that 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—Tests that 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 feet of lumber may trigger a review.
  - Logic tests—Tests that include the use of range limits or value/alphanumeric tests. For example, credit card numbers have a predefined format.
  - Calculations—Numerical manipulations performed by an automated processing routine configured within applications
- IT-dependent manual controls (hybrid)—Essentially a combination of manual and automated processes. System-generated reports are most commonly found in hybrid controls since they provide data for management review. For instance, the valuation of accounts receivable might include a control whereby the receivables manager reviews the monthly aging report for reasonableness. In this example, a report is produced from the receivables system (automated process) and reviewed for reasonableness (manual process). As a result, both the automated process (report generation) and manual process (review by management) are required to support the valuation of accounts receivable.

The Business Case for Application Controls

There are advantages and disadvantages to manual and automated control activities. In some cases, it is easier to document and gather evidence for manual control activities in small companies of low complexity. However, documenting manual controls can become a very expensive endeavor in large companies of high complexity. For large and complex companies, the effort associated with documenting and testing automated controls is much more appealing in the long term as controls need to be tested only once, whereas manual controls need to be tested based on the frequency of their operation. It is important to note that while the sample size for manual controls varies with the frequency of performance, the sample size for automated controls does not. This can add up to a very significant savings for companies. For instance, consider an organization that needs to identify 500 controls for its Sarbanes-Oxley program and is considering whether to document manual or automated controls. The tables in **figure 28** were prepared to assist in their analysis.

Figure 28—Comparison of Manual and Application Control Approaches

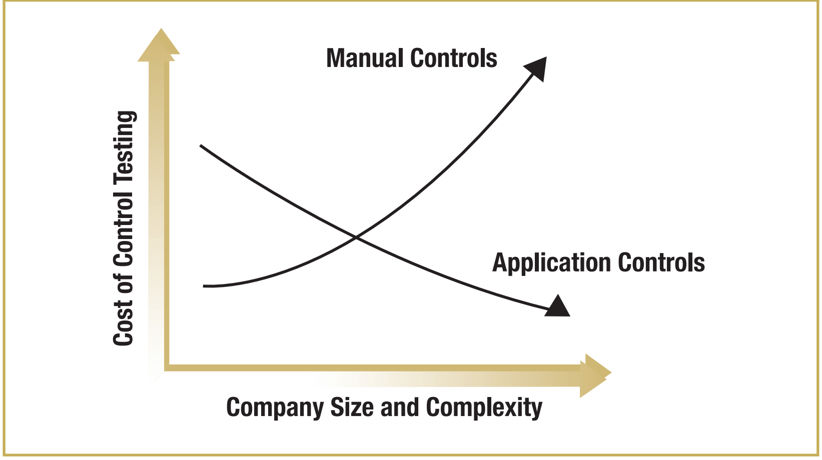
Manual Control Approach		**Automated Control Approach**	
Total controls	500	Total controls	500
Effort to document per control	1 hour	Effort to document per control	3 hours
Total effort to document	500 hours	Total effort to document	1,500 hours
Average sample size per control	10	Average sample size per control	1
Total sample items to test	5,000	Total sample items to test	500
Effort to test per sample	30 minutes	Effort to test per sample	30 minutes
Total effort to test	2,500 hours	Total effort to test	250 hours
Total effort	**3,000 hours**	**Total effort**	**1,750 hours**

A few observations should be noted in this example. First, it shows that the initial effort to document manual controls is less than that required for automated controls. This is due primarily to the complexity of IT systems and the requirement to understand how the application works. Second, the effort required for testing manual controls is greater than that required for automated controls. This is due to the fact that automated controls operate as designed and need to be tested only once provided that the general IT controls are reliable (program development, program change, access to programs and data, and computer operations).

However, if "sustained compliance" is considered over a period of five years, the impact is much more significant. In this example, savings in year one amounts to 1,250 hours, but in year two and thereafter, when the company needs only to retest its controls, this savings increases to 2,250 hours annually. Therefore, after five years of compliance, a company could save 10,250 hours of effort if they selected to document and test automated controls. **Figure 29** illustrates how the size and complexity of a company impact the effort and, therefore, the cost of documenting and testing manual vs. automated controls.

When one considers that automated controls are generally more reliable, the benefits of taking this approach are compelling.

Figure 29—Effect of Size and Complexity on Effort to Document and Test Controls



Establishing the Application Benchmark

Application benchmarking involves documenting and testing the relevant controls embedded within financial applications that support the financial statements to confirm their design and operating effectiveness. Once these controls have been identified and tested, they qualify for benchmarking, which essentially allows for a reduction in the frequency of testing as long as certain conditions are met as described in the following paragraphs.

While there are additional costs required to establish an application benchmark (such as understanding how the application works and documenting the relevant controls over its processing), the benefits can be compelling. As noted in **figure 28**, the reduction of testing effort alone provides a solid business case. However, there are other benefits, including:

- Further reduction of testing effort since applications controls may not require testing every year because they are not subject to human error and typically operate as designed as long as certain conditions exist as further explained in the next paragraph.
- Improved reliance since application controls are typically preventive and more reliable than manual controls. They often serve as dual-purpose controls since they not only support financial control objectives, but may support antifraud objectives as well.

Application benchmarking was addressed by the PCAOB in its November 2004 guidance stating that benchmarking is an acceptable practice as long as certain conditions are met, specifically that:

- The relevant segments of the application that support the application controls are identified (for instance, the accounts payable module that supports automated aging of accounts or the inventory module that supports complete and accurate listing of inventory balances)

- The relevant application controls are appropriately designed
- The relevant application controls have not changed during the year
- The most recent test of the application controls confirms their operating effectiveness
- The relevant supporting IT general controls, particularly access controls and change controls supporting the application, are appropriately designed and operating effectively

Examples of Automated Application Controls

To assist companies in applying an automated control approach, examples of automated controls are provided in **figures 31** to **38**. For the most part, these controls 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 in **figures 31** to **38** 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 31 to **38** refer to controls that extend into applications and business processes that contribute to financial "statement assertions," including completeness, accuracy, valuation and authorization controls. Definition and some examples of these financial statement assertions are summarized in **figure 30**.

Figure 30—Financial Statement Assertion Definitions and Examples

Financial Statement Assertions	Definition	Example
Existence	Assertions about existence or occurrence address whether assets or liabilities of the entity exist at a given date and whether recorded transactions have occurred during a given period.	Management asserts that finished goods inventories in the balance sheet are available for sale. Similarly, management asserts that sales in the income statement represent the exchange of goods or services with customers for cash or other consideration.
Completeness	Assertions about completeness address whether all transactions and accounts that should be presented in the financial statements are included.	Management asserts that all purchases of goods and services are recorded and are included in the financial statements. Similarly, management asserts that notes payable in the balance sheet include all such obligations of the entity.
Valuation	Assertions about valuation or allocation address whether asset, liability, equity, revenue and expense components have been included in the financial statements in appropriate amounts.	Management asserts that property is recorded at historical cost and that such cost is systematically allocated to appropriate accounting periods. Similarly, management asserts that trade accounts receivable included in the balance sheet are stated at net realizable value. statement are properly classified and described.

Figure 31—Application Control Objectives for the Financial Statement Close Cycle

Illustrative Control Objectives	Financial Assertions
Entries booked in the close process are complete and accurate.	Completeness Existence
Automated amortization timing, periods and methods are appropriate and accurately entered.	Valuation Existence
Variance reports are generated for use to identify posting errors/out-of-balance conditions.	Completeness Existence Valuation
Standard, recurring period-end journal entries submitted from subsidiary ledger systems are automated, appropriately approved and entered accurately.	Completeness Existence Valuation
Systems generate reports of all recurring and nonrecurring journal entries.	Completeness Existence
All nonstandard journal entries are tracked and are appropriate.	Completeness Existence
Account codes and transaction amounts are accurate and complete, with exceptions reported.	Completeness Existence
General ledger balances reconcile to subledger balances.	Completeness Existence
Recorded amounts undergo an automated comparison to predicted amounts.	Completeness Existence
Out-of-balance entries are prohibited.	Completeness Existence
Enterprisewide consolidation, including standard intercompany eliminations, is automated/performed using a third-party software product.	Completeness Existence Valuation
System functionality supports the segregation of the posting and approval functions.	Existence
Access to general ledger records is appropriate and authorized.	Completeness Existence Valuation
Transactions cannot be recorded outside of financial close cutoff requirements.	Completeness Existence Valuation
Annually approved recurring accruals are accurately booked in the appropriate periods.	Completeness Existence Valuation
System controls are in place for appropriate approval of write-offs.	Existence
Interrelated balance sheets and income statement accounts undergo automated reconciliation.	Completeness Existence
The sources of all entries are readily identifiable.	Existence
Transactions are either rejected, or accepted and identified, on exception reports in the event of data exceptions.	Completeness Existence
Account mappings are up to date.	Existence

Figure 32—Application Control Objectives for the General Ledger

Illustrative Control Objectives	Financial Assertions
Access to general ledger entries is appropriate and authorized.	Completeness Existence Valuation
General ledger balances reconcile to subledger balances and such reconciliations are reviewed for accuracy and approved by supervisory personnel.	Completeness Existence
Interrelated balance sheets and income statement accounts undergo automated reconciliations to confirm accuracy of such accounts.	Completeness Existence
Systems generate reports of all recurring and nonrecurring journal entries for review by management for accuracy.	Completeness Existence
System functionality exists to segregate the posting and approval functions.	Existence
All nonstandard journal entries are tracked and are appropriate.	Completeness Existence
Account codes and transaction amounts are accurate and complete, with exceptions reported.	Completeness Existence
Recorded amounts undergo automated comparison to predicted amounts to confirm accuracy of entries.	Completeness Existence
Out-of-balance entries are prohibited.	Completeness Existence
Enterprisewide consolidation, including standard intercompany eliminations, is automated/performed.	Completeness Existence Valuation
Variance reports are generated for use to identify posting errors/out-of-balance conditions.	Completeness Existence Valuation
System controls are in place for appropriate approval of write-offs.	Existence
Journal entries of exceptional amount that were posted to the general ledger during the month are flagged by the system and subsequently reviewed for accuracy and approved by the controller or CFO after month-end.	Completeness Existence Valuation
A report of all journal entries completed as part of the closing process is reviewed by management to confirm the completeness and appropriateness of all recorded entries.	Completeness Existence
General ledger master file change reports are generated by the system and reviewed as necessary by an individual who does not input the changes.	Completeness Existence

Figure 32—Application Control Objectives for the General Ledger *(cont.)*

Illustrative Control Objectives	Financial Assertions
Actual-to-actual, actual-to-budget and yield reports are produced from the general ledger system on a monthly basis prior to the final close of the general ledger. Reports are distributed to and reviewed by the controller and CFO. Unusual amounts or variances are investigated and reclassified when applicable.	Completeness Existence Valuation
A standard chart of accounts has been approved by management and is utilized within all entities of the corporation. Adding to or deleting from the general ledger is limited to authorized accounting department personnel.	Completeness Existence
A stale items report (e.g., reconciling items outstanding over 90 days) is generated by the system to monitor timely follow-up and resolution of outstanding items.	Completeness Existence
Entries booked in the close process are complete and accurate.	Completeness Existence
Automated amortization timing, periods and methods are appropriate and accurately entered.	Valuation Existence
Standard, recurring period-end journal entries submitted from subsidiary ledger systems are automated, appropriately approved and entered accurately.	Completeness Existence Valuation
Transactions cannot be recorded outside of financial close cutoff requirements.	Completeness Existence Valuation
Annually approved recurring accruals are accurately booked in the appropriate periods.	Completeness Existence Valuation
The sources of all entries are readily identifiable.	Existence
Transactions are rejected, or accepted and identified, on exception reports in the event of data exceptions.	Completeness Existence
Account mappings are up to date.	Existence

Figure 33—Application Control Objectives for the Sales Cycle

Illustrative Control Objectives	Financial Assertions
Orders are processed only within approved customer credit limits.	Valuation
Orders are approved by management as to prices and terms of sale.	Existence
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.	Existence
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
Credit notes for all goods returned and adjustments to accounts receivable are issued in accordance with organization policy.	Existence
Invoices relate to valid shipments.	Existence
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.	Existence
Invoices are recorded in the appropriate period.	Valuation
Credit notes issued are recorded in the appropriate period.	Valuation
Cash receipts are recorded in the period in which they are received.	Valuation
Cash receipts data are entered for processing accurately.	Valuation
All cash receipts data are entered for processing.	Existence
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 Existence
Only valid changes are made to the customer master file.	Completeness Existence
All valid changes to the customer master file are input and processed.	Completeness Existence

Figure 33—Application Control Objectives for the Sales Cycle *(cont.)*

Illustrative Control Objectives	Financial Assertions
Changes to the customer master file are accurate.	Valuation
Changes to the customer master file are processed in a timely manner.	Completeness Existence
Customer master file data remain up to date.	Completeness Existence

Figure 34—Application Control Objectives for the Purchasing Cycle

Illustrative Control Objectives	Financial Assertions
Purchase orders are placed only for approved requisitions.	Existence
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.	Existence
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
Accounts payable are adjusted only for valid reasons.	Completeness Existence
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 Existence
Credit notes and other adjustments are recorded in the appropriate period.	Valuation
Disbursements are made only for goods and services received.	Existence
Disbursements are distributed to the appropriate suppliers.	Existence
Disbursements are accurately calculated and recorded.	Valuation
All disbursements are recorded.	Completeness
Disbursements are recorded in the period in which they are issued.	Valuation
Only valid changes are made to the supplier master file.	Completeness Existence

Figure 34—Application Control Objectives for the Purchasing Cycle *(cont.)*

Illustrative Control Objectives	Financial Assertions
All valid changes to the supplier master file are input and processed.	Completeness Existence
Changes to the supplier master file are accurate.	Valuation
Changes to the supplier master file are processed in a timely manner.	Completeness Existence
Supplier master file data remain up to date.	Completeness Existence

Figure 35—Application Control Objectives for the Inventory Cycle

Illustrative Control Objectives	Financial Assertions
Adjustments to inventory prices or quantities are recorded promptly and in the appropriate period.	Existence Completeness Valuation
Adjustments to inventory prices or quantities are recorded accurately.	Valuation
Raw materials are received and accepted only if they have valid purchase orders.	Existence
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
Defective raw materials are returned promptly to suppliers.	Existence
All transfers of raw materials to production are recorded accurately and in the appropriate period.	Valuation Completeness
All direct and indirect expenses associated with production are recorded accurately and in the appropriate period.	Valuation
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
Finished goods received from production are recorded completely and accurately in the appropriate period.	Completeness Valuation
All shipments are recorded.	Existence
Shipments are recorded accurately.	Valuation
Shipments are recorded promptly and in the appropriate period.	Valuation
Inventory is reduced only when goods are shipped with approved customer orders.	Completeness Existence

Figure 35—Application Control Objectives for the Inventory Cycle *(cont.)*

Illustrative Control Objectives	Financial Assertions
Costs of shipped inventory are transferred from inventory to cost of sales.	Existence Valuation
Costs of shipped inventory are accurately recorded.	Valuation
Amounts posted to cost of sales represent those associated with shipped inventory.	Completeness Existence
Costs of shipped inventory are transferred from inventory to cost of sales promptly and in the appropriate period.	Valuation
Only valid changes are made to the inventory management master file.	Existence Completeness
All valid changes to the inventory management master file are input and processed.	Existence Completeness
Changes to the inventory management master file are accurate.	Valuation
Changes to the inventory management master file are promptly processed.	Existence Completeness
Inventory management master file data remain up to date.	Completeness Existence

Figure 36—Application Control Objectives for the Fixed Asset Cycle

Illustrative Control Objectives	Financial Assertions
Fixed asset acquisitions are accurately recorded.	Valuation
Fixed asset acquisitions are recorded in the appropriate period.	Valuation
All fixed asset acquisitions are recorded.	Completeness
Depreciation charges are accurately calculated and recorded.	Valuation
All depreciation charges are recorded in the appropriate period.	Existence Valuation Completeness
All fixed asset disposals are recorded.	Existence
Fixed asset disposals are accurately calculated and recorded.	Valuation
Fixed asset disposals are recorded in the appropriate period.	Valuation
Records of fixed asset maintenance activity are accurately maintained.	Completeness
Fixed asset maintenance activity records are updated in a timely manner.	Completeness
Only valid changes are made to the fixed asset register and/or master file.	Completeness Existence

Figure 36—Application Control Objectives for the Fixed Asset Cycle *(cont.)*

Illustrative Control Objectives	Financial Assertions
All valid changes to the fixed asset register and/or master file are input and processed.	Completeness Existence
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 Existence
Fixed asset register and/or master file data remain up to date.	Completeness Existence

Figure 37—Application Control Objectives for the Human Resources Cycle

Illustrative Control Objectives	Financial Assertions
Additions to the payroll master files represent valid employees.	Existence
All new employees are added to the payroll master files.	Completeness
Terminated employees are removed from the payroll master files.	Existence
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
Payroll (including compensation and withholdings) is accurately calculated and recorded.	Valuation
Payroll is disbursed to appropriate employees.	Existence
Only valid changes are made to the payroll master files.	Existence Completeness
All valid changes to the payroll master files are input and processed.	Existence Completeness
Changes to the payroll master files are accurate.	Valuation
Changes to the payroll master files are processed in a timely manner.	Existence Completeness
Payroll master file data remain up to date.	Existence Completeness
Only valid changes are made to the payroll withholding tables.	Existence Completeness

Figure 37—Application Control Objectives for the Human Resources Cycle *(cont.)*

Illustrative Control Objectives	Financial Assertions
All valid changes to the payroll withholding tables are input and processed.	Existence Completeness
Changes to the payroll withholding tables are accurate.	Valuation
Changes to the payroll withholding tables are promptly processed.	Existence Completeness
Payroll withholding table data remain up to date.	Existence Completeness

Figure 38—Application Control Objectives for the Tax Cycle

Illustrative Control Objectives	Financial Assertions
Automated workflows are used for timely filing of returns.	Completeness
Tax payments are correctly calculated and recorded to the general ledger.	Completeness Valuation Existence
Tax exposures and valuation allowances are correctly calculated and recorded.	Completeness Existence Valuation
Tax expenses are recorded in the correct periods.	Completeness Existence Valuation
Permanent and temporary differences are identified and recorded accurately.	Completeness Existence Valuation
Correct book income is used in the tax accrual.	Completeness Existence
Tax assets, liabilities and expenses are complete and correctly calculated and reported.	Completeness Existence
Depreciation is calculated using appropriate bases, resulting in correct charges and tax ramifications.	Completeness Existence
Sales and use tax is calculated appropriately, correctly and in a timely manner.	Completeness Existence
Value-added tax is correctly accounted for and filed appropriately.	Completeness Existence
Transfer pricing policies are up to date and accurately represented in the systems.	Completeness Existence
All tax payments are accurately reflected in the general ledger.	Valuation
Property tax filings are timely and accurate.	Completeness Existence Valuation

Appendix E—Sample Application and Technology Layers Inventory

Figure 39—Sample Application and Technology Layers Inventory

Application Name	Related Business Process	Application Details			Database		Operating System/Network		Hardware Platform		Physical Location	
		Package/ In-house	Customized	Owner	Version	Owner	Version	Owner	Version	Owner	Facility	Owner
SAP	Financials	Package	Yes	Kerry M	Oracle 9*i* v9.2.0	Craig T	Solaris 3.2/ Novell	Ryan S	HP 9000	Doug W	Calgary	D'Arcy M
PeopleSoft	HR payroll	Package	Yes	Tom M	Oracle 9*i* v9.2.0	Craig T	HP-UX v11.11/ Novell	Adel M	HP 9000	Doug W	Houston	Rhonda M
ACCPAC	Subsidiary accounting	Package	No	Esther C	Oracle 9*i* v9.2.0	Craig T	HP-UX v11.11/ Novell	Adel M	HP 9000	Doug W	Denver	Robert P
TIMS	Time recording	Package	Yes	Darryl J	DB2 400	Alan S	OS400/ Novell	Reid C	AS400	Rob K	Calgary	D'Arcy M
VIBS	Billing	Custom	Yes	Paul Z	DB2 400	Alan S	OS400/ Novell	Ryan R	AS400	Barb V	Calgary	D'Arcy M
SunGard	Investment	Outsourced processing	No	Kerry M	Refer to SAS 70	Craig T	Refer to SAS 70	Ryan S	Refer to SAS 70	Doug W	Refer to SAS 70	Doug W

Appendix F—Project Estimating Tool

Figure 40—Project Estimating Tool

Project Phase	Estimated Effort for Each Project Phase by Size of Company (These are estimates only and could be higher or lower depending on the unique circumstances of each company.)					
	Small (Single Location, <5 Applications)		Medium (<5 Locations, 5-10 Applications)		Large (>5 to 10 Locations, >10 to 15 Applications)	
Effort Estimate (Days)	Low Estimate	High Estimate	Low Estimate	High Estimate	Low Estimate	High Estimate
1. Plan and scope.	2	5	5	10	10	20
2. Assess risk.	2	5	2	5	5	15
3. Identify and document controls.	5	10	10	20	20	50
4. Evaluate design and operating effectiveness.	5	10	10	20	20	30
5. Prioritize and remediate deficiencies.	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1
6. Build sustainability.	Note 2	Note 2	Note 2	Note 2	Note 2	Note 2

Note 1—Remediation effort depends on the severity of the deficiency. Companies may choose to go beyond remediation and address operational efficiency issues, such as implementing a new system development or change management process.

Note 2—Sustainment efforts include the evaluation of automation and rationalization opportunities but do not include the time required to implement, which is unique to every organization.

Figure 41—Estimate of Effort to Document and Test (Days

Estimate of Effort to Document and Test (Days)		
IT Environment (Each)	Low Estimate	High Estimate
Small package application	1	2
Large package application	2	5
Small custom application	1	2
Large custom application	5	10
Assess segregation of duties—small application	2	10
Assess segregation of duties—large application	5	30

Figure 42—Estimated Effort to Document and Test (Days)

Estimate of Effort to Document and Test (Days)		
IT Environment (Each)	Low Estimate	High Estimate
Spreadsheet—low complexity	.25	1
Spreadsheet—high complexity	.5	2
Database	2	5
Operating system	.5	2
Network	.5	5
Physical facility	.5	1

Once the initial assessment has been performed, the estimates of effort for sustaining these controls may decrease over time. The estimates noted in **figure 41** and **42** are initial planning estimates and may vary. For instance, companies that are very decentralized and have a significant number of applications may require substantially more effort. Similarly, very small companies with simple processes and few applications may require less effort.

Appendix G—Inherent Risk Assessment and Control Prioritization Grid

Risk Assessment Considerations

By performing a risk assessment of the in-scope applications and their related subsystems, companies can prioritize efforts in areas of higher risk and reduce efforts in areas of lower risk. It is important to note that the assessment of risk is a judgmental decision; however, there are common risk factors that should be taken into consideration. **Figures 43** through **45** are provided to assist in the inherent risk assessment.

Figure 43—Inherent Risk Considerations

Example Risk Factors	Considerations for Higher Risk	Considerations for Lower Risk
Nature of technology	Complex, unique, customized, developed in-house	Simple, commonly used, not customized, off-the-shelf
Nature of people	Inexperienced, lack of training, limited number of people, high turnover	Experienced, trained and specialized, sufficient resources, low turnover
Nature of processes	Decentralized, multilocation, *ad hoc*	Centralized, formalized, consistent
Past experience	History of problems including processing errors, system outages, data corruption	No history of problems
Significance to the financial reports	Direct—Used for initiating and recording amounts into the financial reports	Indirect—Used for analytical purposes but does not initiate or record amounts into the financial reports

Information Technology Risk Assessment

An assessment should be performed for each in-scope application. In some cases, the subsystems (database, operating system, network and physical environment) will be the same for many or all applications. In this case, subsystems can be assessed once.

Figure 44—Inherent Risk Assessment for Technology Layers

Inherent Risk Factors	**Technology Layers**				
	Application	**Database**	**Operating System**	**Network**	**Physical**
Nature of technology	H/M/L	H/M/L	H/M/L	H/M/L	H/M/L
Nature of people	H/M/L	H/M/L	H/M/L	H/M/L	H/M/L
Nature of processes	H/M/L	H/M/L	H/M/L	H/M/L	H/M/L
Past experience	H/M/L	H/M/L	H/M/L	H/M/L	H/M/L
Significance to the financial reports	H/M/L	H/M/L	H/M/L	H/M/L	H/M/L
Overall conclusion (judgment)	**H/M/L**	**H/M/L**	**H/M/L**	**H/M/L**	**H/M/L**

In performing the risk assessment and establishing a risk rating it is important to document the considerations or rationale for the risk rating. The considerations in **figure 37** may be used as a starting point, but further analysis should be completed and documented to support the risk assessment.

Recommendations on Where Controls Should Be Considered

This grid provides guidance on the IT controls that should be considered for each of the technology layers. Generally speaking, the grid reflects the theory that financial applications that more directly support financial controls are of greater risk to financial reporting and, therefore, require the greatest consideration. Similarly, physical security controls, which support the general control environment but are far removed from the financial statements, present less risk and require less consideration. As always, there is no one-size-fits-all approach, and each company will have to customize this grid based on its particular needs and circumstances.

Figure 45—Control Prioritization Grid

PCAOB Headings	IT Controls for Sarbanes-Oxley	Technology Layers				
		Application	Database	Operating System	Network	Physical
Program Change and Program Development	Acquire and develop application software.	**R**	**R**	D	D	D
	Acquire technology infrastructure.	D	D	D	D	D
	Develop and maintain policies and procedures.	**R**	**R**	**R**	**R**	**R**
	Install and test application software and technology infrastructure.	**R**	**R**	D	D	D
	Manage changes.	**R**	**R**	**R**	D	D
Access to Programs, Data and Computer Operations	Define and manage service levels.	D	D	D	D	D
	Manage third-party services.	**R**	**R**	**R**	D	D
	Ensure systems security.	**R**	**R**	**R**	**R**	D
	Manage the configuration.	**R**	**R**	**R**	D	D
	Manage problems and incidents.	**R**	**R**	**R**	**R**	D
	Manage data.	**R**	**R**	D	D	D
	Manage operations.	**R**	**R**	D	D	D

R—Recommended. IT controls should be considered for each technology layer as noted. The extent of work in each area will depend on the inherent risk assessment.
D—Discretionary. IT controls should be considered where risks have been identified.

Appendix H—Sample Control Documentation and Testing Template

This matrix provides guidance on the types of control attributes that should be documented and maintained as part of the compliance program. As always, there is no one-size-fits-all approach, and each company will have to customize this matrix based on its particular needs and circumstances.

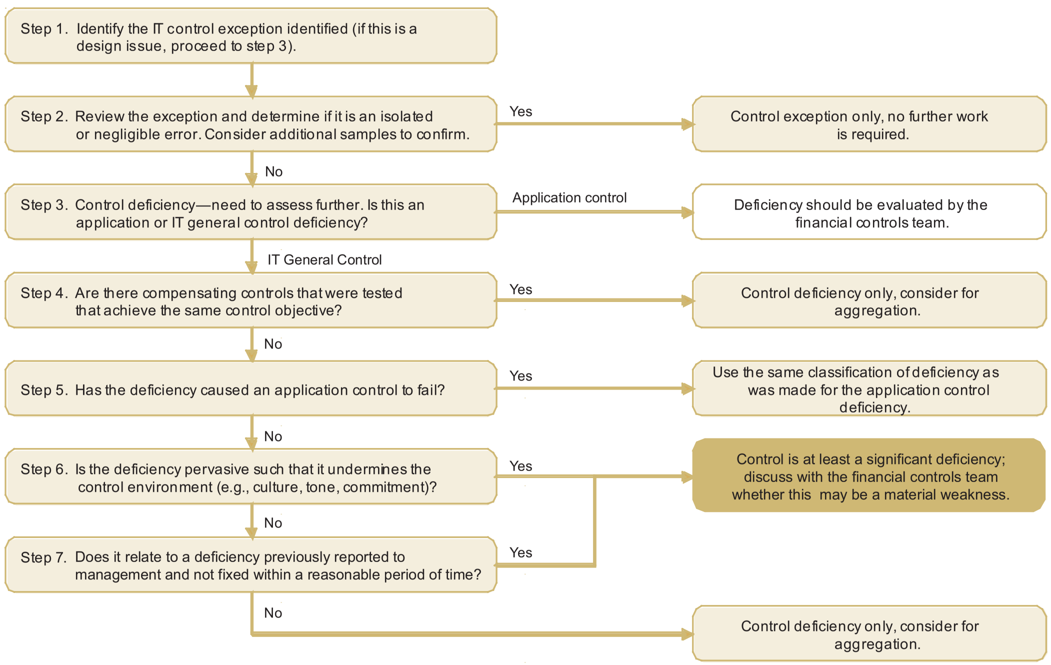
Figure 46—IT General Control Matrix

IT General Control Matrix				
Control Objective #:				
Conclusion: Controls are operating with sufficient effectiveness to achieve this objective.				
Control Activity	**Control Frequency**	**Sample Size**	**Test of Control**	**Results of Testing**

Appendix I—Sample Deficiency Evaluation Decision Tree

The decision tree in **figure 47** can be used to assist in the evaluation of control design or operating effectiveness issues. Companies should consult with their financial compliance teams and, ultimately, with their senior executive officers before concluding whether a control deficiency is a significant deficiency or a material weakness. This sample tree is not based upon authoritative pronouncement but reflects a common approach followed by many companies.

Figure 47—Sample Deficiency Evaluation Decision Tree


Step 1. Identify the IT control exception identified (if this is a design issue, proceed to step 3).
Step 2. Review the exception and determine if it is an isolated or negligible error. Consider additional samples to confirm.
Yes
Control exception only, no further work is required.
No
Step 3. Control deficiency—need to assess further. Is this an application or IT general control deficiency?
Application control
Deficiency should be evaluated by the financial controls team.
IT General Control
Step 4. Are there compensating controls that were tested that achieve the same control objective?
Yes
Control deficiency only, consider for aggregation.
No
Step 5. Has the deficiency caused an application control to fail?
Yes
Use the same classification of deficiency as was made for the application control deficiency.
No
Step 6. Is the deficiency pervasive such that it undermines the control environment (e.g., culture, tone, commitment)?
Yes
Control is at least a significant deficiency; discuss with the financial controls team whether this may be a material weakness.
No
Step 7. Does it relate to a deficiency previously reported to management and not fixed within a reasonable period of time?
Yes
No
Control deficiency only, consider for aggregation.

Appendix J—Sample Approach for Spreadsheets

Many companies rely on spreadsheets as tools in their financial reporting processes. Unfortunately, spreadsheets lack the inherent controls that many applications provide, including user access and change management controls. Therefore, significant risks are introduced into the financial reporting process.

The same scoping/top-down approach should be used to determine which spreadsheets should be evaluated as not all spreadsheets are of the same importance and risk. The objective is to identify those spreadsheets that are most significant to the financial reporting process and determine if controls are in place and whether they are tested in a reasonable manner. To do so, the following three-step approach has been developed using the guidance from **figure 27**. As always, professional judgment needs to be considered and customization of this approach made to suit the individual needs of each company. The three-step approach:

1. Spreadsheet inventory—Using the business process documentation as a starting point, inventory all spreadsheets that are involved in the financial reporting process and document the spreadsheet name, business process name related to the spreadsheet, financial statement line items impacted by the spreadsheet, description of what the spreadsheet does, and dollar value of transactions processed in the spreadsheet.
2. Risk assessment—For each of the spreadsheets inventoried, assess the impact and likelihood of financial statement error.
   - Impact—When assessing the impact of spreadsheets, organizations should consider the dollar value processed by the spreadsheet as well as how the spreadsheet is used.
   - Likelihood—When assessing the likelihood of error arising from a spreadsheet, organizations should consider the spreadsheet's complexity, the numbers of users and the frequency of changes made to the spreadsheet.

   Consider the guidelines provided in **figures 48** and **49** in performing an assessment of impact and likelihood.

   Using the impact and likelihood assessments, calculate a composite risk assessment (see **figure 50**) by multiplying the impact and likelihood assessments together. For instance, a spreadsheet that has an impact assessment of "2" (Moderate) and a likelihood assessment of "3" (High) would have a composite risk assessment of "6" (2*3). Once all spreadsheets have a composite risk assessment, prioritize them accordingly and be sure to review in aggregate to confirm the relative importance of spreadsheets.

Figure 48—Impact Assessment

Considerations for Assessing Impact	Low	Moderate	High
Total dollar value processed by the spreadsheet	<20% of materiality	20-50% of materiality	>50% of materiality
Purpose of the spreadsheet output	Analytical review	Financial reporting disclosures	Posting to the general ledger
Overall assessment of impact:	**(1-Low, 2-Moderate, 3-High)**		

Figure 49—Likelihood Assessment

Considerations for Assessing Likelihood	Low	Moderate	High
Complexity of the spreadsheet	Low (used for logging or data tracking)	Moderate (simple calculations or minor journal entries)	High (complex modeling, pivot tables, or other data source)
Number of users of the spreadsheet	1 user	<5 users	>5 users
Frequency of changes to the spreadsheet	Infrequent	Occasional	Frequent
Overall assessment of likelihood:		**(1-Low, 2-Moderate, 3-High)**	

Figure 50—Composite Risk Assessment

Assessment of Impact (1-3)	3 (Low)	6 (Moderate)	9 (High)
	2 (Low)	4 (Moderate)	6 (Moderate)
	1 (Low)	2 (Low)	3 (Low)
		Assessment of Likelihood (1-3)	

Once the risk rating is complete, establish an action plan to address the spreadsheets. The following action plan is provided as a guideline:

– Composite risk rating 1-3—The inherent risk of the spreadsheet is low. No action will be taken.
– Composite risk rating 4-6—The inherent risk of the spreadsheet is moderate. Implement and assess spreadsheet controls described in 3a-3c.
– Composite risk rating 7-9—The inherent risk of the spreadsheet is high. Implement and assess spreadsheet controls described in 3a-3g.

3. Implement/assess spreadsheet controls—Based on the composite risk ratings noted previously, the following spreadsheet controls are provided as a guideline. Other controls may be considered necessary depending on the circumstances of the organization and its use of spreadsheets.
   a) Access control—Limit access to the spreadsheets by storing them on a network server and assigning appropriate access restrictions.
   b) Change control—Establish a process for making changes to the spreadsheet, including documenting the change in a tab within the spreadsheet.
   c) Documentation—Ensure that the appropriate level of spreadsheet documentation is maintained and kept up to date to understand the business objective and specific functions of the spreadsheet.
   d) Testing—Formally test the spreadsheet by having someone who is independent of the business process review it. Have that individual confirm that the spreadsheet processing and related output is functioning as intended.
   e) Input control—Reconcile data inputs to source documents to confirm that data are input completely and accurately.
   f) Security and integrity of data—Prevent unauthorized or inadvertent changes to the spreadsheet by “locking” or protecting sensitive cells that are important for data processing, such as formulas and master data.
   g) Logic inspection—Have someone other than the user or developer of critical spreadsheets inspect the spreadsheets’ logic. This review should be formally documented.

Appendix K—Lessons Learned

There were many lessons learned during the first and second years of Sarbanes-Oxley implementation. The list in **figures 51** through **56** is not meant to be exhaustive, but illustrative of those experiences—organized by the steps outlined in the six-step IT compliance road map referenced in **figure 3**.

Figure 51—Lessons Learned—Plan and Scope

Lessons Learned	Way Forward
a) Inadequate organization and reporting structures were established so IT could not be fully integrated into the overall Sarbanes-Oxley steering committee of the organization. This led to ineffective overall communication.	Organizations should form an IT control subcommittee that is integrated into and reports to the overall Sarbanes-Oxley steering committee. The IT control subcommittee should oversee the IT Sarbanes-Oxley process, facilitate communication and integration with the overall Sarbanes-Oxley project, and facilitate the role of the independent auditors in the Sarbanes-Oxley IT process.
b) The responsibility for IT controls was not clearly defined. Common areas of confusion included identifying business owners for significant applications and those responsible for application controls and significant spreadsheets. This resulted in difficulties in ensuring that effective IT controls met the requirements for section 404.	The responsibility for IT controls should be clearly defined. Business owners of significant applications should be clearly identified. There should be formal agreement on responsibility for relevant application controls, significant spreadsheets and other end-user computing tools.
c) In many cases, the initial scope of the section 404 implementation process was not well understood. Further, some applications that were not relevant to the financial reporting process were not taken out of scope, and some applications that should have been included were not included until an issue was raised by the external auditor. This led to over- or underscoping for IT controls to meet the requirements for section 404. A top-down approach to planning and scoping IT controls was often not taken. Both management and auditors frequently began testing control activities without considering the impact on risks of other COSO controls. Considerable work was performed at the control activity level that could potentially have been reduced as other controls may have	Additional guidance from PCAOB, as well as experience and lessons learned from complying with section 404 during the last two years, has resulted in a better understanding of the scoping process for documenting and testing the effectiveness of IT controls. Organizations should refer to the scoping section (within the road map) in this document to leverage the experience gained and adopt a more streamlined and cost-effective scoping process for documenting and testing the effectiveness of IT controls. Organizations should adopt a top-down approach as described in the planning and scoping section in this document to avoid any over- or underscoping for testing IT controls and achieve a more streamlined and cost-effective scoping process.

Figure 51—Lessons Learned—Plan and Scope *(cont.)*

Lessons Learned	Way Forward
reduced the risk that relevant control breakdowns would not be detected. Without the top-down approach, over- or underscoping for IT controls could result.	
d) Implementation plans did not include communication plans. Without formal communication plans, new controls were not always implemented effectively. Communication plans are necessary so stakeholders are kept informed of progress and their responsibilities.	Communication plans should be included as part of the implementation rollout plans for new controls. For example, as new policies are developed, there should be a plan to communicate these to employees and contractors.
e) The time frames to execute work for the external auditors were not included in implementation plans. Thus, some external audit work was performed later than preferred. In some cases, significant deficiencies were not identified until late in the process and could not be remediated until after year-end.	Planning with external auditors should be completed early during the year, including agreeing on a time frame for executing the work. The time frame should be communicated to all responsible for IT controls. This will help ensure that there will be time allowed to remediate any significant deficiencies and for external auditors to perform year-end testing.
f) Opportunities to implement standardized or centralized controls were missed, or the potential impact of standardized or centralized controls and processes on the testing strategy were not considered. This resulted in ineffective internal controls and increased testing efforts.	Organizations should implement a standardized and centralized internal control platform to help achieve design and operating effectiveness. In addition, organizations should customize their testing strategy to be compatible with the standardized and centralized internal control structure. Such an approach will achieve a more efficient and effective process of testing controls.
g) There was often poor communication between Sarbanes-Oxley financial/operational teams and IT teams. Both teams often identified relevant controls that addressed the same control objectives. In addition, opportunities for relying on automated controls rather than manual controls were missed and assumptions about the adequacy of the controls in the other team's area were sometimes invalid. This led to redundancy of work performed.	Sarbanes-Oxley financial/operational teams and IT teams should work collaboratively to ensure effective communication. Where possible, they should integrate their assessment of controls, both manual and automated, to draw a conclusion on the overall control effectiveness for any given business processes. In addition, when appropriate, the two teams should work closely to ensure that more reliance be placed on automated controls rather than manual controls.
h) Other than spreadsheets and word processing software, there was little automation of the compliance process. It was often difficult to track progress or identify the root causes of control deficiencies that could be addressed with a single solution.	Organizations should consider automating the compliance process to gain productivity, track progress more effectively and identify the root cause of any control deficiency.

Figure 51—Lessons Learned—Plan and Scope *(cont.)*

Lessons Learned	Way Forward
i) The skill sets required to address implementation needs were often in short supply, e.g., control design, risk assessments and documentation. In the final quarter of a year, it became increasingly difficult to find and retain public accounting audit expertise as this was focused on meeting the firm's external audit obligations. Often, the required external expertise was more costly than initially anticipated. This increased the risk of not being able to remediate all deficiencies identified and not meeting the requirements of section 404.	Organizations should plan ahead to secure internal resources with the appropriate skill sets early in the year. This could include recruiting, outsourcing or training internal resources to acquire the required skill sets.
j) In many cases, internal audit provided significant assistance in the 404 implementation effort. However, this meant that internal audit plans could not be achieved and areas of risk outside of financial reporting may not have been reviewed. There was also an independence issue as auditors who design controls should not be reviewing and testing the controls they have implemented. This may have an impact on internal audit activity in the future.	The organization's audit committee and Sarbanes-Oxley steering committee should coordinate and approve the allocation of resources to internal audit and section 404 compliance efforts early in the year. In addition, internal audit should only recommend controls and business process owners should have the final say in determining, approving and implementing improved controls. As such, internal audit could maintain independence when testing control effectiveness. If possible, section 404 compliance should be implemented as part of the ongoing business processes instead of annual projects.
k) The potential to use the internal audit function to test the controls self-assessment process as part of its normal audit plans was not considered. The potential impact of a controls self-assessment process to reduce the testing of control activities was not considered.	Organizations should consider utilizing a controls self-assessment process to reduce the testing of control activities.
l) The fact that an application is included in scope indicates that it supports a relevant application control required for Sarbanes-Oxley compliance. In most cases, the application and its related subsystems had to be assessed, even if the application supported a very limited number of relevant application control. This resulted in documenting and testing controls in applications that could have been excluded from the scope.	If the application supports just one control, consideration could be given to eliminating the application control (and therefore the application itself) and either identifying a relevant manual control or increasing reliance on existing manual controls to reduce overall effort. While this is rare, it is a consideration for companies that have many applications that support very few controls. Care should be taken to ensure that inadvertent reliance does not occur in these situations (e.g., relying on a system-generated report).

Figure 52—Lessons Learned—Assess Risks

Lessons Learned	Way Forward
a) The risks associated with IT general controls were often not considered. Levels of tests were often set at a higher level than necessary for low-risk areas. Conversely, the impact of higher risks was not considered on the level of testing. Failure to assess the risk on the IT environment in relation to the financial reporting resulted in over- or underscoping for 404 compliance. Risk assessments were often not performed on IT general controls. Absent the assessment of risk on the IT environment in relation to the financial reporting, over- or underscoping for the 404 compliance resulted.	Organizations should consider the process described in step 2, Assess IT Risk, of the IT Compliance Road Map section of this document and customize the IT risk assessment process to fit their particular needs.

Figure 53—Lessons Learned—Identify and Document Controls

Lessons Learned	Way Forward
a) In a number of cases, the external auditors were not consulted about the nature and extent of the documentation required. This meant that a process could have been overdocumented and that documentation could become quickly out of date. Similarly, a process could have been underdocumented and additional work would have to be performed.	Organizations should work closely with their external auditor early in the year to help ensure that the scope, approach used, nature and extent of documentation, and expected deliverables will meet their requirements. Organizations and their external auditors should communicate on an ongoing basis during the year to address SEC and PCAOB's new requirements and guidance.
b) A holistic approach to the control framework was not taken. The impact of manual controls, automated application controls, IT general controls, monitoring controls (including internal audit as a periodic monitoring control) and the control environment were not considered in their entirety in the risk assessment process when such consideration could have reduced the risk of unnecessary testing.	Organizations should adopt a holistic approach to the control framework whereby the financial and IT auditors work collaboratively to assess the impact of the entire control environment in the organization. This should include reviewing the manual controls, automated application controls, IT general controls and monitoring controls, and determining the optimal approach to testing controls.

Figure 54—Lessons Learned—Evaluate Design and Operating Effectiveness

Lessons Learned	Way Forward
a) Process documentation often became the relevant objective instead of serving as an aid to identifying relevant controls. This led to not fully identifying all relevant controls.	Process documentation is not the end but the means to achieving reasonable support for documenting business processes supporting significant accounts at the company and transaction level. As part of this process, organizations should identify risks that could result in misstatement and controls to address these risks. After identifying significant accounts, relevant assertions and significant processes, organizations should consider the steps described in step 3 of the IT Compliance Road Map section of this document to identify the relevant controls to be tested.
b) In some instances, all controls identified were considered to be relevant controls, resulting in unnecessary testing.	Organizations should critically differentiate relevant controls from other controls to ensure an appropriate level of effort in documenting and testing relevant controls. As noted previously, organizations should also consider the actions described in step 3 of the IT Compliance Road Map section of this document to identify the relevant controls to be tested.
c) The documentation required for parameter-driven IT general controls and the documentation of process-driven IT general controls was not considered. This resulted in inadequate documentation of the internal control structure.	The effort to document and assess internal controls should address parameter-driven as well as process-driven IT general controls.
d) In some cases, a centralized gap list, including manual control gaps, IT application control gaps and IT general control gaps, was not created. This made it difficult to assess potential compensating controls and determine if solutions to common control gaps could be remediated centrally, rather than having individual groups create different solutions for the same issue.	Organizations should develop a centralized gap repository including manual control gaps, IT application control gaps and IT general control gaps. Related compensating controls should be identified to determine the most appropriate remediation solution.
e) Walk-throughs of parameter-driven IT general controls were sometimes reperformed during the evaluation of operational effectiveness. This led to redundant documentation and testing.	As a general rule, organizations should not perform redundant tasks in the documentation and testing of IT controls. This applies to, among others, walk-throughs of parameter-driven IT general controls.

Figure 54—Lessons Learned—Evaluate Design and Operating Effectiveness *(cont.)*

Lessons Learned	Way Forward
f) Service auditor reports were not mapped to the risk and control matrix (which should also include the organization's controls). This resulted in relevant controls not being detected. Similarly, there was often confusion as to whether the controls documented in the service organization's narrative, but not in the service auditor's narrative, could be relied upon or whether additional management testing was required.	When preparing the risk and control matrix, organizations should include the control documentation and test results from the service auditor's report. This will help ensure that all relevant controls, in-house or outsourced, are being considered for overall and aggregate control assessment. Reliance should be placed on the control narratives in the service auditor's report.

Figure 55—Lessons Learned—Prioritize and Remediate Deficiencies

Lessons Learned	Way Forward
a) In some cases, rather than management identifying relevant controls and deficiencies, the external auditor challenged management's assessment. Management accepted the external auditor's assessment and performed additional work. This led to some control deficiencies being identified late in the year. As a result, management did not have enough time to take remedial action.	Organizations should communicate early and on an ongoing basis with their external auditor to help ensure that the relevant controls identified by management are meeting the external auditor's scope and expectations. This will help avoid the need for management to perform additional work at the end of the year.

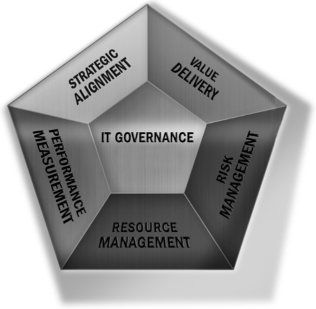
Figure 56—Lessons Learned—Build Sustainability

Lessons Learned	Way Forward
a) There were often no postimplementation reviews or assessments of how the Sarbanes-Oxley process could be improved. Once one year's section 404 process was completed, the next year's started. When postimplementation reviews were performed, they did not always include all stakeholders. This could lead to missed opportunities that could have resulted in time and cost savings to the compliance process.	Organizations should perform postimplementation reviews with all stakeholders to assess how their Sarbanes-Oxley process could be improved. In this way, management can identify lessons learned and implement more cost-effective plans for the following year.

Figure 56—Lessons Learned—Build Sustainability *(cont.)*

Lessons Learned	Way Forward
b) Consideration was not given to extending the Sarbanes-Oxley compliance framework to monitor compliance in other regulatory areas and to comply with overall company policies. This resulted in duplication in efforts in meeting multiple regulatory and governance requirements.	Organizations should consider extending the Sarbanes-Oxley compliance framework to include compliance with company policies and other regulatory requirements. This will help to optimize the overall organizational compliance efforts.
c) Compliance with section 404 requirements was often initiated to meet regulatory requirements as a one-off project, instead of integrating the IT governance part into the corporate governance process. This led to an inability to sustain long-term compliance.	Organizations should consider implementing the following relevant focus areas of IT governance as part of overall corporate governance: • Strategic alignment • Value delivery • Resource management • Risk management • Performance measurement Refer to **figure 57** and COBIT 4.0 for more information. The implementation of IT governance will help organizations continue to advance in the control reliability model, as outlined in **figure 5**, and build long-term sustainability.

Figure 57—IT Governance Focus Areas



- **Strategic alignment** focuses on ensuring the linkage of business and IT plans; on defining, maintaining and validating the IT value proposition; and on aligning IT operations with enterprise operations.
- **Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.
- **Resource management** is about the optimal investment in, and the proper management of, critical IT resources, including applications, information, infrastructure and people. Key issues relate to the optimization of knowledge and infrastructure.
- **Risk management** requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise, and embedding of risk management responsibilities into the organization.
- **Performance measurement** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

Appendix L—Issues in Using SAS 70 Examination Reports

Many organizations outsource a portion of their operations, including information systems, to service organizations. AICPA US Auditing Standards section 324 “Service Organizations” (SAS 70) paragraph 3 (AU 324.03) states:

> *A service organization’s services are part of an entity’s information system if they affect any of the following:*
> - *The classes of transactions in the entity’s operations that are significant to the entity’s financial statements*
> - *The procedures, both automated and manual, by which the entity’s transactions are initiated, recorded, processed, and reported from their occurrence to their inclusion in the financial statements*
> - *The related accounting records, whether electronic or manual, supporting information, and specific accounts in the entity’s financial statements involved in initiating, recording, processing and reporting the entity’s transactions*
> - *How the entity’s information system captures other events and conditions that are significant to the financial statements*
> - *The financial reporting process used to prepare the entity’s financial statements, including significant accounting estimates and disclosures*

When a service organization’s services are part of an organization’s information system, they are part of internal control over financial reporting, and in accordance with PCAOB Auditing Standard No. 2, management should consider the activities of the service organization in making its assessment of internal control over financial reporting. Auditing Standard No. 2 permits management and the organization’s auditor(s) to rely on a service auditor’s report on controls placed in operation and tests of operating effectiveness (SAS 70 report) to support the assessment and opinion if the SAS 70 report is deemed sufficient.

The remainder of this appendix identifies issues by SAS 70 topics that may exist or surface when evaluating the sufficiency of a SAS 70 report.

Scope

There are several issues that may result in the scope of the SAS 70 report not being sufficient to provide the evidence that the service organization’s controls are operating effectively. These issues include the following:

- The description of controls is not relevant or is relevant to only a portion of the outsourced services that are part of the information system.

- The description of controls does not sufficiently cover the service organization locations that provide services to the user organization.
- The service organization relies on a subservicer, the subservicer has been "carved out" of the scope of the SAS 70 report and no SAS 70 report is available from the subservicer.

In these instances, management and the auditor(s) should consider:

- Obtaining an understanding of the controls placed in operation at the service organization that are not covered by a SAS 70 report and are relevant to the user organization's financial statement assertions
- Obtaining evidence that the controls are operating effectively through direct testing or other means

In performing these procedures, management and the auditor(s) should recognize that the procedures to be performed will vary depending on the importance of the controls at the service organization to management's assessment and on the level of interaction between the company's controls and the controls at the service organization.

Description of Controls

PCAOB Auditing Standard No. 2, paragraph B20 states that the description of controls provided by the service organization is designed to permit user organizations and their auditors to obtain:

> *… an understanding of the controls at the service organization that are relevant to the entity's internal control and the controls at the user organization over the activities of the service organization.*

While the service organization is responsible for fair presentation of the description of controls and the service auditor opines on the fairness of the description, unique aspects of the user organization's process and financial statement assertions may result in the description of controls not meeting the needs of the user organization and its auditors.

Issue: The description of controls is not presented at a level of detail that is sufficient to permit management or the auditor(s) to:

- Identify types of user organization financial statement assertions that are likely to be affected by the controls and sources of potential misstatements
- Consider factors that affect the risk of material misstatement
- Support management's assessment with regard to internal control
- Support the auditor's opinion on internal controls

Issue: The control objectives specified by management of the service organization do not address all of the financial statement assertion risks identified by user management or are not sufficiently described to determine whether the risks have been addressed.

Issue: The controls specified by management, in the judgment of user management or the user auditor(s), are not sufficient to achieve the specified control objectives as they relate to the user organization's financial statement assertions.

Issue: The description of controls does not present sufficient information about the relevant entity-level IT controls to permit user organization management or the user auditor(s) to assess their operating effectiveness in establishing, enhancing, or mitigating the effectiveness of the activity-level IT controls.

These issues may often be addressed by augmenting the description of controls presented in the SAS 70 report with information available from a variety of sources, such as user manuals, system overviews, technical manuals, the contract between the user organization and the service organization, and reports by internal auditors and regulatory authorities of the service organization. This information may need to be supplemented with information obtained directly from the service organization through verbal or written inquiry and response.

Issue: The description of controls does not contain a description of controls that should be in place at the user organization that were contemplated in the design of the service organization's controls.

The controls at service organizations are usually designed in such a manner that effective internal control over the processes requires the user organizations to implement certain controls. If the description of controls does not identify such user organization controls, the user organizations and their auditors consider whether any controls should have been identified. In making this evaluation, user organizations may wish to compare the sources of potential misstatements they have identified to the controls from the SAS 70 report.

Timing

An inherent tradeoff exists between the need for management and the auditor(s) to have the most current evaluation of service organization controls possible and the receipt of the SAS 70 report with sufficient timeliness that any control exceptions or control objective qualification can be assessed and the risk mitigated. This tradeoff often results in the SAS 70 report date preceding the balance sheet date of the user organization. This results in two issues that may need to be addressed.

First, significant changes have occurred to the controls over the services provided during the period of time that has elapsed between the time period covered by the tests of operating effectiveness and the date of management's assessment.

If a significant change(s) has occurred in the controls at the service organization, management and the auditor(s) should consider:

- Obtaining an understanding of the controls that have changed and are relevant to the user organization's financial statement assertions
- Obtaining evidence that the changed controls are operating effectively

Change notifications, technical manual updates, training materials and other communications from the service organization are often sufficient to permit management and the auditor(s) to understand the effect of the change on the user organization's financial statement assertions. However, additional inquiry of service organization personnel, supplemented with the receipt of additional documentation, may be necessary.

Evidence that the changed controls are operating effectively may be more difficult to obtain. If the service organization maintains effective IT general controls, management and the auditor(s) may be able to evidence the functioning of application control changes at the user organization site through direct tests of the application controls or participation in user acceptance testing and inspection of the results of the testing.

In other instances, the changed controls may be redundant with controls in place and functioning at the user organization. In these instances, management and the auditor(s) may choose to test these redundant controls. Finally, management or the auditor(s) may determine that the control can be tested only at the service organization location. In these instances, management or the auditor may need to travel to the service organization location or make arrangement to have the service auditor test the changed controls and issue an agreed-upon procedures or attestation report.

The nature and extent of management and the auditor's procedures will vary depending on the importance of the controls to management's assessment and on the level of interaction between the company's controls and the controls at the service organization.

The second timing issue is that a significant period of time has elapsed between the time period covered by the tests of operating effectiveness and the date of management's assertions.

In such a case, there is a risk that the controls at the service organization have changed or have ceased to operate effectively. Management should perform procedures to identify whether any such changes have occurred. The procedures to be performed are discussed in PCAOB Auditing Standard No. 2, paragraphs B25 through B27. If a change in the controls of the service organization has occurred, it should be assessed in the manner described above.

Nature and Extent of Testing

When the nature or extent of testing performed by the service auditor is not sufficient to support management's assessment of controls as they relate to the financial statement assertions, management and the auditor(s) need to perform additional procedures.

Issue: The report covers controls placed in operation but does not include tests of operating effectiveness.

Issue: The tests of operating effectiveness of controls specified by the service organization do not provide sufficient evidential matter to support a conclusion about control risk for the financial statement assertions of the user organization.

PCAOB Audit Standard No. 2, paragraph B21 notes:

> *A service auditor's report that does not include tests of controls, results of the tests, and the service auditor's opinion on operating effectiveness (in other words, reports on controls placed in operation described in paragraph .24a of AU sec. 324) does not provide evidence of operating effectiveness.*

A similar problem exists if the controls specified in the report are not sufficiently tested to address the financial statement risks identified by management. SAS 70 states that in these instances:

> *Evidence that the controls that are relevant to management's assessment and the auditor's opinion are operating effectively may be obtained by following the procedures described in paragraph .12 of AU sec. 324. These procedures include:*
>
> *a. Performing tests of the user organization's controls over the activities of the service organization (for example, testing the user organization's independent reperformance of selected items processed by the service organization or testing the user organization's reconciliation of output reports with source documents).*
> *b. Performing tests of controls at the service organization.*

If the service organization makes an agreed-upon procedures report available that reports on procedures performed to test the operating effectiveness of the controls described in the description of controls, management and the auditor(s) should evaluate the sufficiency of the testing performed in a manner similar to that used for evaluating reports on controls placed in operation.

Issue: The description of the tests of controls is not presented in sufficient detail regarding the nature, timing and extent of testing to permit management or the user auditor to assess the control risk for the financial statement assertions of the user organization.

In this instance, management and the auditor may be able to arrange a discussion with the service organization and its auditor(s) to obtain additional information regarding the description of the tests. Such inquiries and the responses should be documented in accordance with standards and an evaluation of the sufficiency of the responses received.

If such a discussion cannot be arranged, the specific testing should be treated as providing insufficient evidential matter to support a conclusion.

Issue: The description of tests performed on the relevant aspects of the control environment, information and communication, risk assessment, and monitoring related to the services provided is not sufficient to permit user organization management or the auditor(s) to assess their operating effectiveness in establishing, enhancing or mitigating the effectiveness of the specified controls.

According to SAS 70, if the description of tests performed does not include tests of "the relevant aspects of the control environment, information and communication, risk assessment, and monitoring related to the services provided," management and the user auditor(s) should consider the importance of these controls to management's assessment and the level of interaction between the company's controls and the controls at the service organization. Management and the auditor(s) should then consider performing limited procedures to test these controls through inquiry and inspection of regulatory filings and other documents.

Issue: In describing the results of tests of operating effectiveness performed, the description of exceptions is not sufficient (e.g., sample size, number of exceptions noted, the nature of the exceptions, causative factors, corrective actions or other relevant qualitative information) to permit management or the user auditor(s) to assess their impact on the control risk for the financial statement assertions of the user organization.

In this instance, management and the auditor may be able to arrange a discussion with the service organization and its auditor to obtain additional information regarding the description of the exception(s). Such inquiries and the responses should be documented in accordance with standards, and the control should be evaluated based on the response received.

If such a discussion cannot be arranged, management and the auditor(s) should consider the control as not operating effectively and should evaluate its impact on the user organization's financial statement assertions.

Qualifications and Exceptions

Issue: The opinion of the service auditor or the exceptions reported within the Information Provided by the Service Auditor section of the report result in the evaluation of those aspects of internal control provided by the service organization as ineffective.

When the service auditor's opinion contains a qualification in the opinion or an exception is noted in the description of the results of testing, management should identify the qualification or exception as a control deficiency and identify any controls implemented by the user organization that compensate for the control deficiency noted, or otherwise mitigate the risk associated with the deficiency. The deficiency should then be evaluated in accordance with the user organization's methodology for evaluating deficiencies.

Issue: Qualifications contained within the service auditor's opinion are not sufficiently described to permit user management or the user auditor(s) to assess the impact on the control risk for the financial statement assertions of the user organization.

In this instance, management and the auditor may be able to arrange a discussion with the service organization and its auditor(s) to obtain additional information regarding the description of the qualification. Such inquiries and the responses should be documented in accordance with standards, and the control objective and related controls should be evaluated based on the response received.

If such a discussion cannot be arranged, management and the auditor(s) should consider the control objectives as not having been achieved and should evaluate its impact on the user organization's financial statement assertions.

Service Auditor

Issue: The reputation, competence, independence and professional standing of the service auditor are not sufficient to support management's assessment and the auditor's opinion.

PCAOB Auditing Standard No. 2, paragraph B24 requires:

> *In determining whether the service auditor's report provides sufficient evidence to support management's assessment and the auditor's opinion, management and the auditor should make inquiries concerning the service auditor's reputation, competence, and independence. Appropriate sources of information concerning the professional reputation of the service auditor are discussed in paragraph .10a of AU sec. 543, Part of Audit Performed by Other Independent Auditors.*

Where the reputation, competence, independence or professional standing of the service auditor is not sufficient, management and the auditor should deem the nature and extent of the procedures performed to be insufficient and should perform such procedures noted previously.

Appendix M—Segregation of Duties in Significant Accounting Applications

Adequate segregation of duties is an important consideration in determining if a company's control activities are effective in achieving the objectives of internal control. The basic concept underlying segregation of duties is that no employee or group should be in a position both to perpetrate and to conceal errors or fraud in the normal course of their duties. In general, the principal incompatible duties to be segregated are:

- Authorization or approval of related transactions affecting those assets
- Custody of assets
- Recording or reporting of related transactions

Traditional systems of internal control have relied on assigning these duties to different individuals or segregating incompatible functions. Such segregation of duties is intended to prevent one person from having both access to assets and responsibility for maintaining the accountability for such assets. In the IT environment, the segregation of functions is historically considered and tested as a critical component of IT general controls. For example, companies implement controls that restrict to authorized individuals the ability to migrate programs to production. Likewise, companies usually segregate duties over requesting and granting access to systems and data.

However, appropriate segregation of functions is also critical at the application/business process level. For instance, in an inventory management system, different individuals are typically responsible for duties such as:

- Initiating or requesting a purchase
- Placing and inputting purchase orders
- Receiving goods
- Ensuring custody of inventories
- Maintaining inventory records and/or authorizing adjustments to costs or quantities, including authorizing disposal or scrapping
- Making changes to inventory master files
- Performing independent inventory counts
- Following up on inventory count discrepancies
- Authorizing production requests and/or material transfers
- Receiving/transferring goods into/from manufacturing
- Shipping goods

A challenge facing many companies is identifying these incompatible or conflicting duties at the application level. Legacy system environments necessitated and facilitated the segregation of duties because of the predominantly manual control framework surrounding them. The fragmentation of legacy systems also facilitated the segregation of duties since purchasing systems, inventory systems and general ledger systems were separate. However, this traditional notion of segregation of duties needs to be refined in a fully automated ERP system environment. ERP systems have shifted the emphasis to user empowerment, enabling users to have access across business functions, or, alternatively, to handle physical assets and record their movements directly into the computing and accounting systems. The notion of segregation of duties control needs to be developed to include a risk management perspective and a tradeoff balance.

There are various approaches to identifying segregation of duty conflicts at the business process level. What follows are two examples of tools/templates that companies might be able to leverage/adapt for their environments. The first one in **figure 58** may be more applicable for legacy systems, and the second in **figure 59** for integrated systems.

Figure 58 is an illustration of an approach to highlight conflicting duties performed as it relates to a sales application. Similar documents would need to be created for other significant applications involved in financial reporting. The template is completed by indicating the name(s) of the individual(s) responsible for each function within the applications listed. If a function is performed by a computer application, “computer” or “IT” can be entered as the individual.

Figure 58—Sales Application

	Authorization	Custody of Assets	Recording	Control Activity
Issues sales orders				
Approves credit and credit terms				
Approves access to credit-related data files				
Authorizes shipments				
Initiates shipping documents				
Handles inventories ready for shipment				
Initiates billings				
Verifies accuracy of billings				
Approves access to pricing-related data files				
Approves deviations from standard prices				
Verifies completeness of billings				
Maintains sales records				
Maintains accounts receivable records				
Reconciles shipments to billings				
Reconciles accounts receivable records to the general ledger				

After the form(s) has been completed for each significant application, it is reviewed for any instances where one individual is performing duties that would be considered to be incompatible. Potentially incompatible duties exist if one individual performs duties in more than one category (authorization or approval, custody, or recording/reporting) or if an individual is responsible for performing a control over the same transaction that the individual is responsible for recording/reporting. In addition, when no one performs a duty, it may indicate a weakness in controls. Keep in mind that not all instances where an individual performs duties in more than one column represent a lack of segregation of duties. In addition, companies need to consider that there is the possibility of a lack of segregation of duties within the same category (e.g., the individual who authorizes credit also approves the write-off of uncollectible accounts).

Once an individual is identified as performing incompatible duties, all duties performed by that individual should be considered to determine whether the effectiveness of those duties is reduced or eliminated by the lack of segregation of duties. If it is, the next step is to address the effects on the controls over the applications(s) and the risk of error or fraud. If an increase in risk is identified, companies should look for other controls that would prevent or detect such risk and assess their effectiveness. If no additional controls are identified, the risk of a financial reporting error would be greater due to the lack of segregation of duties.

A second approach to evaluating segregation of duties is to utilize a matrix that lists business process functions. Within the matrix, companies indicate which functions are compatible and would not create a conflict if performed by the same individual. As part of Sarbanes-Oxley 404 compliance, many companies have developed such segregation of duties matrices that reflect their risk management perspective and the tradeoff between functional access and security. Such templates should be modeled for each business process in the organization and appropriate tradeoffs made between empowerment and the need to minimize the risk of fraud or unauthorized transactions. **Figure 59** is an example of applying this concept to the purchase-to-pay business function. As illustrated in the example, an “x” would indicate an incompatible function based on management’s definition of incompatible duties.

Figure 59—Purchase-to-pay Segregation of Duties Matrix

Functions	Create and maintain vendor records.	Approve/release purchase orders.	Process goods receipt.	Process vendor invoices.	Process cash payment.	Release blocked invoices.	Enter vendor debit memos.
Create and maintain vendor records.		X	X	X			
Approve/release purchase orders.			X	X			
Process goods receipt.				X			
Process vendor invoices.						X	X
Cash payment processing.							X
Release blocked invoices.							
Enter vendor debit memos.							

Specific techniques for automating the testing of segregation of duties are beyond what is covered here. However, a starting point is to consider reports that might already be available within the system itself. Audit software should also be considered to automate as much of the review and testing process as possible.

Appendix N—List of Figures

References

Committee of Sponsoring Organizations of the Treadway Commission

(COSO), *Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting*, USA, July 2006, *www.coso.org*

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management Framework*, USA, September 2004, *www.coso.org*

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control—Integrated Framework*, USA, 1992, *www.coso.org*

CSE (Canada), SCSSI (France), BSII (Germany), NLNCSA (Netherlands), CESG (UK), NIST (USA) and NSA (USA), *Common Criteria and Methodology for Information Technology Security Evaluation*, 1999

Deloitte & Touche LLP, "Moving Forward–A Guide to Improving Corporate Governance Through Effective Internal Control," 2003

Deloitte & Touche LLP, "Taking Control, A Guide to Compliance with Section 404 of the Sarbanes-Oxley Act of 2002," 2003

Dewitt, Ron; "Managing Change is Managing People," 30 April 2004, *www.cioupdate.com*

Ernst & Young LLP, "The Sarbanes-Oxley Act of 2002, The Current Landscape—Rules, Updates and Business Trends," 2003

International Organization for Standardization (ISO), *Code of Practice for Information Security Management*, ISO/IEC 17799, Switzerland, 2005

IT Governance Institute, COBIT 4.0, USA, 2005, *www.itgi.org*

IT Governance Institute, *Board Briefing on IT Governance, 2nd Edition*, USA, 2003, *www.itgi.org*

IT Governance Institute, *IT Governance Implementation Guide*, USA, 2003, *www.itgi.org*

KPMG, "The Defining Issues—Implications of Proposed Auditing Standard on Internal Control," 2003

LaMarsh & Associates Inc., Managed Change™ Model, USA

Office of Government Commerce (OGC), Central Computer and Telecommunications Agency (CCTA), IT Infrastructure Library (ITIL), UK, 1989

Public Company Accounting Oversight Board, "Report on the Initial Implementation of Auditing Standard No. 2," Standard: Release No. 2005-023, USA, 30 November 2005

Public Company Accounting Oversight Board, Staff Questions and Answers on Auditing Internal Control Over Financial Reporting, USA, 16 May, 21 January 2005

Public Company Accounting Oversight Board, Staff Questions and Answers on Auditing Internal Control Over Financial Reporting, USA, 22 November, 6 October 2004

Public Company Accounting Oversight Board, Staff Questions and Answers on Auditing Internal Control Over Financial Reporting, USA, 23 June 2004, revised 27 July 2004

Public Company Accounting Oversight Board, "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements," Final Auditing Standard: Release No. 2004-00 1, USA, 9 March 2004

PricewaterhouseCoopers LLP, "The Sarbanes-Oxley Act of 2002, Strategies for Meeting New Internal Control Reporting Challenges," 2003

PricewaterhouseCoopers LLP, "Understanding the Independent Auditor's Role in Building Trust," 2003

Securities and Exchange Commission, Concept Release Concerning Management's Reports on Internal Control Over Financial Reporting (Release No. 34-54122, File No. 57-11-06), USA, 11 June 2006

Securities and Exchange Commission, SEC Announces Next Steps for Sarbanes-Oxley Implementation, USA, 17 May 2006

Securities and Exchange Commission, Commission Statement on Implementation of Internal Control Reporting Requirements, USA, 16 May 2005

Securities and Exchange Commission, Office of the Chief Accountant, "Division of Corporation Finance: Staff Statement on Management's Report on Internal Control Over Financial Reporting," USA, 16 May 2005

Securities and Exchange Commission, Office of the Chief Accountant, "Division of Corporation Finance: Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports-Frequently Asked Questions," USA, revised October 6, 2004

Securities and Exchange Commission, "Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports," Release Nos. 33-8238; 34-47986; IC-26068; File Nos. S7-40-02; S7-06-03, USA, June 2003, *www.sec.gov/rules/final/33-8238.htm*

Attribution

Figures 2, 3, 4, 30, 31, 32, 33 and 34 in this document have been provided by Deloitte & Touche LLP.