Information Systems Audit and Control Association®

IT GOVERNANCE INSTITUTE®

3701 ALGONQUIN ROAD, SUITE 1010 TELEPHONE: 847.253.1545
ROLLING MEADOWS, ILLINOIS 60008, USA FACSIMILE 847.253.1443
WEB SITES: *www.isaca.org* and *www.itgi.org*

November 21, 2003

Office of the Secretary
Public Company Accounting Oversight Board
1666 K Street, NW
Washington, DC 20006-2803

Via E-mail to comments@pcaobus.org

RE: PCAOB Rulemaking Docket Matter No. 008
PCAOB Release No. 2003-017, October 7, 2003
(Proposed Auditing Standard – An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements)

Dear Board Members:

We very much appreciate the opportunity to provide comments to the Public Company Accounting Oversight Board's ("Board" or "PCAOB") proposed auditing standard. These comments are offered on behalf of the Information Systems Audit and Control Association (ISACA) and IT Governance Institute (ITGI), in my capacity as the International President of both of these organizations.

ISACA is an international professional, technical and educational organization dedicated to being a recognized global leader in IT governance, security, control and assurance. With members in more than 100 countries, ISACA is uniquely positioned to fulfill the role of a central, harmonizing source of IT control practice standards the world over. Its strategic alliances with other organizations in the financial, accounting, auditing and IT professions ensure an unparalleled level of integration and commitment by business process owners.

ITGI strives to assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals. Its goals are to raise awareness and understanding among, and provide guidance and tools to, boards of directors, executive management and chief information officers (CIOs). The ultimate goal is to ensure that IT meets and exceeds expectations, and its risks are mitigated.

Taken as a whole, we support the draft standard and what it sets out to accomplish. We list below our comments on some of the areas covered in the draft standard. We have made comments in 4 areas:

- IT Controls—We suggest clarification of some of the IT control-related terminology used in the standard.

- IT Control Framework—We suggest an alternative view of IT controls using the *Control Objectives for Information and related Technology* (COBIT) as a formal guidance framework.
- Reliance on IT Internal Audit—We suggest revisiting this area and allowing public accounting firms to rely on the work of IT internal audit.
- Audit Committee Effectiveness—We suggest that additional definition regarding the role of the audit committee in the IT governance area be provided, and that the IT Governance Institute be used as a resource for this.

IT Controls

We note that "IT general controls" are referred to throughout the proposed standard. However, the scope of the IT general controls is not defined. We are concerned that organizations and auditors may focus on only the control activities component of general controls defined in COSO, i.e., "General controls commonly include controls over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance." We explain below what we feel is a more comprehensive view of IT controls.

We also noted an inconsistency and lack of clarity in the references to application controls within the draft standard. We feel that this should be addressed as well, and provide below a view on how this could be accomplished.

If the scope of IT general and application controls is not further clarified, then there is an increased risk that organizations and their auditors will not consider the entire IT governance framework in their evaluation of the effectiveness of the financial reporting control framework. We believe that further clarification and definition of the term "certain information technology general controls" used within the document should be considered. Once again, we offer the alternative detailed below to cover this concern.

As noted in our recent publication, *IT Control Objectives for Sarbanes-Oxley*, which we have attached to this submission, IT controls apply to all COSO components, not just the control activities component. We believe that the Board may want to consider referencing COBIT within the final guidance, as a framework for the IT control environment, much as COSO has been recommended as the internal control framework (see the Framework section below for further clarification).

COSO identifies five essential components of effective internal control. Below, we highlight, in each of the five COSO component areas, our rationale for requesting further clarification be provided within the standard, by referring to COBIT as the IT control framework. A description of the relationship of IT to all five COSO components follows.

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

- IT is often mistakenly regarded as a separate organization of the business and thus a separate control environment.
- IT is complex, not only with regard to its technical components but also in how those components integrate into the company'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.
- The ownership of IT controls may be unclear.

2. Risk Assessment
   It is likely that internal control risks could be more pervasive in the IT organization than in other areas of the company. Risk assessment may occur at the company level (for the overall organization) or at the activity level (for a specific process or business unit). At the company level, the following may be expected:
   - An IT strategy subcommittee of the company's overall Sarbanes-Oxley steering committee, with the following responsibilities:
     - 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., data integrity, security, confidentiality and availability

   At the activity level, the following may be expected:
   - 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

3. Control Activities
   Control activities primarily address the activity level. Without reliable information systems and effective IT control activities, public companies would not be able to generate accurate financial reports. As general and application controls increasingly replace manual controls, IT general and application controls are becoming more important.

4. 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. Supporting the other four components of the COSO framework, are 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. The IT organization processes most financial reporting information. However, its scope is usually much broader. For example, the

IT department may also assist in implementing mechanisms to identify and communicate significant information or events, such as regulatory reporting or accounting disclosures.

5. Monitoring
   Monitoring, which covers the oversight of internal control by management through continuous and point-in-time assessment processes, is becoming increasingly important to IT management. There are two types of monitoring activities: continuous monitoring and separate evaluations. IT performance and effectiveness are increasingly monitored using performance measures that indicate if an underlying control is operating effectively. Consider the following examples:
   - Defect identification and management—Establishing metrics and analyzing the trends of actual results against metrics can provide a basis for understanding the underlying reasons for processing failures. Correcting these causes can improve system accuracy, completeness of processing and system availability.
   - Security monitoring—Building an effective IT security infrastructure reduces the risk of unauthorized access. Improving security can reduce the risk of processing unauthorized transactions and generating inaccurate reports, and can ensure a reduction of the availability of key systems if applications and IT infrastructure components have been compromised.

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

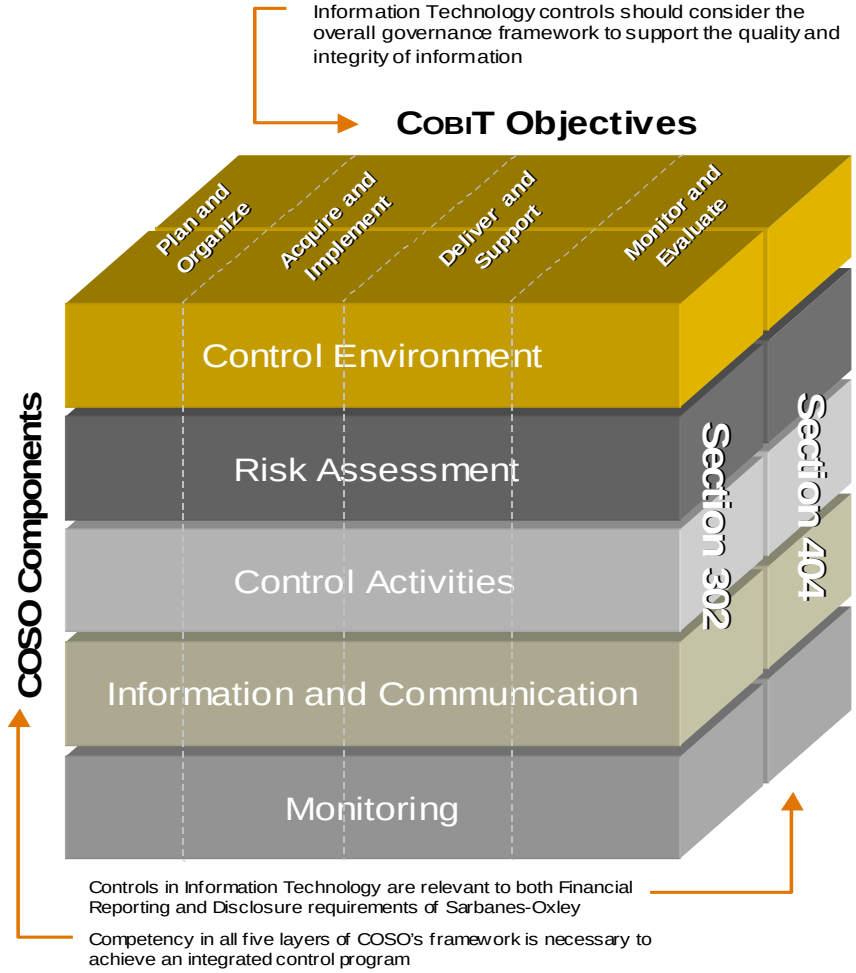
   At the activity level, the following may be expected:
   - Defect identification and management
   - Local monitoring of computer operations or security
   - Supervision of local IT personnel

IT Control Framework

We believe that, where IT is significant to the financial reporting of business enterprises, these enterprises need to use an IT control framework to supplement the overall COSO framework, as illustrated in the attached publication *IT Control Objectives for Sarbanes-Oxley*.

COBIT, originally introduced in 1996, is an open, *de facto* IT governance and control framework, now in its third edition. The framework, which is entirely compliant with COSO, is referred to and used globally by assurance and control professionals, and by business process owners and IT management. Again, we applaud the PCAOB for taking on the issues, especially as they apply to IT controls.

We would like to recommend that the Board adopt COBIT as the IT control framework. While the importance of IT control is embedded in the COSO internal control framework, IT management requires more examples to help document and evaluate controls. COBIT is an IT governance model, which provides both company-level and activity-level objectives and associated controls. Using the COBIT framework, a company can design a system of IT controls to comply with S404 of the Sarbanes-Oxley Act. The following depicts the COSO–COBIT relationship within the requirements of Sarbanes-Oxley.



Reliance on IT Internal Audit

While we agree that a public accounting firm should independently review IT controls within the IT control environment, we do have reservations about the inference that the public accountant cannot use the results of testing performed by management and others within other COSO components. IT audit professionals normally perform this testing. Many of those hold the Certified Information Systems Auditor (CISA) certification, offered by ISACA since 1978 and earned by more than 30,000 professionals worldwide. We suggest that the public accounting firm could determine the adequacy and appropriateness of such testing, based on the competence of the internal auditor and the auditor's positioning and independence, with additional testing being performed as necessary in the circumstances. If reliance cannot be placed on IT general controls testing then no credit can be given to the work that internal audit professionals are carrying out every day. We recommend that the Board consider revising this rule to provide further

clarification on the reliance public accounting firms can place on the work of IT internal auditors.

Audit Committee Effectiveness

Reference paragraph 56:
"Evaluating the Effectiveness of the Audit Committee's Oversight of the Company's External Financial Reporting and Internal Control Over Financial Reporting"

The company's audit committee plays an important role within the control environment, including the monitoring components of internal control over financial reporting. Within the control environment, the existence of an effective audit committee is essential to setting a positive tone at the top. Within the monitoring component, an effective audit committee is crucial to challenging the company's activities in the financial arena.

However we do have the following comments:

- We suggest that the main issue is the effectiveness of the audit committee in overseeing corporate governance over financial reporting, which includes governance over the IT function. Additional emphasis on the spirit of the controls over IT governance should be considered.
- IT governance is such an integral part of corporate governance, including internal control, which we believe boards and the audit committee need to extend governance to IT. Doing so will in turn provide the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the enterprises strategies and objectives. The current environment, which encompasses the new standard and other issues the PCAOB is addressing, calls for increasing emphasis on a broader corporate governance role for audit committees. The audit committee must deal effectively with IT governance and its implications if it is to deal effectively with processes to monitor risk and ensure that the system of internal control is effective in reducing those risks to an acceptable level.
- The ITGI was created for such reasons, and has been focusing on creating and delivering seminal research to assist in the provision of solutions to deal with these issues. We feel that the ITGI can provide some value going forward to the PCAOB, especially as it deals with the overarching issues of governance and IT. Much of the research and thought-provoking work the ITGI has created is closely linked back to COBIT—the framework for IT governance and control.

Again, we appreciate the opportunity to comment on the proposed standard. Thank you for considering our views. We would be happy to discuss them with you in further detail.

Respectfully submitted,

Marios Damianides, CISA, CISM, CA, CPA
2003-2004 International President
ISACA (info@isaca.org) ITGI (info@itgi.org)

Enc. *IT Control Objectives for Sarbanes Oxley*

GOVERNANCE INSTITUTE®

IT CONTROL OBJECTIVES FOR SARBANES-OXLEY

THE IMPORTANCE OF IT IN THE DESIGN, IMPLEMENTATION AND SUSTAINABILITY OF INTERNAL CONTROL OVER DISCLOSURE AND FINANCIAL REPORTING

DISCUSSION DOCUMENT

IT Governance Institute®

The IT Governance Institute (ITGI) strives to assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals. Its goals are to raise awareness and understanding among and provide guidance and tools to boards of directors, executive management and chief information officers (CIOs) such that they are able to ensure within their enterprises that IT meets and exceeds expectations, and its risks are mitigated.

Information Systems Audit and Control Association®

The Information Systems Audit and Control Association (ISACA®) is an international professional, technical and educational organization dedicated to being a recognized global leader in IT governance, control and assurance. With members in more than 100 countries, ISACA is uniquely positioned to fulfill the role of a central, harmonizing source of IT control practice standards the world over. Its strategic alliances with other organizations in the financial, accounting, auditing and IT professions ensure an unparalleled level of integration and commitment by business process owners.

Disclaimer

The IT Governance Institute, Information Systems Audit and Control Association and the authors of *IT Control Objectives for Sarbanes-Oxley* have designed this publication primarily as an educational resource for control professionals. The IT Governance Institute, Information Systems Audit and Control Association, authors and expert reviewers ("the Development Team") make no claim that use of this product will assure a successful outcome. This publication should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the controls professional should apply his/her own professional 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 Securities and Exchange Commission (SEC) or the Public Company Accounting Oversight Board (PCAOB). Accordingly, the Development Team makes no representation or warranties and provides no assurances that an organization's disclosure controls and procedures and the internal controls and procedures for financial reporting are compliant with the certification requirement and internal control reporting requirement of Sarbanes-Oxley, nor that an organization's plans are sufficient to address and correct any shortcomings that would prohibit the organization from making the required certification or reporting under Sarbanes-Oxley. Additional considerations are provided in the Preface of this publication.

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.

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@isaca.org*
Web site: *www.itgi.org* and *www.isaca.org*
ISBN: 1-893209-67-9
Printed in the United States of America

Acknowledgements

The IT Governance Institute wishes to recognize:

The authors, for their thought leadership
Christopher Fox, CA, PricewaterhouseCoopers LLP, USA
Paul A. Zonneveld, CISA, CISSP, CA, Deloitte & Touche LLP, Canada

The expert reviewers, whose comments helped shape the final document
Neil Anderson, CISA, CA, MBA, Electrolux AB, USA
Sean Ballington, CISA, CA, PricewaterhouseCoopers LLP, USA
Don Caniglia, CISA, Crowe Chizek LLP, USA
Sally Chan, CMA, PAdm, ACIS, RBC Financial Group, Canada
Tom Church, Deloitte & Touche LLP, USA
Pamela A. Fredericks, CISM, CISSP, Forsythe Solutions, USA
John Gimpert, CPA, Deloitte & Touche LLP, USA
Gary Hardy, CISA, IT Winners Ltd., UK
Edward L. Hill, Protiviti Inc, USA
Audrey Katcher, CISA, CPA, PricewaterhouseCoopers LLP, USA
Pierre Lapointe, CA, Deloitte & Touche LLP, Canada
Jennifer Laudermilch, CISA, CPA, PricewaterhouseCoopers LLP, USA
Elsa Lee, CISA, MA, CSQA, Crowe Chizek LLP, USA
William Levant, Deloitte & Touche LLP, USA
William Malik, CISA, Waveset Technologies, USA
Tiffany McCann, Financial Executives Institute-Research Foundation (FERF), USA
Todd McGowan, CISA, CPA, Deloitte & Touche LLP, USA
Therese E. Michael, PricewaterhouseCoopers LLP, USA
Robert G. Parker, CISA, FCA, CMC, Deloitte & Touche LLP, Canada
Hugh Parkes, CISA, FCA, The Q Alliance, Australia
Al Passori, META Group Inc., USA
Brian Reinke, FCA, Deloitte & Touche LLP, Canada
Robert S. Roussey, CPA, Leventhal School of Accounting, University of Southern California, USA
Michael Schirmbrand, Ph.D., CISA, CISM, CPA, KPMG LLP, Austria
Lily M. Shue, CISA, CCP, CITC, LMS Associates, USA
Hayward Walls, EnCana Corporation, Canada
Graham D. Ward, CISA, CA, ABCP, PricewaterhouseCoopers LLP, USA

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

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

Table of Contents

Preface

Despite all the publicity surrounding the Sarbanes-Oxley Act of 2002, relatively little attention has focused specifically on the role of information technology (IT) in the financial reporting process. This is unfortunate, given that the accuracy and timeliness of financial reporting is, at most companies, heavily dependent on a well-controlled IT environment.

IT organizations need to become involved in Sarbanes-Oxley attestation activities quickly. While the US Securities and Exchange Commission (SEC) has extended the dates for compliance with Section 404 of the Act, this move was only an acknowledgement that the original time frame was unrealistic and more time was needed for companies to comply. It was not an invitation to delay readiness and implementation work.

Accordingly, there is an urgent need for guidance material that specifically addresses the information technology control environment. This document is intended to help meet that need.

The Sarbanes-Oxley Act provides the foundation for new corporate governance rules, regulations and standards issued by the SEC. On 7 October 2003, the Public Company Accounting Oversight Board (PCAOB) issued both a briefing paper and a proposed auditing standard, release no. 2003-17—"An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements." While this guidance has provided further clarification on the nature and extent of the work required to provide an audit opinion, there are significant rules and standards that have yet to be issued. Among others, these might include detailed guidance on documentation requirements and further clarification on the requirements for real-time disclosure. The issuance of rules, standards and guidelines will be an ongoing process that will continually adapt to the results of regulatory examinations and the changing business and accounting environments. It is likely that there will never be a time when the rules for Sarbanes-Oxley will be "black and white"; many areas will still require professional judgment and interpretation. The development of industry standards and practices and the public debate over what could be considered to be good practice should facilitate this process.

Unlike previous event-driven control activities (e.g., Y2K), Sarbanes-Oxley activity will continue as a routine part of doing business. This document focuses on the aspects of Sarbanes-Oxley that will have the greatest impact on an organization in the short to medium term, that is, compliance with Section 302 and 404 of the act. The document deliberately does not focus on operational and efficiency issues, as the first priority should be demonstrating that strong IT controls over financial reporting are in place. However, it is inevitable (and desirable) that operational and efficiency issues will be addressed over time and built into the structures and processes that are developed. Once the ongoing cost of Sarbanes-Oxley compliance is assessed, there will be pressure to replace existing manual controls and processes with automated processes. In addition, there are other aspects of Sarbanes-Oxley that may have considerable impact on IT, e.g., the potential impact of real-time disclosure.

Readers may find the material in the appendix—IT Control Objectives for Sarbanes-Oxley—particularly useful. *COSO—Internal Control—Integrated Framework* was used as the overall framework upon which the supplementary IT guidance was based. *Control Objectives for Information and related Technology* (COBIT®), established by the IT Governance Institute, was used as the initial IT controls baseline to develop a control objective template. While COBIT addresses control objectives that relate to operational and compliance issues, only those related to financial reporting have been used to develop this document.

COBIT is a very rich and robust framework, comprising four domains, 34 IT processes and 318 detailed control objectives. It is a comprehensive approach for managing risk and control of information technology. As such, the control objectives and considerations set forth in this document may exceed, or be deficient in, what is necessary for organizations seeking to comply with the requirements of Sarbanes-Oxley. The suggested internal control framework (COSO) to be used for compliance with Sarbanes-Oxley, as supported by the Securities and Exchange Commission (SEC), addresses the topic of IT general controls, but does not dictate requirements for such control objectives and related control activities. Similarly, the audit standards issued by the PCAOB on 7 October 2003 highlight the importance of IT general controls, but do not specify which in particular must be included. Such decisions remain the responsibility of an organization's management and independent auditors for their respective purposes. Accordingly, companies should assess the nature and extent of information technology controls necessary to support their internal control program on a case-by-case basis. Additional considerations are provided in the disclaimer section of this publication.

In developing this publication, the approach that was taken started with reviewing the detailed COBIT control objectives, reconciling the objectives to COSO, determining if the objectives related to financial reporting objectives, extracting the IT general control objectives and rewriting objectives, as appropriate, so that they focus on financial reporting objectives—the requirement of Sarbanes-Oxley. The resulting general control objectives framework has four domains, 27 IT processes and 136 detailed control objectives.

However, a "one size fits all" approach is not the way to proceed. Each organization may want to tailor the control objective template to fit its specific circumstances, e.g., if systems development is considered to be of low risk, an organization may choose to amend or delete some of the suggested detailed control objectives. It is further suggested that each organization consult with its external auditors to ensure that all attestation-critical control objectives are addressed. An organization may then choose to incorporate additional aspects of COBIT.

Your comments on this document are welcome. Please submit your suggestions no later than 26 November 2003 to *research@isaca.org*, referencing this document by name: IT Control Objectives for Sarbanes-Oxley. After that date, the ITGI will review all comments received, finalize and reissue the document.

This page intentionally left blank.

A Focus on Internal Control

Recent events have ushered in a new era in the history of business, characterized by a firm resolve to increase corporate responsibility. The Sarbanes-Oxley Act of 2002 was created to restore investor confidence in US public markets, which were devastated by business scandals and lapses in corporate governance. Although it has literally rewritten the rules for accountability, disclosure and reporting, the Act's myriad pages of legalese support a simple premise: good corporate governance and ethical business practices are no longer optional niceties—they are the law.

With the future of the capital markets—a pillar of the economy—at stake, the need to link sound corporate governance with effective internal control has never been greater. Forward-thinking companies and executives will seize the opportunity. Those who fail to act may pay a heavy price.

Sarbanes-Oxley—Enhancing Corporate Accountability

Some observers have described Sarbanes-Oxley as the most significant piece of business legislation in the last half-century. Sarbanes-Oxley fundamentally changes the business and regulatory environment, and public companies cannot afford to underestimate the task ahead. The clock is ticking on compliance, and any delays in dealing with the issue may have serious consequences. Immediate and decisive action is required.

Sarbanes-Oxley aims to enhance corporate governance through measures that will strengthen internal checks and balances and, ultimately, strengthen corporate accountability. However, it is important to emphasize that Section 404 does not merely require companies to establish and maintain an adequate internal control structure, but also to assess its effectiveness on an annual basis. This distinction is significant.

For those organizations that have begun the compliance process, it has quickly become apparent that information technology plays a vital role in internal control—supporting the systems, data and infrastructure components that are critical to the financial reporting process. On 7 October 2003, the PCAOB issued a proposed auditing standard that discusses the importance of information technology in the context of internal control. In particular it states:

> *70. The nature and characteristics of a company's use of information technology in its information system affect the company's internal control over financial reporting.*

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

Accordingly, the goal of this publication is to offer guidance to those responsible for corporate IT systems on the following:
A. Assessing the current state of their IT control environment
B. Designing control improvements necessary to meet the directives of Sarbanes-Oxley Section 404
C. Closing the gap between A and B

Specific Requirements of Sarbanes-Oxley

Much of the discussion surrounding Sarbanes-Oxley has focused on Sections 302 and 404. A brief primer can be found in **figure 1**.

Figure 1—Sarbanes-Oxley Requirements Primer

	302	404
Who	Corporate management, executives and financial officer	Corporate management, executives and financial officer
What	1. Evaluate effectiveness of disclosure controls (with focus on changes since the most recent evaluation)* 2. Evaluate changes in internal control over financial reporting 3. Disclose all known control deficiencies and weaknesses 4. Disclose acts of fraud	1. Evaluate design and operating effectiveness of internal controls over financial reporting 2. Disclose all known controls, significant deficiencies and material weaknesses 3. Disclose acts of fraud
When	Already in effect as of July 2002	Year-ends beginning on or after June 2004**
How often	Quarterly assessment by management	Annual assessment by management and independent auditors

*Annual for foreign private issuers

**Nonaccelerated filers (<US $75M) can defer to 2005

Section 302

Under Section 302, the company's principal executive officer and financial officer must personally certify—quarterly and annually—that they:

- Are responsible for disclosure controls and procedures
- Have designed (or supervised the design of) disclosure controls to ensure that material information is made known to them
- Have evaluated the effectiveness of disclosure controls and procedures and material changes in internal control over financial reporting
- Have presented their conclusions regarding the effectiveness of disclosure controls
- Have disclosed to their audit committee and the independent auditors any significant control deficiencies, material weaknesses and acts of fraud that involve management or other employees who have a significant role in the company's internal control
- Have indicated in the filing any significant changes to disclosure controls
- Have disclosed in their quarterly reports any change that has (or is likely to) materially affect internal control over financial reporting

Auditor Evaluation Responsibilities

The draft audit standard issued by the PCAOB on 7 October 2003 discusses the external auditors responsibilities in regards to Section 302 in paragraphs 185 through 189. In particular it states:

185. 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.*

Disclosure Controls and Procedures

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

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; and

(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."

186. 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, and*
- *Determine, through a combination of observation and inquiry, whether significant changes in internal control over financial reporting may introduce significant deficiencies or material weaknesses in the design of internal control over financial reporting.*

Section 404

The directives of Sarbanes-Oxley Section 404 require that management provide an annual report on its assessment of internal control over financial reporting in the annual filing. This assessment must contain the following elements:

- A statement that company management is responsible for establishing and maintaining adequate internal control over financial reporting
- A statement identifying the internal control framework (such as COSO) used by management to evaluate the effectiveness of the company's internal control over financial reporting
- An assessment of the design and effectiveness of the company's internal control over financial reporting
- Disclosure of any material weaknesses in the company's system of internal control over financial reporting
- The company's independent auditor's attestation report on management's assessment of internal control over financial reporting

Auditor Attestation

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

Under the Sarbanes-Oxley Act, standards for the auditor's attestation are now the responsibility of the PCAOB. While the 404 attestation is "as of" a specific date the draft PCAOB standard issued on 7 October 2003 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:

95. 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.

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

Management should meet with their external auditors to determine the period of time a control is required to be operating before the attestation date.

Audit Committee

The draft audit standard of 7 October 2003 specifically addresses the external auditor's evaluation of the audit committee in paragraphs 56 through 59. In particular it states:

56. Evaluating the Effectiveness of the Audit Committee's Oversight of the Company's External Financial Reporting and Internal Control Over Financial Reporting. The company's audit committee plays an important role within the control environment and monitoring components of internal control over financial reporting. Within the control environment, the existence of an effective audit committee is essential to setting a positive tone at the top. Within the monitoring component, an effective audit committee is crucial to challenging the company's activities in the financial arena.

As a result, it would be advisable if the audit committee is aware of any significant activities impacting the IT environment as it relates to financial reporting.

Fraud Considerations in an Audit of Internal Control Over Financial Reporting

In the introduction to PCAOB draft audit standard of 7 October 2003, the board makes specific reference to fraud considerations:

> *Strong internal controls provide better opportunities to detect and deter fraud. For example, many frauds resulting in financial statement restatement relied upon the ability of management to exploit weaknesses in internal control. To the extent that the internal control reporting required by Section 404 can help restore investor confidence by improving the effectiveness of internal controls (and reducing the incidence of fraud), the auditing standard on performing the audit of internal control over financial reporting should emphasize controls that prevent or detect errors as well as fraud. For this reason, the proposed standard specifically addresses and emphasizes the importance of controls over possible fraud and requires the auditor to test controls specifically intended to prevent or detect fraud that is reasonably likely to result in material misstatement of the financial statements.*

Paragraphs 24 through 26 of the draft audit standard of 7 October 2003 address fraud considerations. In particular paragraph 25 states:

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

The Foundation for Reliable Financial Reporting

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

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

To emphasize this point, the PCAOB draft audit standard of 7 October 2003 discusses the relationship of information technology and its importance in testing the design and operational effectiveness of internal control. In particular paragraph 41 states:

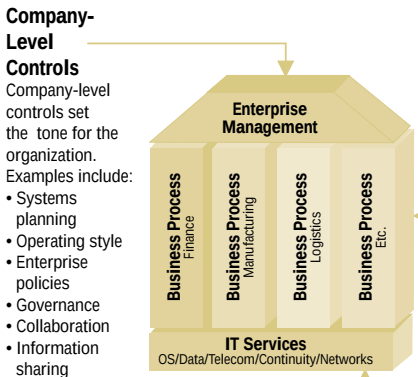
> *…controls should be tested, including controls over relevant assertions related to all significant accounts and disclosures in the financial statements. Generally, such controls include [among others]:*
> - *Controls, including information technology general controls, on which other controls are dependent.*

The draft audit standard continues in paragraph 67 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.*

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

Figure 2—Common Elements of Organizations



Enterprise Management	Business Process	Shared Services
Enterprise management is the manner in which strategy is established and incorporated into business activities. At the company 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 strategic business processes. Increasingly, business processes are being automated and integrated with complex and highly efficient IT systems.	Shared services are those that are required by more than one department or process and are often delivered as a common service. From an IT perspective, services such as security, telecommunications and storage are necessary services for any department or business unit, and are often managed by a central IT function.

Figure 2 demonstrates how IT controls are embedded within each element of business. For instance, consider the following areas where IT enables the controls sought for reliable financial reporting:

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

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

Information Technology Controls—A Unique Challenge

Sarbanes-Oxley makes corporate executives explicitly responsible for establishing, evaluating and monitoring the effectiveness of internal control over financial reporting. For most organizations, the role of information technology will be crucial to achieving this objective. Whether through a unified enterprise resource planning 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 will need representation from IT on their Sarbanes-Oxley teams to ensure that IT general controls and application controls exist and support the objectives of the compliance effort. Some of the key areas of responsibility for IT will include:

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

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

1. There is no need to reinvent the wheel; virtually all public companies have some semblance of IT control. While they may be informal and lacking sufficient documentation, IT controls generally exist in areas such as security and availability.
2. Many companies will be able to tailor existing IT control processes to comply with the provisions of Sarbanes-Oxley. Frequently, it is the consistency and quality of control documentation and evidential matter that is lacking, but the general process is often in place, only requiring some modification.

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

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

Turning Compliance into Competitive Advantage

There is no such thing as a risk-free environment, and compliance with Sarbanes-Oxley 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 Act will undoubtedly provide lasting benefits. In particular, IT organizations can seize this opportunity to turn compliance into competitive advantage.

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

- Enhance overall IT governance
- Enhance the understanding of IT among executives

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

International Considerations

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

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

Examples of international IT assessment considerations include:

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

Setting the Ground Rules

Until recently, assertions on control by an organization were mostly voluntary and based on a wide variety of internal control frameworks. To improve consistency and quality, the SEC has mandated the use of a recognized internal control framework that is established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment. In its final rules, specific reference is made to the recommendations of the Committee of Sponsoring Organizations of the Treadway Commission, otherwise known as COSO.[1]

COSO Defined

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

The sections that follow provide further insight into COSO as well as its implications for IT.

Adopting a Control Framework

For years, IT has played an important role in the operation of strategic and managerial information systems. Today, these systems are inseparable from an organization's ability to meet the demands of customers, suppliers and other important stakeholders. With widespread reliance on IT for financial and operational management systems, controls have long been recognized as necessary, particularly for significant information systems.

In the draft audit standard of 7 October 2003, the PCAOB states:

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

It will be important to demonstrate how IT controls support the COSO integrated framework. An organization should have IT control competency in all COSO components.

[1] *www.coso.org*

COSO identifies five essential components of effective internal control. The following is a description of each component and its relationship to IT. Detailed IT control objectives have been included at the end of this document to provide considerations for Sarbanes-Oxley compliance.

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

The control environment primarily addresses the company level.

However, IT frequently has characteristics that may require additional emphasis on business alignment, roles and responsibilities, policies and procedures, and technical competence. The following list describes some considerations related to the control environment and IT:
- IT is often mistakenly regarded as a separate organization of the business and thus a separate control environment.
- IT is complex, not only with regard to its technical components but also as to how those components integrate into the company'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.
- The ownership of IT controls may be unclear.

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

At the company level, the following may be expected:
- An IT planning subcommittee of the company's overall Sarbanes-Oxley steering committee. Its responsibilities may include 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., data security, availability and performance analysis

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

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

Control activities primarily address the activity level.

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

General controls, which are designed to ensure that the financial information generated from a company's application systems can be relied upon, include the following types:
- Data center operation controls—Controls such as job setup and scheduling, operator actions, backup and recovery procedures, and contingency or disaster recovery planning
- System software controls—Controls over the effective acquisition, implementation and maintenance of system software, database management, telecommunications software, security software and utilities
- Access security controls—Controls that prevent inappropriate and unauthorized use of the system
- Application system development and maintenance controls—Controls over the development methodology, which include system design and implementation, outlining specific phases, documentation requirements, approvals, and checkpoints to control the development or maintenance of the project

The draft audit standard of 7 October 2003 from the PCAOB specifically precludes the external auditor from using the results of certain information technology general controls testing performed by management and others as well as any work related to companywide antifraud programs. The previously mentioned controls are those on which the operating effectiveness of other controls depend.

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

- Balancing control activities—These controls 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—Calculations to validate data. A company's part numbers contain a check digit to detect and correct inaccurate ordering from its suppliers. Universal product codes include a check digit to verify the product and the vendor.
- Predefined data listings—Provide the user with predefined lists of acceptable data. For example, a company's intranet site might include drop-down lists of products available for purchase.
- Data reasonableness tests—Compare data captured to a present or learned pattern of reasonableness. For example, an order to a supplier by a home renovation retail store for an unusually large number of board feet of lumber may trigger a review.
- Logic tests—Include the use of range limits or value/alphanumeric tests. For example, credit card numbers have a predefined format.

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

4. 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 represents an ever-increasing challenge to the IT department. The determination of which information is required to achieve control objectives, and the communication of this information in a form and time frame that allows people to carry out their duties, supports the other four components of the COSO framework.

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

COSO also notes that the quality of information includes ascertaining whether the information is:
- Appropriate—Is it the right information?
- Timely—Is it available when required and reported in the right period of time?
- Current—Is it the latest available?
- Accurate—Are the data correct?
- Accessible—Can authorized individuals gain access to it as necessary?

At the company level, the following may be expected:
- Development and communication of corporate policies
- Development and communication of reporting requirements, including deadlines, reconciliations, and the format and content of monthly, quarterly and annual management reports
- Consolidation and communication of financial information

At the activity level, the following may be expected:
- Development and communication of standards to achieve corporate policy objectives
- Identification and timely communication of information to assist in achieving business objectives
- Identification and timely reporting of security violations

5. Monitoring

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

IT performance and effectiveness are increasingly monitored using performance measures that indicate if an underlying control is operating effectively. Consider the following examples:
- Defect identification and management—Establishing metrics and analyzing the trends of actual results against metrics can provide a basis for understanding the underlying reasons for processing failures. Correcting these causes can improve system accuracy, completeness of processing and system availability.
- Security monitoring—Building an effective IT security infrastructure reduces the risk of unauthorized access. Improving security can reduce the risk of processing unauthorized transactions and generating inaccurate reports, and can ensure a reduction of the availability of key systems if applications and IT infrastructure components have been compromised.

An IT organization also has many different types of separate evaluations, including:
- Internal audits
- External audits

- Regulatory examinations
- Attack and penetration studies
- Independent performance and capacity analyses
- IT effectiveness reviews
- Control self-assessments
- Independent security reviews
- Project implementation reviews

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

At the activity level, the following may be expected:
- Defect identification and management
- Local monitoring of computer operations or security
- Supervision of local IT personnel

Assessing the Readiness of IT

Sarbanes-Oxley now requires *all* qualifying SEC-registered organizations to document, evaluate, monitor and report on internal control over financial reporting and disclosure controls and procedures, which include IT controls. The first step in this process will be to assess the overall strength of IT control in the organization by considering the questions illustrated in **figure 3**.

Figure 3—Sarbanes-Oxley IT Diagnostic Questions

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

The responses to these questions will help determine (1) if the IT department is integrated with the overall Sarbanes-Oxley Section 404 implementation plan, (2) if the IT department has documented and evaluated IT controls and (3) if executive management, including the CIO, appreciates the impact that the IT department has on Sarbanes-Oxley Section 404 compliance.

Establishing IT Control Guidelines for Sarbanes-Oxley

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

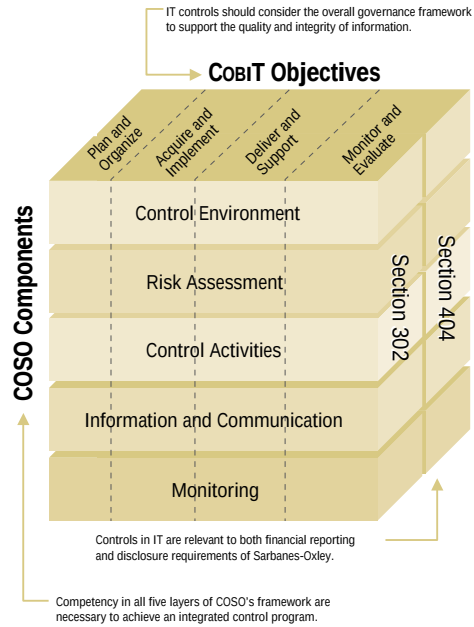
Several IT internal control frameworks exist. However, the IT control objectives known as COBIT are considered particularly useful, and are an open framework, which aligns with the spirit of the Sarbanes-Oxley requirement that any framework used be open and generally acceptable. COBIT is an IT governance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

Before deciding to use COBIT as the basis for developing the IT control objectives considered in this research, consideration was also given to other IT control guidelines—including ISO17799, the Information Technology Infrastructure Library (ITIL) and the Common Criteria—to ensure that important general and application controls necessary to satisfy Sarbanes-Oxley were addressed.

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

While COSO identifies five components of internal control (as illustrated in **figure 4**) that need to be in place and integrated to achieve financial reporting and disclosure objectives, COBIT provides similar 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/Organize through Monitor/Evaluate—applying to each individually and in aggregate.

Figure 4—Internal Control Components



Closing the Gap

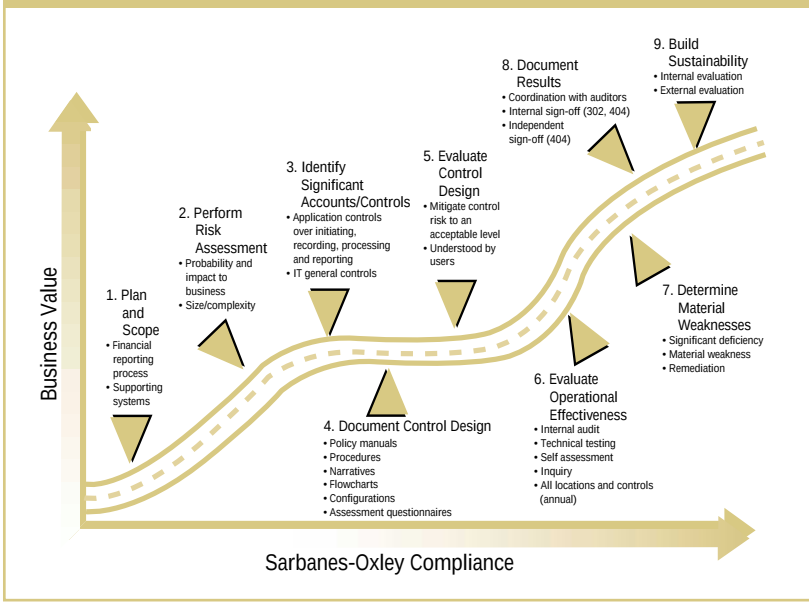
The following section provides a compliance road map that is tailored to the specific objectives and responsibilities of IT departments.

Road Map for Compliance

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

The compliance road map, illustrated in **figure 5**, provides direction for IT professionals on meeting the challenges of Sarbanes-Oxley.

Figure 5—Compliance Road Map



1. Plan and Scope

Scoping the project is, without question, one of the most important activities in the entire program. While it is true that general controls cut across geographies and business processes, not all IT processes are relevant.

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

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

As defined in paragraph 43 of the draft audit standard of 7 October 2003 from the PCAOB, processes and controls to be included in the scope of the program generally include:

- *Controls over initiating, recording, processing, and reporting significant accounts and disclosures and related assertions embodied in the financial statements.*
- *Controls over the selection and application of accounting policies that are in conformity with generally accepted accounting principles.*
- *Antifraud programs and controls.*
- *Controls, including information technology general controls, on which other controls are dependent.*
- *Controls over significant nonroutine and nonsystematic transactions, such as accounts involving judgments and estimates.*
- *Controls over the period-end financial reporting process, including controls over procedures used to enter transaction totals into the general ledger; to initiate, record, and process journal entries in the general ledger; and to record recurring and nonrecurring adjustments to the financial statements (e.g., consolidating adjustments, report combinations, and reclassifications).*

2. Perform Risk Assessment

Risk assessment enables organizations to understand how events can inhibit the achievement of business objectives. Risk assessment requires two perspectives: likelihood and impact. Likelihood reflects the potential for events to occur, while impact reflects the effect of such events.

In the context of the IT compliance program, a risk assessment must be performed for systems supporting the financial reporting process. Examples of risks that could undermine financial reporting include failures of:

- The quality and integrity of information managed by IT systems
- Access controls over IT systems and related applications
- Authorizations designed and automated into application systems
- The availability and timeliness of information
- The confidentiality of information disclosure
- Recoverability controls designed to support continued reporting

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

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

When determining which locations or business units to include in the scope of the Sarbanes-Oxley program, organizations should consider the following:

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

3. Identify Significant Accounts/Controls

COSO identifies two broad groupings of information system control activities:

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

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

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

The appendix of IT Control Objectives for Sarbanes-Oxley, provides details on the specific control objectives that should be considered for both general and application controls. Since company-level controls are primarily related to the control environment and risk assessment components of COSO, and their existence sets the tone for the effectiveness of all other controls, assessing company-level controls is a key objective for this phase. It includes such elements as:

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

4. Document Control Design

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

While the PCAOB has not given detailed guidance on documentation requirements, it states in the draft standard that documentation should be sufficient for the external auditor to review the design and test the effectiveness of a control.

The draft standard addresses documentation in paragraphs 43 through 47. In addition to stating that documentation should include the five components of internal control over financial reporting, the draft standard states:

> *44. Documentation might take many forms of presentation and can include a variety of information, including policy manuals, process models, flowcharts, job descriptions, documents, and forms. No one form of documentation is required, and the extent of documentation will vary depending on the size, nature, and complexity of the company.*
>
> *45. Documentation of the design of controls over relevant assertions related to significant accounts and disclosures is evidence that controls related to management's assessment about the effectiveness of internal control over financial reporting, including changes to those controls, have been identified, are capable of being communicated to those responsible for their performance, and are capable of being monitored by the company. Such documentation also provides the foundation for appropriate communication concerning responsibilities for performing controls and for the company's evaluation of and monitoring of the effective operation of controls.*

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

Management should discuss the proposed extent and detail of their control documentation with their external auditors early in the process to reduce the risk that the external auditor will consider their control documentation deficient.

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

Equally important in this phase is the documentation that supports an organization's control program. Documentation should be prepared—both at the company level as well as the activity level—of the objectives that the controls are designed to achieve to support the organization's internal control over financial reporting and disclosure controls and procedures.

It is advisable that an organization document its approach to IT control, including the assignment of authority and responsibility for IT controls as well as their design and operation.

5. Evaluate Control Design

In this phase, an IT organization must step back and evaluate the ability of its control program to reduce IT risk to an acceptable level and to ensure it is understood by users. The PCAOB draft audit standard of 7 October 2003 discusses the factors that might contribute to controls not operating effectively. In particular paragraph 74 states:

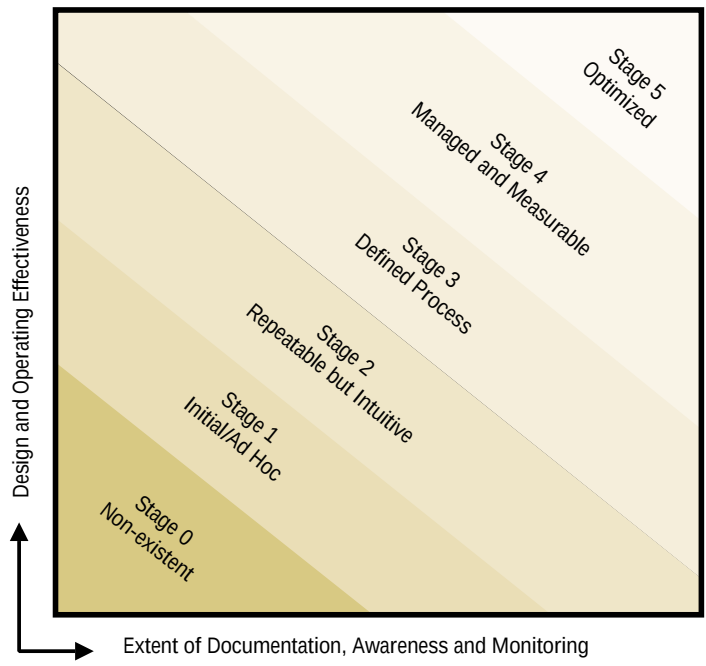
Factors that affect whether the control might not be operating effectively include the following:

- *The degree to which the control relies on the effectiveness of other controls (for example, the control environment or information technology general controls)*

To help in this process, consider the IT control design and effectiveness model in **figure 6**. 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 6 demonstrates the stages of control reliability that may exist within organizations. For the purposes of establishing internal control, some organizations may be willing to accept IT controls that fall somewhere short of stage 3. However, given the Act's requirements for independent attestation of controls by external audit, controls will more than likely require the attributes and characteristics of stage 3 or higher for key control activities.

Figure 6—Stages of Control Reliability



The table presented in **figure 7** provides insight into the various characteristics of each stage as well as the related implications. IT organizations must realize that there is little definition or guidance regarding the attributes or characteristics necessary to comply with the 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.

6. Evaluate Operational Effectiveness

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

Figure 7—Control Quality

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

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

The PCAOB draft audit standard of 7 October 2003 specifically addresses service auditor's reports in paragraphs B29 through B34. In particular:

> *There are a number of areas in which the auditor should not use the results of testing performed by management and others, including [among others]:*
>
> • *Controls that have a pervasive effect on the financial statements, such as certain information technology general controls on which the operating effectiveness of other controls depend.*

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.

Furthermore, the PCAOB draft audit standard of 7 October 2003 states:

> *B25. The use of a service organization does not reduce management's responsibility to maintain effective internal control over financial reporting. Rather, management should evaluate controls at the service organization, as well as related controls at the company, when making its assessment about internal control over financial reporting.*

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

Traditionally, audit opinions commonly known as SAS70 reports (Section 5900 in Canada) have been performed for service organizations. If these audit reports do not include tests of controls, results of the tests and the service auditor's opinion on operating effectiveness, they may not be deemed sufficient for purposes of Sarbanes-Oxley compliance. In such cases, organizations may wish to consult with their external auditors and understand the specific requirements.

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

In making the judgment as to which IT control deficiencies are significant, independent auditors will consider various factors such as the size of operations, complexity and diversity of activities, organizational structure, and the likelihood that the IT control deficiency could result in a misstatement of the organization's financial records.

To prepare, IT organizations should engage individuals with experience performing IT control audits to identify the weaknesses in IT internal control programs. Once a reliable control state has been reached, a sustainability model should be implemented to ensure its operating effectiveness over time.

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

9. Build Sustainability
The final phase ensures that internal controls are sustainable. At this point, IT management should be in a position to sign off on the IT internal control program effectiveness and the effectiveness may then be approved through an external evaluation. Control assessment and management competencies must 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.

What Is the Difference Between a Deficiency and a Weakness?

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

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

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

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

How Compliance Should Be Documented

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

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

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

- Company level
  - Statement of control and approach to confirming its existence and continued effectiveness over time
- 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
  - Description of the approach followed to confirm (test) the existence and operational effectiveness of the control activities
  - Conclusions reached about the effectiveness of controls, as a result of testing

Lessons Learned

Parallels can be drawn between the affect of the Sarbanes-Oxley Act of 2002 on public companies and the impact of the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) on the banking industry.

Both statutes introduced regulations to remedy perceived market failures, and each enacted significant new reporting requirements. There are several lessons public companies can learn from the FDICIA example:

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

Past events ushered in a new era in the history of business, characterized by a firm resolve to increase corporate responsibility. Sarbanes-Oxley was created to restore investor confidence in public markets, which have been devastated by business scandals and lapses in corporate governance. Although it has literally rewritten the rules for accountability, disclosure and reporting, good corporate governance and ethical business practices are no longer optional niceties—they are the law.

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

This page intentionally left blank.

Appendix—IT Control Objectives for Sarbanes-Oxley

Having set the stage for the importance of IT in preparing for Sarbanes-Oxley compliance, the specific control objectives that will form the basis of the IT control program must be addressed.

The table in **figure 8** illustrates the segments of CobiT and maps their relationship to the appropriate COSO component. In reviewing this material, readers may notice that not all CobiT control objectives are mapped to the COSO framework; for instance, "identify automated solutions." In such cases, the CobiT objective has not been mapped since it has more to do with operational efficiencies than financial reporting or disclosure controls. It is immediately evident that many CobiT segment elements have relationships with more than one COSO component. This is expected, given the nature of general IT controls, as they form the basis for achieving reliable information systems. This multirelationship attribute further demonstrates why IT controls are the basis for all others and are essential for a reliable internal control program.

CobiT is a very rich and robust framework, comprising four domains, 34 IT processes and 318 detailed control objectives. It is a comprehensive approach for managing risk and control of information technology. As such, the control objectives and considerations set forth in this document may exceed, or be deficient in, what is necessary for organizations seeking to comply with the requirements of Sarbanes-Oxley. The suggested internal control framework (COSO) to be used for compliance with Sarbanes-Oxley, as supported by the Securities and Exchange Commission (SEC), addresses the topic of IT general controls, but does not dictate requirements for such control objectives and related control activities. Similarly, the audit standards issued by the PCAOB on 7 October 2003 highlight the importance of IT general controls, but do not specify which in particular must be included. Such decisions remain the responsibility of an organization's management and independent auditors for their respective purposes. Accordingly, companies should assess the nature and extent of information technology controls necessary to support their internal control program on a case-by-case basis. Additional considerations are provided in the disclaimer section of this publication.

The reader may find the following materials particularly useful. Preparing this guide is not 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 of the suggested detailed control objectives. An organization may also consult with its external auditors to ensure that all attestation-critical control objectives are addressed.

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

Figure 8—COBIT Relationship to COSO

	COSO Component				
COBIT Control Objectives	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
Plan and Organize					
Define a strategic IT plan.		●		●	●
Define the information architecture.			●	●	
Determine technological direction.					
Define the IT organization and relationships.	●			●	
Manage the IT investment.					
Communicate management aims and direction.	●			●	●
Manage human resources.	●			●	
Ensure compliance with external requirements.			●	●	●
Assess risks.		●			
Manage projects.					
Manage quality.	●		●	●	●
Acquire and Implement					
Identify automated solutions.					
Acquire and maintain application software.			●		
Acquire and maintain technology infrastructure.			●		
Develop and maintain procedures.			●	●	
Install and accredit systems.			●		
Manage changes.			●		●
Deliver and Support					
Define and manage service levels.	●		●		●
Manage third-party services.	●	●	●		●
Manage performance and capacity.	●		●		
Ensure continuous service.	●		●		●
Ensure systems security.	●		●	●	●
Identify and allocate costs.					
Educate and train users.	●			●	
Assist and advise customers.					
Manage the configuration.	●		●	●	
Manage problems and incidents.			●	●	●
Manage data.			●	●	
Manage facilities.			●		
Manage operations.			●	●	
Monitor and Evaluate					
Monitor the processes.				●	●
Assess internal control adequacy.					●
Obtain independent assurance.	●				●
Provide for independent audit.					

The control objectives that follow are based on the guidance provided in COBIT. Those familiar with COBIT will recognize that the control objectives in this publication are not presented exactly as they are in COBIT. The end result is a series of IT controls, designed specifically for COSO and Sarbanes-Oxley.

As always, IT organizations should consider the nature and extent of their operations in determining which, if not all, of the control objectives need to be included in their internal control program.

1. General Controls—Plan and Organize

This domain addresses strategy and tactics, and focuses on identifying the way IT can best contribute to the achievement of the business objectives. Furthermore, the realization of the strategic vision needs to be planned, communicated and managed for different perspectives.

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

- Define a strategic plan.
- Define the information architecture.
- Define the IT organization and relationships.
- Communicate management aims and direction.
- Manage human resources.
- Ensure compliance with external requirements.
- Assess risks.
- Manage quality.

Each of these control processes is outlined in **figures 9** through **16**.

Figure 9—Define a Strategic IT Plan	
Control Objective	**COSO Component**
The strategic planning process is a fundamental control for IT because it provides the direction and mandate for helping the business achieve its objectives. The plan identifies what IT must do to support the business, the related risks that need to be considered by the business, the investments required to meet these objectives and sustain them over time, as well as senior management's support of the overall IT mandate. Activities performed in this area align with the risk assessment, information and communication, and monitoring components of COSO. Without appropriate IT planning, over time, the business will struggle to achieve its objectives and, the risk of noncompliance with financial reporting and disclosure requirements will increase.	
Management prepares strategic plans for IT that align business objectives with IT strategies. The planning approach includes mechanisms to solicit input from relevant internal and external stakeholders impacted by the IT strategic plans.	Risk assessment
Management obtains feedback from business process owners and users regarding the quality and usefulness of its IT plans for use in the ongoing risk assessment process.	Risk assessment
An IT planning or steering committee exists to oversee the IT function and its activities. Committee membership includes representatives from senior management, user management and the IT function.	Risk assessment
The IT organization ensures that IT plans are communicated to business process owners and other relevant parties across the organization.	Information and communication
IT management communicates its activities, challenges and risks on a regular basis with the CEO and CFO. This information is also shared with the board of directors.	Information and communication
The IT organization monitors its progress against the strategic plan and reacts accordingly to meet established objectives.	Monitoring

Figure 10—Define the Information Architecture	
Control Objective	**COSO Component**
Information should be identified, captured and communicated in a form and time frame that enables the business to carry out its responsibilities effectively and on a timely basis. As processing deadlines become tighter and availability requirements become more important, an organization will place increasing reliance on automated, rather than manual, systems and related controls. Accordingly, the increasing demands on systems require appropriate planning and design to support these business requirements. Activities performed in this area align with the control activities and information and communication components of COSO. If information architecture is not defined or consistently applied, there is increased risk that the information required to prepare financial statements will not be available in a timely manner.	
IT management has defined information capture, processing and reporting controls—including completeness, accuracy, validity and authorization—to support the quality and integrity of information used for financial and disclosure purposes.	Information and communication
IT management has defined information classification standards in accordance with corporate security and privacy policies.	Control activities
IT management has defined, implemented and maintained security levels for each of the data classifications. These security levels represent the appropriate (minimum) set of security and control measures for each of the classifications and are reevaluated periodically and modified accordingly.	Control activities

Figure 11—Define the IT Organization and Relationships	
Control Objective	**COSO Component**
The IT organization is responsible for managing all aspects of the system environment. Ensuring the employment of appropriate people with the necessary skills to meet the mandate of IT, and ultimately the business, is critical to its overall effectiveness. Furthermore, the definition of roles and responsibilities is necessary to establish accountability over systems and data. Activities in this area align to the control environment and information and communication components of COSO. Without appropriate skills and the definition of roles and responsibilities, there is increased risk that systems and data will not be reliable and will, thereby, compromise the business' ability to comply with legal and regulatory requirements.	
IT managers have adequate knowledge and experience to fulfill their responsibilities.	Control environment
Key systems and data have been inventoried and their owners identified.	Control environment
Roles and responsibilities of the IT organization are defined, documented and understood.	Control environment
IT personnel have sufficient authority to exercise the role and responsibility assigned to them.	Control environment
The IT organizational structure is sufficient to provide for necessary information flow to manage its activities.	Control environment
IT management has implemented a division of roles and responsibilities (segregation of duties) that reasonably prevents a single individual from subverting a critical process.	Control environment
IT management has ensured that personnel are performing only those duties stipulated in their respective jobs and position descriptions.	Control environment
IT staff evaluations are performed regularly (e.g., to ensure that the IT function has a sufficient number of competent IT staff necessary to achieve their objectives).	Control environment
Contracted staff and other contract personnel are subject to policies and procedures, created to control their activities by the IT function, to assure the protection of the organization's information assets.	Control environment
IT staff understand and accept their responsibility regarding internal control.	Control environment
IT strategies and ongoing operations are formally defined and communicated to senior management and the board of directors, e.g., through periodic meetings of an IT steering committee.	Information and communication
Significant IT events or failures, e.g., security breaches, major system failures or regulatory failures, are reported to senior management or the board.	Information and communication

Figure 12—Communicate Management Aims and Direction	
Control Objective	**COSO Component**
Establishing a reliable system requires participation from all members of the IT organization. To accomplish this, members of the IT organization should be informed and committed to the direction of IT and its ability to meet the objectives outlined in the strategic plan. Activities in this area align to the control environment and information and communications, and monitoring components of COSO. Without communicating its direction, IT organizations may be unable to obtain the commitment of their members and, ultimately, achieve their goals.	
IT management has formulated, developed and documented policies and procedures governing the IT organization's activities.	Control environment
IT management has communicated policies and procedures governing the IT organization's activities.	Information and communication
IT management periodically reviews its policies, procedures and standards to reflect changing business conditions.	Monitoring
IT management has processes in place to investigate compliance deviations and introduce remedial action.	Monitoring
IT management has a process in place to assess compliance with its policies, procedures and standards.	Monitoring

Figure 13—Manage Human Resources	
Control Objective	**COSO Component**
Education and training of IT staff address how an organization supports its people to perform their job responsibilities in a reliable and controlled manner. Actions performed in this area align with the control environment and information and communication components of COSO. The ability, or lack thereof, to cross-train, learn and continually enhance skill levels will directly impact the enterprise's ability to meet new challenges and demands of the business.	
Controls are in place to support appropriate and timely responses to job changes and job terminations so that internal controls and security are not impaired by such occurrences.	Control environment
The IT organization subscribes to a philosophy of continuous learning, providing necessary training and skill development to its members.	Information and communication
The IT organization adopts and promotes the entity's culture of integrity management, including ethics, business practices and human resource evaluations, to ensure compliance.	Control environment

Figure 14—Ensure Compliance with External Requirements	
Control Objective	**COSO Component**
The organization should establish and maintain procedures to ensure compliance with Sarbanes-Oxley, the SEC and other external regulatory requirements. The compliance function should identify and communicate requirements that could potentially impact the IT organization. The IT organization should establish a framework of control to ensure that external requirements are understood and managed. If external requirements that could impact financial reporting are not addressed, then this could jeopardize accurate reporting of financial results. Activities in this area are aligned with the control activities, information and communication, and monitoring components of COSO.	
The organization monitors changes in external requirements for legal, regulatory or other external requirements related to IT practices and controls.	Monitoring
Control activities are in place and followed to ensure compliance with external requirements, such as regulatory and legal rules.	Control activities
Internal events are considered in a timely manner to support continuous compliance with legal and regulatory requirements.	Information and communication

Figure 15—Assess Risks	
Control Objective	**COSO Component**
Risk assessment is defined as "the identification and analysis of relevant risks to achievement of the objectives." Risk assessment is usually pervasive in the IT organization. Activities in this area align with the risk assessment component of COSO. Without adequate risk assessments, there is an increased risk that an appropriate framework of internal controls will not be implemented. An inadequate framework of internal control would jeopardize the Section 302 and 404 management assertions.	
The IT organization has an entity- and activity-level risk assessment framework, which is used periodically to assess information risk to achieving business objectives.	Risk assessment
Management's risk assessment framework focuses on the examination of the essential elements of risk and the cause/effect relationship among them, including risks related to achieving business objectives, regulatory compliance, legal compliance, technology reliability, information integrity and human resources.	Risk assessment
A risk assessment framework exists and considers the probability and likelihood of threats.	Risk assessment
The IT organization's risk assessment framework measures 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.	Risk assessment
The IT organization's risk assessment framework is designed to support cost-effective controls to mitigate exposure to risks on a continuing basis, including risk avoidance, mitigation or acceptance.	Risk assessment
A comprehensive security assessment is performed for critical systems and locations based on their relative priority and importance to the organization.	Risk assessment

Figure 15—Assess Risks *(cont.)*	
Control Objective	**COSO Component**
Where risks are considered acceptable, there are formal documentation and acceptance of residual risk with related offsets, including adequate insurance coverage, contractually negotiated liabilities and self-insurance.	Risk assessment
The IT organization is committed to active and continuous risk assessment processes as an important tool in providing information on the design and implementation of internal controls, in the definition of the IT strategic plan, and in the monitoring and evaluation mechanisms.	Risk assessment

Figure 16—Manage Quality	
Control Objective	**COSO Component**
Quality programs address both general and project-specific quality assurance activities and should prescribe the type(s) of quality assurance activities (such as reviews, audits, inspections, etc.) to be performed to achieve the objectives of the general quality plan. Activities in this area align with all components of the COSO framework. Without quality assurance, the organization may not be able to rely on its systems of control, and thereby, management's 302 and 404 assertions may be jeopardized.	
Documentation is created and maintained for all significant IT processes and activities.	Control environment
A plan exists to maintain the overall quality assurance of IT activities based on the organizational and IT plans.	Control environment
Documentation standards are in place, have been communicated to all IT staff and are supported with training.	Control environment
A quality plan exists for significant IT functions (e.g., system development and deployment) and provides a consistent approach to address both general and project-specific quality assurance activities.	Control environment
The quality plan prescribes the type(s) of quality assurance activities (such as reviews, audits, inspections, etc.) to be performed to achieve the objectives of the quality plan.	Control environment
The quality assurance process includes a review of the adherence to IT policies, procedures and standards.	Control environment
Data integrity ownership and responsibilities have been communicated to the appropriate data owners and they have accepted these responsibilities.	Information and communication

2. General Controls—Acquire and Implement

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

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

- Acquire and maintain application software.
- Acquire and maintain technology infrastructure.
- Develop and maintain procedures.
- Install and accredit systems.
- Manage changes.

Each of these control processes is outlined in **figures 17** through **21**.

Figure 17—Acquire and Maintain Application Software

Control Objective	COSO Component
Acquiring and maintaining application software include the design, acquisition/building and deployment of systems that support the achievement of business objectives. Actions performed in this area align with the control activities component of COSO. This is also where controls are designed and implemented to support the initiating, recording, processing and reporting of 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. Activities in this area align with the control activities component of COSO.	
The organization has a system development life cycle methodology that considers security, availability and processing integrity requirements of the organization.	Control activities
The system development life cycle methodology ensures that information systems are designed to include application controls that support complete, accurate, authorized and valid transaction processing.	Control activities
The organization has an acquisition and planning process that aligns with its overall strategic direction.	Control activities
The organization acquires software in accordance with its acquisition and planning process.	Control activities
Procedures exist to ensure that system software is installed and maintained in accordance with the organization's requirements.	Control activities
Procedures exist to ensure that system software changes are controlled in line with the organization's change management procedures.	Control activities

Figure 18—Acquire and Maintain Technology Infrastructure	
Control Objective	**COSO Component**
Acquiring and maintaining technology infrastructure include 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. Actions performed in this area align with the control activities component of COSO. Infrastructure controls support timely processing of financial information and also help ensure its confidentiality. Deficiencies in this area may have a significant impact on financial reporting and disclosure. For instance, without sufficient controls over network communications, financial information could be obtained and publicized without authorization.	
IT management ensures that the setup and implementation of system software do not jeopardize the security of the data and programs being stored on the system.	Control activities
Procedures exist and are followed to ensure that infrastructure systems, including network devices and software, are installed and maintained in accordance with the acquisition and maintenance framework.	Control activities
Procedures exist and are followed to ensure that infrastructure system changes are controlled in line with the organization's change management procedures.	Control activities

Figure 19—Develop and Maintain Procedures	
Control Objective	**COSO Component**
Developing and maintaining procedures include the design and implementation of service level agreements, operational practices and training materials. Actions performed in this area align with the control activities and information and communication components of COSO. Controls designed and implemented in this area support an organization's ability to perform business process activities in a consistent and objective manner. For instance, without controls to maintain consistency in how application systems generate reports, the organization may not be able to reconcile financial information in a reliable manner.	
The organization's system development life cycle methodology requires that user reference and support manuals (including documentation of controls) be prepared as part of every information system development or modification project.	Control activities
The IT organization ensures that its systems and applications are supported with documentation and processes to enable long-term sustainability and maintainability.	Information and communication

Figure 20—Install and Accredit Systems	
Control Objective	**COSO Component**
Installation and accreditation relate to the migration of new systems into production. Before such systems are installed, appropriate testing and validation that systems are operating as designed must be performed. Activities in this area align with the control activities component of COSO. Without adequate testing, systems may not function as intended and may provide invalid information, which could result in unreliable financial information and reports.	
There exists a testing strategy for all significant changes in technology, which ensures that deployed systems operate as intended.	Control activities
Testing is performed at the unit, system, integration and user acceptance level and is included for all significant systems.	Control activities
Load and stress testing is performed according to a test plan and established testing standards.	Control activities
Interfaces with other systems are tested to confirm that data transmissions are complete, accurate and valid.	Control activities
The conversion of data is tested between its origin and its destination to confirm that it is complete, accurate and valid.	Control activities

Figure 21—Manage Changes	
Control Objective	**COSO Component**
Managing changes addresses how an organization modifies system functionality to help the business meet its objectives. Actions performed in this area align with the control activities and monitoring components of COSO. Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, changes to the accounts to which financial data are allocated require appropriate controls to ensure classification and reporting integrity.	
Requests for changes, system maintenance and supplier maintenance are standardized and are subject to formal change management procedures.	Control activities
Policies and procedures to manage emergency changes exist and are followed.	Control activities
IT management ensures that users are appropriately involved in the design of applications, selection of packaged software and the testing thereof, to ensure a reliable environment.	Control activities
Changes to systems and applications are performed in a timely manner and adhere to the organization's overall change management standards.	Control activities
Changes to IT systems and applications are performed as designed and meet the expectations of users.	Monitoring

3. General Controls—Deliver and Support

This domain deals with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training. To deliver services, the necessary support processes must be set up. This domain includes the actual processing of data by application systems, often classified under application controls.

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

- Define and manage service levels.
- Manage third-party service levels.
- Manage performance and capacity.
- Ensure continuous service.
- Ensure systems security.
- Educate and train users.
- Manage the configuration.
- Manage problems and incidents.
- Manage data.
- Manage facilities.
- Manage operations

Each of these control processes is outlined in **figures 22** through **32**.

Figure 22—Define and Manage Service Levels

Control Objective	COSO Component
Defining and managing service levels address how an organization meets the functional and operational expectations of its users and, ultimately, the objectives of the business. Roles and responsibilities are defined and an accountability and measurement model is used to ensure services are delivered, as required. Actions performed in this area align with the control activities and control environment components of COSO. 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.	
Selection of vendors for outsourced services is performed in accordance with the organization's vendor management policy.	Control activities
A framework is defined to establish key performance indicators to manage service level agreements, both internally and externally.	Control environment

Figure 23—Manage Third-party Service Levels	
Control Objective	**COSO Component**
Managing third-party services includes the use of outsourced service providers to support financial applications and related systems. Actions performed in this area align with the control environment, monitoring, control activities and risk assessment components of COSO. 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.	
IT management ensures that, before selection, potential third parties are properly qualified through an assessment of their capability to deliver the required service and their financial viability.	Control environment
Third-party service contracts address the risks, security controls and procedures for information systems and networks in the contract between the parties.	Control activities
Business continuity controls consider business risk related to third-party service providers in terms of continuity of service, and escrow contracts exist where appropriate.	Risk assessment
Procedures exist and are followed to ensure that a formal contract is defined and agreed to for all third-party services before work is initiated, including definition of internal control requirements and acceptance of the organization's policies and procedures.	Control activities
A designated individual is responsible for regular monitoring and reporting on the achievement of the third-party service level performance criteria.	Control activities
A regular review of security, availability and processing integrity is performed for service level agreements and related contracts with third-party service providers.	Monitoring

Figure 24—Manage Performance and Capacity	
Control Objective	**COSO Component**
Performance and capacity support an organization's efforts to maintain complete and accurate data. They also allow an organization to trace back transactions to source information to support their validity. Activities in this area align with the control activities and monitoring components of COSO. The lack of performance and capacity could result in the financial reporting process not meeting its reporting deadlines.	
IT management monitors the performance and capacity levels of the systems.	Monitoring
IT management has a process in place to respond to suboptimal performance and capacity measures in a timely manner.	Control activities
Performance and capacity planning is included in system design and implementation activities.	Control activities

Figure 25—Ensure Continuous Service	
Control Objective	**COSO Component**
Managing continuous service includes the ability to recover from a disaster. Controls need to be in place to manage various disaster scenarios, from backup and recovery to full business continuity. Actions performed in this area align with the control activities and monitoring components of COSO. Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, the inability to recover from a disaster after year-end could prevent the organization from producing financial reports that are supported with source documentation and details of transactions that make up financial reporting balances.	
IT management, in cooperation with business process owners, has established a business continuity framework that defines the roles, responsibilities, risk-based approach/methodology to be adopted, and the approval procedures.	Control activities
The business continuity plan identifies the critical application programs, third-party services, operating systems, personnel and supplies, data files, and time frames needed for recovery.	Control activities
The IT continuity plan is aligned with the overall business continuity plan to ensure consistency.	Control activities
The IT organization's members responsible for disaster continuity plans have been trained regarding the procedures to be followed in case of an incident or disaster.	Control activities
IT management has ensured that the continuity plan is adequately tested, at least annually, and that any deficiencies are addressed within a reasonable period of time.	Control activities
Where new risks are identified, appropriate changes are made to the business continuity and disaster recovery plans.	Control activities
Offsite storage and recovery facilities are periodically assessed, at least annually, for viability, adequacy and security mechanisms.	Monitoring
A business impact assessment has been performed that considers the impact of systems failure on the financial reporting and disclosure process.	Control activities
Management has reviewed the impact assessment in determining the nature and extent of system recovery procedures necessary to support the timeliness of financial reporting and disclosure processes.	Control activities

Figure 26—Ensure Systems Security	
Control Objective	**COSO Component**
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. Actions performed in this area align with the control activities, information and communication, and monitoring components of COSO. Deficiencies in this area could significantly impact financial reporting. For instance, insufficient controls over transaction authorization may result in unreliable financial reporting and disclosure controls.	
An IT security plan exists that is aligned with overall IT strategic plans.	Control activities
The IT security plan is updated to reflect changes in the IT environment as well as security requirements of specific systems.	Control activities

Figure 26—Ensure Systems Security *(cont.)*	
Control Objective	**COSO Component**
Procedures exist and are followed to ensure that all users are authenticated to the system to support the validity of transactions.	Control activities
Procedures exist and are followed to maintain the effectiveness of authentication and access mechanisms (e.g., regular password changes).	Control activities
Procedures exist and are followed to ensure timely action relating to requesting, establishing, issuing, suspending and closing user accounts.	Control activities
A formal approval process exists for granting access privileges to systems and data.	Control activities
A control process exists and is followed to periodically review and confirm access rights.	Control activities
Where appropriate, controls exist to ensure that transactions cannot be denied by either party and that controls are implemented to provide nonrepudiation of origin or receipt, proof of submission and receipt of transactions.	Control activities
Where network connectivity is used, appropriate controls, including firewalls, intrusion detection and vulnerability assessments, exist and are used to prevent unauthorized access.	Control activities
The IT security plan, and its related activities and priorities, reflects results of recent security assessments.	Information and communication
The IT security administrator monitors and logs security activity, and identified security violations are reported to senior management.	Monitoring

Figure 27—Educate and Train Users	
Control Objective	**COSO Component**
Educating and training users address how an organization supports its people to perform their job responsibilities in a reliable and controlled manner. Actions performed in this area align with the control environment component of COSO. Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, personnel unfamiliar with financial reporting policies may share confidential financial information with unauthorized parties, thereby undermining disclosure controls.	
The entity has established procedures for identifying and documenting the training needs of all personnel using information services in support of the long-range plan.	Control environment
IT management provides education and ongoing training programs that include ethical conduct, system security practices, confidentiality standards, integrity standards and security responsibilities of all staff.	Control environment

Figure 28—Manage the Configuration	
Control Objective	**COSO Component**
Configuration management ensures that security, availability and processing integrity controls are set up in the system and maintained through its life cycle. Activities in this area align with the control activities and monitoring components of COSO. Insufficient configuration controls can lead to security and availability exposures that may permit unauthorized access to systems and data. This would negatively impact an organization's ability to meet the internal control provisions of Section 404.	
Only authorized software is permitted for use by employees using company IT assets.	Control activities
System infrastructure, including firewalls, routers, switches, network operating systems, servers and other related devices, is properly configured to prevent unauthorized access.	Control activities
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.	Control activities
IT management has established procedures across the organization to protect information systems and technology from computer viruses.	Control activities
Periodic testing and assessment is performed to confirm that software and network infrastructure is appropriately configured.	Monitoring

Figure 29—Manage Problems and Incidents	
Control Objective	**COSO Component**
Managing problems and incidents addresses how an organization identifies, documents and responds to events that fall outside of normal operations. Actions performed in this area align with the control activities and information and communication components of COSO. Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, significant events such as breach of corporate security or unauthorized access to confidential information may result in a material weakness in disclosure controls.	
IT management has defined and implemented a problem management system to ensure that all operational events that are not part of the standard operation (incidents, problems and errors) are recorded, analyzed and resolved in a timely manner.	Control activities
Emergency program changes are approved, tested, documented and monitored.	Control activities
Problem escalation procedures are defined and implemented to ensure that problems are resolved in a timely manner.	Control activities
The problem management system provides for adequate audit trail facilities, which allow tracing from incident to underlying cause.	Information and communication
A security incident response process exists to support timely response and investigation of unauthorized activities.	Control activities

Figure 30—Manage Data	
Control Objective	**COSO Component**
Managing data includes the controls and procedures used to support information integrity, including its completeness, accuracy, authorization and validity. Controls are designed to support initiating, recording, processing and reporting financial information. These controls align with the control activities and information and communication components of COSO. Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, without appropriate authorization controls over the initiation of transactions, resulting financial information may not be reliable.	
Data processing controls, including processing totals, are used to support the completeness and accuracy of transaction processing, authorization and validity.	Control activities
Control procedures exist for maintaining the accuracy and validity of data inputs, including edit checks, validity checks and bound checks.	Control activities
Procedures exist and are followed to manage errors in a consistent and authorized manner.	Control activities
Policies and procedures exist for the handling, distribution and retention of data and reporting output.	Control activities
Management protects sensitive information, both logically and physically, in storage and during transmission against unauthorized access or modification.	Control activities
Procedures are defined and implemented to prevent access to sensitive information stored on offline physical media, e.g., laptop computers and offsite storage.	Control activities
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.	Control activities
Procedures exist to ensure that the contents of a media library containing sensitive data are inventoried and that discrepancies from physical inventory are remedied in a timely manner.	Control activities
Management has implemented a strategy for cyclical backup of data and programs.	Control activities
Procedures exist and are followed to periodically test the effectiveness of the restoration process and the quality of backup media.	Control activities
Policies and procedures exist and are followed to ensure that data retention practices meet business, legal and regulatory requirements.	Control activities
Policies and procedures exist and are followed to ensure that personally identifiable information is appropriately safeguarded and meets regulatory requirements.	Control activities
Changes to data structures are authorized, made in accordance with design specifications and are implemented in a timely manner.	Control activities
Changes to data structures are assessed for their impact on financial reporting processes.	Control activities
Procedures are in place to ensure that source documents are retained or are reproducible by the organization for an adequate amount of time to facilitate retrieval or reconstruction of data, and to satisfy legal requirements.	Information and communication

Figure 31—Manage Facilities	
Control Objective	**COSO Component**
Physical security and related controls help IT organizations maintain the security and availability of their systems. Activities performed in this area align with the control activities component of COSO. Without controls to protect physical access to systems and infrastructure, there is an increased risk of manipulation and destruction of data, which would adversely impact an organization's ability to accurately report its financial results.	
Access to facilities is restricted to authorized personnel and requires appropriate identification and authentication.	Control activities
Physical facilities are equipped with adequate environmental controls to maintain systems and data, including fire suppression, uninterrupted power service (UPS) power backup, air conditioning and elevated floors.	Control activities

Figure 32—Manage Operations	
Control Objective	**COSO Component**
Managing operations addresses how an organization maintains reliable application systems in support of the business to initiate, record, process and report financial information. Actions performed in this area align with the control activities and information and communication components of COSO. 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.	
Management has established and documented standard procedures for IT operations, including managing, monitoring and responding to security, availability and processing integrity events.	Control activities
Controls exist to maintain processing continuity during operator shift changes by providing for the formal handover of activity, status updates and reports on current operations.	Control activities
IT management has established appropriate metrics to effectively manage the day-to-day activities of the IT department.	Control activities
System event data are sufficiently retained to provide chronological information and logs to enable the reconstruction, review and examination of the time sequences of processing.	Information and communication

4. General Controls—Monitor and Evaluate

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

Most recently, the COSO framework has been identified as meeting the framework requirements of Section 404 of the Sarbanes-Oxley Act. Under these rules, management must disclose any material weakness and will be unable to conclude that the company's internal control over financial reporting is effective if there is one or more material weakness in such control. Furthermore, the framework on which management's evaluation is based will have to be a suitable, recognized control framework that is established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment.

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

- Monitor the processes.
- Assess internal control adequacy.
- Obtain independent assurance.

Each of these control processes is outlined in **figures 33** through **35**.

Figure 33—Monitor the Processes

Control Objective	COSO Component
The collection of information aligns with the information and communication and monitoring components of COSO. If insufficient information is collected, it could impact the effectiveness of internal control assessment.	
Performance indicators (e.g., benchmarks) from both internal and external sources are defined, and data are collected and reported regarding achievement of these benchmarks.	Information and communication
IT management monitors its delivery of services to identify shortfalls and responds with actionable plans to improve.	Monitoring

Figure 34—Assess Internal Control Adequacy	
Control Objective	**COSO Component**
The monitoring of internal control relates to the monitoring component of COSO. It is a process that assesses the quality of the system's performance over time. This can be accomplished through regular management and supervisory activities. The Sarbanes-Oxley attestation process could also be viewed as a separate evaluation of internal control. A deficiency in this area could significantly impact financial reporting and disclosure controls.	
IT management monitors the effectiveness of internal controls in the normal course of operations through management and supervisory activities, comparisons and benchmarks.	Monitoring
Serious deviations in the operation of internal control, including major security, availability and processing integrity events, are reported to senior management.	Monitoring
Internal control assessments are performed periodically, using self-assessment or independent audit, to examine whether internal controls are operating satisfactorily.	Monitoring

Figure 35—Obtain Independent Assurance	
Control Objective	**COSO Component**
Independent assurance over critical IT services and activities supports management's ability to deliver reliable systems. Activities in this area align with the monitoring component of COSO. Without independent assurance, IT systems may be at risk of unauthorized access or failure. Where appropriate, IT management should assess the frequency, priority and focus of independent assurance and promptly engage in a method to prevent unexpected loss of financial and operational systems.	
IT management obtains independent reviews prior to implementing significant IT systems that are directly linked to the organization's financial reporting environment.	Monitoring
IT management obtains independent internal control reviews of third-party service providers (e.g., by obtaining and reviewing copies of SAS70, SysTrust or other independent audit reports).	Monitoring

5. Application Controls—Business Cycles

Figures 36-41 refer to controls that extend into applications and business processes that contribute to the completeness, accuracy, validity and authorization controls. These application controls are provided as examples of controls that are commonly enabled by financial and related IT systems. These objectives should not be considered an exhaustive list, but rather an example of controls that are commonly enabled by application systems. Organizations will have to consider what additional control objectives are required based on their particular industry and operating environment.

Figure 36—Application Control Objectives for the Sales Cycle

Application Control Objective	COSO Component
Application controls apply to the business processes they support. They are controls designed within the application to prevent or detect unauthorized transactions. When combined with manual controls, as necessary, application controls ensure completeness, accuracy, authorization and validity of processing transactions. For the most part, objectives presented in this section can be supported with automated application controls. They are most effective in integrated ERP environments, such as SAP, PeopleSoft, Oracle, JD Edwards and others. For nonintegrated environments, these control objectives may require a combination of manual and automated procedures.	
Orders are processed only within approved customer credit limits.	Control activities
Orders are approved by management as to prices and terms of sale.	Control activities
Orders and cancellations of orders are input accurately.	Control activities
Order entry data are transferred completely and accurately to the shipping and invoicing activities.	Control activities
All orders received from customers are input and processed.	Control activities
Only valid orders are input and processed.	Control activities
Invoices are generated using authorized terms and prices.	Control activities
Invoices are accurately calculated and recorded.	Control activities
Credit notes and adjustments to accounts receivable are accurately calculated and recorded.	Control activities
All goods shipped are invoiced.	Control activities
Credit notes for all goods returned and adjustments to accounts receivable are issued in accordance with organization policy.	Control activities
Invoices relate to valid shipments.	Control activities
All credit notes relate to a return of goods or other valid adjustments.	Control activities
All invoices issued are recorded.	Control activities
All credit notes issued are recorded.	Control activities
Invoices are recorded in the appropriate period.	Control activities
Credit notes issued are recorded in the appropriate period.	Control activities
Cash receipts are recorded in the period in which they are received.	Control activities
Cash receipts data are entered for processing accurately.	Control activities
All cash receipts data are entered for processing.	Control activities

Figure 36—Application Control Objectives for the Sales Cycle *(cont.)*	
Application Control Objective	**COSO Component**
Cash receipts data are valid and are entered for processing only once.	Control activities
Cash discounts are accurately calculated and recorded.	Control activities
Timely collection of accounts receivable is monitored.	Control activities
The customer master file is maintained.	Control activities
Only valid changes are made to the customer master file.	Control activities
All valid changes to the customer master file are input and processed.	Control activities
Changes to the customer master file are accurate.	Control activities
Changes to the customer master file are processed in a timely manner.	Control activities
Customer master file data remain up-to-date.	Control activities

Figure 37—Application Control Objectives for the Purchasing Cycle	
Application Control Objective	**COSO Component**
Purchase orders are placed only for approved requisitions.	Control activities
Purchase orders are accurately entered.	Control activities
All purchase orders issued are input and processed.	Control activities
Amounts posted to accounts payable represent goods received.	Control activities
Amounts posted to accounts payable represent services received.	Control activities
Accounts payable amounts are accurately calculated and recorded.	Control activities
All amounts for goods received are input and processed to accounts payable.	Control activities
All amounts for services received are input and processed to accounts payable.	Control activities
Amounts for goods or services received are recorded in the appropriate period.	Control activities
Accounts payable are adjusted only for valid reasons.	Control activities
Credit notes and other adjustments are accurately calculated and recorded.	Control activities
All valid credit notes and other adjustments related to accounts payable are input and processed.	Control activities
Credit notes and other adjustments are recorded in the appropriate period.	Control activities
Disbursements are only made for goods and services received.	Control activities
Disbursements are distributed to the appropriate suppliers.	Control activities
Disbursements are accurately calculated and recorded.	Control activities
All disbursements are recorded.	Control activities
Disbursements are recorded in the period in which they are issued.	Control activities
Only valid changes are made to the supplier master file.	Control activities

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

Application Control Objective	COSO Component
All valid changes to the supplier master file are input and processed.	Control activities
Changes to the supplier master file are accurate.	Control activities
Changes to the supplier master file are processed in a timely manner.	Control activities
Supplier master file data remain up-to-date.	Control activities

Figure 38—Application Control Objectives for the Monetary Cycle

Application Control Objective	COSO Component
Borrowings are accurately recorded as to amounts and terms.	Control activities
All borrowings are recorded.	Control activities
Borrowings are recorded in the appropriate period.	Control activities
All interest is accurately calculated and recorded in the appropriate period.	Control activities
Recorded loan repayments are valid.	Control activities
Loan repayments are accurately recorded.	Control activities
All loan repayments are recorded.	Control activities
Loan repayments are recorded in the appropriate period.	Control activities
Investment purchases, sales and maturities are accurately recorded.	Control activities
All investment transactions are recorded.	Control activities
Investment transactions are recorded in the appropriate period.	Control activities
All investment income is accurately calculated and recorded in the appropriate period.	Control activities
Derivative transactions are accurately recorded.	Control activities
Derivative transactions are recorded in the appropriate period.	Control activities

Figure 39—Application Control Objectives for the Inventory Cycle

Application Control Objective	COSO Component
All adjustments to inventory prices or quantities are recorded.	Control activities
Adjustments to inventory prices or quantities are recorded promptly and in the appropriate period.	Control activities
Adjustments to inventory prices or quantities are accurately recorded.	Control activities
All credits to inventory related to billed sales are approved by management and such approval is documented.	Control activities
Raw materials are received and accepted only if they have valid purchase orders.	Control activities
Raw materials received are accurately recorded.	Control activities
All raw materials received are recorded.	Control activities
Receipts of raw materials are recorded promptly and in the appropriate period.	Control activities

Figure 39—Application Control Objectives for the Inventory Cycle *(cont.)*

Application Control Objective	COSO Component
Defective raw materials are promptly returned to suppliers.	Control activities
All transfers of raw materials to production are accurately recorded and in the appropriate period.	Control activities
All recorded production costs are consistent with actual direct and indirect expenses associated with production.	Control activities
All direct and indirect expenses associated with production are recorded as production costs.	Control activities
All direct and indirect expenses associated with production are recorded accurately and in the appropriate period.	Control activities
All transfers of completed units of production to finished goods inventory are recorded completely and accurately in the appropriate period.	Control activities
Finished goods returned by customers are recorded completely and accurately in the appropriate period.	Control activities
Finished goods received from production are recorded completely and accurately in the appropriate period.	Control activities
Goods received from production or returned by customers are accepted only in accordance with the organization's policies.	Control activities
All shipments are recorded.	Control activities
Shipments are accurately recorded.	Control activities
Shipments are recorded promptly and in the appropriate period.	Control activities
Inventory is relieved only when goods are shipped with approved customer orders.	Control activities
Costs of shipped inventory are transferred from inventory to cost of sales.	Control activities
Costs of shipped inventory are accurately recorded.	Control activities
Amounts posted to cost of sales represent those associated with shipped inventory.	Control activities
Costs of shipped inventory are transferred from inventory to cost of sales promptly and in the appropriate period.	Control activities
Only valid changes are made to the inventory management master file.	Control activities
All valid changes to the inventory management master file are input and processed.	Control activities
Changes to the inventory management master file are accurate.	Control activities
Changes to the inventory management master file are promptly processed.	Control activities
Inventory management master file data remain up-to-date.	Control activities

Figure 40—Application Control Objectives for the Asset Management Cycle

Application Control Objective	COSO Component
Fixed asset acquisitions are accurately recorded.	Control activities
Fixed asset acquisitions are recorded in the appropriate period.	Control activities
All fixed asset acquisitions are recorded.	Control activities
Depreciation charges are accurately calculated and recorded.	Control activities
All depreciation charges are recorded in the appropriate period.	Control activities
All fixed asset disposals are recorded.	Control activities
Fixed asset disposals are accurately calculated and recorded.	Control activities
Fixed asset disposals are recorded in the appropriate period.	Control activities
Records of fixed asset maintenance activity are accurately maintained.	Control activities
Fixed asset maintenance activities records are updated in a timely manner.	Control activities
Only valid changes are made to the fixed asset register and/or master file.	Control activities
All valid changes to the fixed asset register and/or master file are input and processed.	Control activities
Changes to the fixed asset register and/or master file are accurate.	Control activities
Changes to the fixed asset register and/or master file are promptly processed.	Control activities
Fixed asset register and/or master file data remain up-to-date.	Control activities

Figure 41—Application Control Objectives for the Human Resources Cycle

Application Control Objective	COSO Component
Additions to the payroll master files represent valid employees.	Control activities
All new employees are added to the payroll master files.	Control activities
Terminated employees are removed from the payroll master files.	Control activities
Employees are terminated only within statutory and union requirements.	Control activities
Deletions from the payroll master files represent valid terminations.	Control activities
Time and attendance data records reflect actual time worked and are authorized.	Control activities
All time worked is input.	Control activities
Time worked is accurately input and processed.	Control activities
Time worked is processed in a timely manner.	Control activities
Payroll is recorded in the appropriate period.	Control activities
Payroll (including compensation and withholdings) is accurately calculated and recorded.	Control activities
Payroll disbursements and recorded payroll expenses relate to actual time worked.	Control activities

Figure 41—Application Control Objectives for the Human Resources Cycle *(cont.)*

Application Control Objective	COSO Component
Payroll is disbursed to appropriate employees.	Control activities
Only valid changes are made to the payroll master files.	Control activities
All valid changes to the payroll master files are input and processed.	Control activities
Changes to the payroll master files are accurate.	Control activities
Changes to the payroll master files are processed in a timely manner.	Control activities
Payroll master file data remain up-to-date.	Control activities
Only valid changes are made to the payroll withholding tables.	Control activities
All valid changes to the payroll withholding tables are input and processed.	Control activities
Changes to the payroll withholding tables are accurate.	Control activities
Changes to the payroll withholding tables are promptly processed.	Control activities
Payroll withholding table data remain up-to-date.	Control activities
Statutory withholding tables are consistent with statutory requirements.	Control activities

References

COBIT 3rd Edition©, IT Governance Institute, Rolling Meadows, Illinois, USA, July 2000

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *www.coso.org*

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

Exposure Draft Enterprise Risk Management Framework, Committee of Sponsoring Organizations of the Treadway Commission (COSO), USA, July 2003

"*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, US Securities and Exchange Commission, USA, June 2003, *www.sec.gov/rules/final/33-8238.htm*

Internal Control—Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission (COSO), AICPA, New York, USA, 1992

ISO IEC 17799, *Code of Practice for Information Security Management*, International Organisation for Standardisation (ISO), Switzerland, 2000

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

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

Public Company Accounting Oversight Board, Proposed Auditing Standard: "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements," Release No. 2003-17, Rulemaking Docket Matter No. 008, USA, 7 October 2003

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

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

"The Standard of Good Practice for Information Security," Information Security Forum, 2003

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