Sarbanes-Oxley and IT Outsourcing

By Lily Shue, CISA, CISM, CCP

The US Sarbanes-Oxley Act of 2002 has ushered in a new era in the history of business. The Act has fundamentally changed the business and regulatory environment in terms of corporate governance, and ultimately strengthens corporate accountability, disclosure and reporting. Sections 302 and 906 of the Act have laid a foundation for restoring investor confidence in the integrity of public reporting. Section 404 requires that management file an internal control report with its annual report and that the report include management’s responsibilities in establishing and maintaining adequate internal control over financial reporting and the effectiveness of these controls. The US Securities and Exchange Commission (SEC) further indicates in its final rule that the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control–Integrated Framework would satisfy these requirements. The SEC also acknowledges that frameworks other than COSO may be used in the future within the US, if they satisfy the intent of the statute without diminishing the benefits to investors.

**Why COBIT?**

*Control Objectives for Information and related Technology* (COBIT) is an open framework and can be aligned with the spirit of Sarbanes-Oxley requirements and any general framework used, such as COSO. It is an IT governance model that provides entity-level and activity/process-level objectives along with associated controls. Using certain sections of the COBIT framework, a company can design a system of IT controls to comply with section 404. Figure 1 depicts the alignment of the domains of COBIT with COSO, as well as sections 302 and 304 of Sarbanes-Oxley.

**Information Technology Controls**

Sarbanes-Oxley makes corporate executives explicitly responsible for establishing, evaluating and monitoring the effectiveness of internal control over financial reporting. With the widespread reliance on IT systems, controls are needed over all such systems. As such, IT is the foundation of an effective system of internal control over financial reporting, since reliance on IT is either through a unified enterprise resource planning (ERP) system or a disparate collection of operational and financial management software applications.

**Types of IT Controls**

IT controls commonly include general controls and application controls. IT general controls refer to controls over:
- IT environment
- Computer operations
- Logical access to programs and data
- Program development and maintenance
- Program and infrastructure changes

These controls apply to all system processing environments from traditional mainframe to client-server to web hosting environments. In addition, the IT control environment includes the IT governance process, monitoring and reporting. The IT governance process includes:
- Information systems strategic plan
- IT risk management process
- Compliance and regulatory management
- IT policies, procedures and standards
- Monitoring and reporting required to ensure IT is aligned with business requirements

Application controls, on the other hand, refer to controls embedded in business process applications such as large ERP systems and smaller, best-of-breed systems. Examples of application controls include system logics designed into the application/system to ensure:
- Completeness
- Accuracy
- Validity
- Authorization
- Segregation of duties

Traditionally, IT general controls were needed to ensure the function of application controls that depend on computer processes. As an IT organization becomes more focused on alignment with the business, IT general controls and application controls become more integrated and IT general controls increasingly supplement application and business process controls. IT general controls are needed to support the functioning of application controls and both are needed to ensure the completeness and accuracy of information processing. Meeting Sarbanes-Oxley requirements within IT can help to enhance overall IT governance, a better understanding of IT among executives, as well as the ability to make better business decisions with higher quality and more timely information.
IT Outsourcing and Service Provider Implications

Some public companies have outsourced their IT functions (e.g., computer operations, application development and maintenance, IT infrastructure supports, web hosting services and application supports) to third-party service organizations or outsourcing suppliers. Some of these arrangements involve moving certain activities to operational locations outside the headquarters (offshoring). As stated in IT Control Objectives for Sarbanes-Oxley, published by the IT Governance Institute (ITGI), “These ‘outsourcing’ services are part of an organization’s overall operations and responsibilities and need to be considered in the overall IT internal control program.”

For the purpose of this discussion, a public company will be referred to as “user company” and the auditor for the public company will be referred to as “user auditor.” An organization that provides outsourcing services will be referred to as “service organization” and the auditor who performs audits for the service organization will be referred to as “service auditor.”

There are a number of challenges in terms of Sarbanes-Oxley requirements and outsourcing. The following outlines some of the challenges that must be addressed under Sarbanes-Oxley:

- The Public Company Accounting Oversight Board (PCAOB) was established by the Sarbanes-Oxley Act to oversee the audits of the financial statements of public companies.

PCAOB, in its auditing standard No. 2, specifically states that:

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

2. “If the service organization is part of a user company’s information system—they are part of the company’s internal control over financial reporting…”

3. “…a service organization does not reduce management’s responsibility to maintain effective internal control.”

4. Management should evaluate controls at the service organization as well as related controls at the user company when assessing internal controls over financial reporting. From the IT perspective, if the services provided are significant, it will require both management and its independent auditors to evaluate the service organization’s controls.

User companies should include an assessment of the service organization in arriving at a conclusion on the reliability of its internal control. Further, when a secondary organization is providing services to the service organization that may be relevant to the user organization, internal controls of the secondary organization should also be included in arriving at a conclusion on the reliability of its internal control.

- Documentation requirements of service organization control activities should be at the same level as the user company. This should include:
  1. Obtaining an understanding of controls at the service organization that are relevant to an organization’s internal control
  2. Obtaining an understanding of the organization’s control over the service organization’s activities
  3. Obtaining evidence that controls that are relevant to management’s assessment and the auditor’s opinion are operating effectively

4. Performing tests of management’s controls over activities of the service organization

5. Performing tests of controls at the service organization

- Obtain, review and evaluate the results of SAS70 reports on relevant subject matters. Traditionally, audit opinions commonly known as SAS70 reports have been performed for service organizations. From a Sarbanes-Oxley compliance perspective, these audit reports must include:
  1. Report on controls placed in operation, which must be as of a point in time and must provide:
     - Control documentation
     - Assurance as to the design of the controls
     - An opinion on the operating effectiveness of the controls for any period
  2. Test of controls, results of the tests and the service organization auditor’s opinion on operating effectiveness.

If audit reports do not include these areas, they may not be deemed sufficient for purposes of Sarbanes-Oxley compliance. Under such conditions, service organizations may wish to consult with their external auditors to understand the specific requirements.

A Service Organization’s Auditor Report

From the IT governance perspective, certain parts of the service auditor’s report need to be reviewed. The parts to be reviewed are:

- Identify where and how service organizations are being used.
- Assess the significance of services provided by the service organization.
- Evaluate service management efforts in assessing controls over the service organization.
- Obtain evidence over the relevance of service organization controls:
  1. Obtain test results performed by service auditor on controls.
  2. Obtain a copy of the service auditor’s report on controls (SAS70 Type 2 reports).

- Review the service auditor’s report:
  1. Evaluate report contents (scope, procedures, results). Since not all SAS70 reports are alike, user management needs to evaluate the relevance of the objectives, controls and tests to service and user management’s objectives.
    (Note: There are two types of SAS70 reports. Type 1 reports on controls placed in operation, and Type 2 reports on test of operating effectiveness of controls for a period of time. User management should review the Type 2 report.)
  2. Determine control objectives addressing the service organization’s procedures:
    - Transaction initiation
    - Authorization
    - Recording
    - Processing
    - Reporting
    - IT general controls and application controls as appropriate
  3. Evaluate the service auditor’s opinion.
  4. If a significant period of time has elapsed, consider changes in the service organization’s controls including:
    - Personnel
    - Reports/data received from the service organization
    - Service level agreements/contracts
– Errors identified in the service organization’s processing
5. Determine if service management has identified any relevant changes and has evaluated the effect of such changes on controls relating to financial reporting.
6. Determine if results of other procedures indicate changes have occurred at the service organization and have not been identified by service management.
7. Determine if there is a history of errors or other reasons that require above-normal risk assessment efforts.
8. Evaluate the service auditor’s professional credentials including independence.
9. Conclude whether sufficient evidence has been obtained to provide reasonable assurance necessary for rendering assessment and opinion.

• In the absence of a SAS70 Type 2 report, consider the following procedures:
  1. Establish clearly defined service level agreements.
  2. Establish a service contract to stipulate controls that need to be in place. This should include IT general and application controls.
  3. Determine whether an independent controls review has ever been performed and the scope and findings that resulted from the review.
  4. Determine service management’s action to gain comfort over the service organization’s control.
  5. Determine if other control areas needed to be addressed.

When reviewing the service auditor’s report, Robert J. Gareis of Baker & McKenzie (Chicago, Illinois, USA office) Corporate & Securities Law Practice, recommended the inclusion of the following factors for evaluation:

Section 404 of Sarbanes-Oxley requires the SEC to prescribe rules requiring each annual report of a public company issuer to make an internal control report containing:

• A statement of management’s responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting
• An assessment by management at the end of the company’s most recent fiscal year of the effectiveness of the company’s internal control structure and procedures for financial reporting
• Controls subject to assessment by management include, but are not limited to:
  – Controls over initiating, recording, processing and reconciling account balances
  – Classes of transactions included in the financial statements
  – Controls related to the initiation and processing of non-routine and non-systematic transactions

• Controls related to the selection and application of appropriate accounting policies
• Controls related to the prevention, identification and detection of fraud

Summary
Public companies that outsource IT processes and their outsourcers have new requirements under Sarbanes-Oxley. Since not all SAS70 reports are alike, the user auditor needs to evaluate the relevance of the objectives, controls and tests to service and user management’s objectives. Management at both companies and their auditors need to be involved. Issues will most likely be derived and addressed through issue identification and focused negotiations. Outsourcing agreements must contain provisions that seek to establish roles and responsibilities of the customer and supplier that facilitate compliance. The CEO and CFO should consider deployment of effective due diligence procedures to assure the discharge of their responsibilities and to avoid penalties for willful noncompliance.

Endnotes
1 IT Control Objectives for Sarbanes-Oxley, IT Governance Institute, Illinois, USA, April 2004, www.itgi.org
2 Zonnevald, Paul; Ken Vander Wal; “Outsourcing and Service Providers: The Implications for Sarbanes-Oxley,” presentation at the Sarbanes-Oxley Symposium, Illinois, USA, 6–7 March 2004
5 Op.cit., IT Control Objectives for Sarbanes-Oxley

Lily Shue, CISA, CISM, CCP
is a director of LMS Associates LLC. In this capacity, she is responsible for risk management and regulatory compliance consulting services and has extensive experience in assisting publicly held companies in assessing Sarbanes-Oxley readiness. In addition, she is a contributor to several ITGI research projects.