

## Chapter 2

# SOX and COBIT Defined

### Solutions in this chapter:

- SOX Overview
- Why IT COBIT?
- Are the Developers of COBIT Controls Crazy? Is This Practical?
- Sustainability Is the Key

- ☑ Summary
- ☑ Solutions Fast Track
- ☑ Frequently Asked Questions

## SOX Overview

As a result of the financial scandals at major Fortune 100 companies in 2001, Congress enacted the Sarbanes-Oxley Act of 2002. This act affects how public companies report financials, and significantly impacts IT. Sarbanes-Oxley compliance requires more than documentation and/or establishment of financial controls; it also requires the assessment of a company's IT infrastructure, operations, and personnel. Unfortunately, the requirements of the Sarbanes-Oxley Act of 2002 do not scale based on the size or revenue of a company. Small to medium-sized companies (IT department) will face unique challenges, both budgetary and with personnel, in their effort to comply with the Sarbanes-Oxley Act of 2002.

### The Transparency Test...

#### The CFO Perspective

"It is not clear that the intent of SOX could not have been met with the requirements under Section 302. However, with the requirements included under Section 404, companies need a framework for implementation. COBIT provides a methodical approach to the IT function for Sarbanes-Oxley implementation and support. While using the framework provided, each company will need to customize the approach to its own size and complexity. A multinational, multidivisional organization is different from a single factory domestic company. The authors provide an example for this customization and rightfully point out that SOX will evolve over time, at least for the first few years." — Steve Lanza

## What Will SOX Accomplish?

There continues to be much controversy and debate about the effectiveness of SOX. Although most people who are aware of the requirements to comply with SOX (Section 404) believe the intention was good, there exists controversy over whether the existing 302 reporting requirements are sufficient.

If you read Sections 302 and 404, you may see similarities, and subsequently, why a controversy may exist as to whether (Section 404) SOX requirements and compliance were necessary. The next two sections in this chapter include an example of Sections 302 and 404 as they pertain to a company's executive management assertions.

## Section 302

In accordance with Section 302, executive management of a public company:

- a) are responsible for establishing and maintaining internal controls
- b) have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared

## Section 404

In accordance with Section 404, executive management of a public company:

- a) are responsible for establishing and maintaining an adequate internal control structure and procedures for financial reporting
- b) must report the effectiveness of the internal control structure and procedures

We will discuss Section 302 and Section 404 in later chapters of this book.

## SOX: Not Just a Dark Cloud

The initial response to Sarbanes-Oxley may be as yet another drain on your already understaffed, overtaxed IT department; however, this does not necessarily have to be the case. Whether SOX compliance is viewed as just another project, or a strategic opportunity for the IT department to reduce the project backlog, will be determined by how the CFO, CIO, or IT Director positions SOX compliance with executive management. However, because a majority of companies will view SOX compliance as a Finance initiative and may not involve IT, or limit IT's involvement to the project's periphery, this may be easier said than done. Because of this "limited" perception of SOX compliance, the process of positioning with executive management to include IT within this initiative may require significant effort, but will be well worth it.

If properly executed, the SOX compliance process gives CFOs, CIOs, and IT Directors an opportunity to address antiquated systems, personnel resource issues, and documentation/process issues. It will also provide them the opportunity to forge stronger alliances with the business units. IT will be critical to the success of SOX compliance, and the support of the business units will be critical to the success of IT.

**TIP**

When implementing new processes, procedures, or applications for SOX compliance, the activities should add value to the business unit(s) or the overall business.

Be prepared for change; as auditors gain more knowledge about SOX, their interpretation will change, and subsequently, so will their requirements of your IT organization.

## Why IT COBIT?

Sarbanes-Oxley compliance will significantly impact the IT organization of most public companies. However, there is one enormous problem: there is no specific mention of IT in Section 404, and more importantly, there are no specifics as to what controls have to be established within an IT organization to comply with Sarbanes-Oxley legislation.

If there is no specific mention in Section 404 as to what IT needs to do to comply with Sarbanes-Oxley, the logical question would be, “How can I comply with something without knowing what I need to do to comply?” Although there are various standards a company can use for defining and documenting its internal controls—ITIL (IT Infrastructure Library), Six Sigma, and COBIT—the majority of auditors have adopted COBIT.

ITIL is an international series of documents used to aid the implementation of a framework for IT Service Management. The intent of the framework is to define how Service Management is applied within specific organizations. Given that the framework consists of guidelines, it is agnostic of any application or platform and can therefore be applied in any organization.

In many organizations, Six Sigma simply means a measure of quality that strives for near perfection. Six Sigma is a disciplined, data-driven approach and methodology for eliminating defects (driving toward six standard deviations between the mean and the nearest specification limit) in any process—from manufacturing to transactional and from product to service.

COBIT stands for Control Objectives for Information and Related Technology. While the COBIT guidelines have been around since 1996, the guidelines and best practices have almost become the de facto standard for auditors and SOX compliance, mostly because the COBIT standards are platform independent. There are approximately 300 generic COBIT objectives, grouped under six COBIT

Components. When reviewing and applying the COBIT guidelines and best practices, keep in mind that they will need to be tailored to your particular environment.

## The Six COBIT Components

COBIT consists of six components:

- **Executive Summary** Explains the key concepts and principles.
- **Framework** Foundation for approach and COBIT elements. Organizes the process model into four domains:
  - Plan and organize
  - Acquire and implement
  - Deliver and support
  - Monitor and evaluate
- **Control Objective** Foundation for approach and COBIT elements. Organizes the process model into the four domains (discussed in a moment).
- **Control Practices** Identifies best practices and describes requirements for specific controls.
- **Management Guidelines** Links business and IT objectives and provides tools to improve IT performance.
- **Audit Guidelines** Provides guidance on how to evaluate controls, assess compliance, and document risk with these characteristics:
  - Define “internal controls” over financial reporting
  - Internally test and assess these controls
  - Support external audits of controls
  - Document compliance efforts
  - Report any significant deficiencies or material weaknesses

In conclusion, although an IT organization is free to select any predefined standards, or even one they develop to assist them in obtaining Sarbanes-Oxley compliance, the mostly widely accepted standard is COBIT. Subsequently, you may find that selecting COBIT will be the path of least resistance to Sarbanes-Oxley compliance.

**TIP**

COBIT guidelines and best practices will need to be tailored to your environment. Although the enormity of the COBIT guidelines and best practices may appear daunting, it can and should be distilled down to what is pertinent to your environment.

## Entity Level Controls versus Control Objectives

Entity level controls consist of the policies, procedures, practices, and organizational structures intended to assure the use of IT will enable the accomplishments of business objectives, and that planned events will be prevented, or detected and corrected.

*Control objective* is a statement of the desired result or purpose to be achieved by implementing control procedures for a particular IT activity. When developing and documenting your controls, you will want to keep in mind several characteristics so your controls will be as effective as possible:

Key control characteristics include:

- Employees are aware of their responsibilities for the control activities.
- The control is clearly understood.
- The control is effective in preventing, detecting, or correcting risk.
- The operating effectiveness of the control activity is adequately evaluated on a regular basis.
- The standards and assertions required to execute the control are clearly understood.
- Deficiencies are identified and remedied in a timely manner.
- The performance of the control can be documented.
- The controls, policies, and procedures are documented.

**TIP**

Although the goal is to implement a control that will be 100-percent effective, it is not realistic. Therefore, the objective should be to implement the most effective control within your environment. Be prepared to explain to your auditors how your environment works and why a particular control is effective in your environment.

## What Are the Four COBIT Domains?

We'll now briefly describe each COBIT domain.

### Planning and Organization

Planning is about developing strategic IT plans that support the business objectives. These plans should be forward looking and in alignment with the company's planning intervals; that is, a two-, three-, or five-year projection.

### Acquisition and Implementation

Once the plans are developed and approved, you may need to acquire new applications, or even acquire or develop a new staff skill set to execute the plans. Upon completion of the Acquisition phase, the plans now need to be enacted in the Implementation phase, which should include maintenance, testing, certifying, and identification of any changes needed to ensure continued availability of both existing and new systems.

### Delivery and Support

This phase ensures that systems perform as expected upon implementation, and continue to perform in accordance with expectations over time, usually managed via service level agreements (SLAs). In this regard, systems can be related to infrastructure components or third-party services.

### Monitoring

The monitoring phase uses the SLAs or baseline established in subsequent phases to allow an IT organization to gauge how they are performing against expectation, and provides them with an opportunity to be proactive.

## Are the Developers of COBIT Controls Crazy? Is This Practical?

A cursory review of the COBIT controls described in this section would convince any CEO, CFO, or IT director that implementation of COBIT controls is a daunting task, and the developers of the controls must be crazy. Neither of the aforementioned assumptions necessarily has to be the case. Whether the task of implementing COBIT controls is daunting will depend on how much effort is put into filtering the COBIT controls. Keep in mind that although all the controls center on good, sound practices, even the largest and most well run organization will not be able to implement all of them as defined by COBIT—a good idea, yes, but not necessarily practical. The keys to culling down COBIT controls center on a couple of questions:

- Which controls are appropriate to your environment?
- Of the appropriate controls, which will maximize your efforts?

After you have successfully answered the preceding questions, you will be in a position to reduce the COBIT controls to a manageable and actionable list for your implementation. Prior to executing your list of controls, you should verify your assumptions with your auditor. In addition, as part of your assessment process, you should identify all areas that are not appropriate for your environment, and be prepared to justify and defend these exclusions to your auditors as part of the Gap and Remediation process.

Tables 2.1 through 2.4 outline a partial list of the COBIT controls, and show some of the control objectives for each process cycle and the risk factor to which they relate. For a complete listing, see Appendix A.

**Table 2.1** Planning and Organization

	<b>Risk</b>	<b>Control Objective</b>
1	IT plans may not be present in the organization's long- and short-range plans. The organization's plans may not support IT.	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 direction.

Continued

**Table 2.1 continued** Planning and Organization

	<b>Risk</b>	<b>Control Objective</b>
2	IT plans may not be updated regularly.	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.
3	IT plans may not be consistent with the organization's goals and may impair the achievement of business objectives.	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.
4	New business processes may conflict with current IT plans, or new IT plans may conflict with current business processes.	The IT organization ensures that IT plans are communicated to business process owners and other relevant parties across the organization.
5	IT activities may not be understood by management or business processes, so conflicts may not be known.	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.
6	Changes in the business or IT environment may unknowingly impact IT plans.	The IT organization monitors its progress against the strategic plan and reacts accordingly to meet established objectives.
7	IT architecture may not support the growth of the business or current business goals.	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.
8	IT security levels may not comply with regulatory or corporate policies regarding information protection.	IT management has defined information classification standards in accordance with corporate security and privacy policies.

Continued

**Table 2.1 continued** Planning and Organization

	<b>Risk</b>	<b>Control Objective</b>
9	IT security levels may not comply with regulatory or corporate policies regarding information protection. IT security plans may not be updated regularly.	IT management has defined, implemented, and maintained security levels for each data classification. These security levels represent the appropriate (minimum) set of security and control measures of each of the classifications and are reevaluated periodically and modified accordingly.
10	Information systems data may not be reliable if systems are not functioning as intended, or errors are not dealt with appropriately.	IT managers have adequate knowledge and experience to fulfill their responsibilities.

**Table 2.2** Acquire and Implement

	<b>Risk</b>	<b>Control Objective</b>
1	Program development may not adhere to regulatory or corporate processes and procedures risking data integrity.	The organization has a system development life cycle methodology that considers security, availability, and processing integrity requirements of the organization.
2	Program implementations may not function as intended, risking the integrity of the calculations, data capture, data integrity, or the implementation of unauthorized processes.	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.
3	New application selection may not support business and regulatory objectives.	The organization has an acquisition and planning process that aligns with its overall strategic direction.
4	Business objectives may not be achieved, or undetected processes may be installed in production systems.	The organization acquires software in accordance with its acquisition and planning process.

Continued

**Table 2.2 continued** Acquire and Implement

Risk	Control Objective
5 Integrity of the implementation may not be achieved, and the program may not function as intended.	Procedures exist to ensure that system software is installed and maintained in accordance with the organization's requirements.
6 Integrity of the implementation may not be achieved, the program may not function as intended, and unauthorized processes may be installed undetected.	Procedures exist to ensure that system software changes are controlled in line with the organization's change management procedures.
7 System program upgrades may change security settings and allow unauthorized access to protected information.	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.
8 System program upgrades may interrupt production and network services, corrupting data or other 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.
9 System program upgrades may interrupt production and network services, corrupting data or other activities.	Procedures exist and are followed to ensure that infrastructure system changes are controlled in line with the organization's change management procedures.
10 Consistent application of application reporting and transaction processing may not occur, jeopardizing the integrity of the data and financial statement reporting.	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.

**Table 2.3** Delivery and Support

	<b>Risk</b>	<b>Control Objective</b>
1	Financial data integrity may be compromised if the system is not functioning as intended.	Selection of vendors for outsourced services is performed in accordance with the organization's vendor management policy.
2	Financial data integrity may be compromised if the system is not functioning as intended.	A framework is defined to establish key performance indicators to manage SLAs, both internally and externally.
3	Vendor viability may risk the delivery of programs and subsequent support of the application.	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.
4	Vendors have access to protected and sensitive data; confidentiality may be compromised.	Third-party service contracts address the risks, security controls, and procedures for information systems and networks in the contract between the parties.
5	If systems fail, data integrity may be compromised, or business objectives may not be met.	Business continuity controls consider business risk related to third-party service providers in terms of continuity of service, and escrow contracts exist where appropriate.
6	Confidentiality and achievement of business objectives may be breached.	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.
7	Vendor failures may go undetected.	A designated individual is responsible for regular monitoring and reporting on the achievement of the third-party service level performance criteria.

Continued

**Table 2.3 continued** Delivery and Support

	<b>Risk</b>	<b>Control Objective</b>
8	Financial data integrity may be compromised if the system is not functioning as intended.	A regular review of security, availability, and processing integrity is performed for SLAs and related contracts with third-party service providers.
9	Capacity to retain the source transaction information may be limited.	IT management monitors the performance and capacity levels of the systems.
10	SLAs may not be met.	IT management has a process in place to respond to suboptimal performance and capacity measures in a timely manner.

**Table 2.4** Monitor and Evaluate

	<b>Risk</b>	<b>Control Objective</b>
1	Breakdowns in performance may not be detected and corrected in a timely fashion.	Performance indicators (e.g., benchmarks) from both internal and external sources are defined, and data are collected and reported regarding achievement of these benchmarks.
2	Breakdowns in performance may not be detected and corrected in a timely fashion.	IT management monitors its delivery of services to identify shortfalls and responds with actionable plans to improve.
3	Breakdowns in performance may not be detected and corrected in a timely fashion.	IT management monitors the effectiveness of internal controls in the normal course of operations through management and supervisory activities, comparisons, and benchmarks.
4	Breakdowns in performance may not be detected and corrected in a timely fashion.	Serious deviations in the operation of internal control, including major security, availability, and processing integrity events, are reported to senior management.

Continued

**Table 2.4 continued** Monitor and Evaluate

	<b>Risk</b>	<b>Control Objective</b>
5	Lack of independent assessment could cause structural control deficiencies to go undetected.	Internal control assessments are performed periodically, using self-assessment or independent audits, to examine whether internal controls are operating satisfactorily.
6	System flaws could lead to errors that impact the financial reporting environment.	IT management obtains independent reviews prior to implementing significant IT systems that are directly linked to the organization's financial reporting environment.
7	Controls for outsourced IT assets and facilities may not be sufficient.	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).

## What Controls Should I Use?

Let's explore how this intimidating list can be reduced based on the size and complexity of a particular company. For this process, we will create a fictitious company named XYZ Sprockets, a small public company with 90 employees. XYZ Sprockets has only one office, which houses its operations and manufacturing. The company's entire IT staff consists of two full-time employees, one server admin and one desktop technician. Although small, the company is the number-one manufacturer of bicycle gears, currently having 80 percent of the market. It generates \$40 million a year in revenue, approximately \$10 million per quarter.

When determining what controls you will need to put in place, you'll discover that what XYZ Sprockets does not have and does not support is as important as what the company does have and support. The importance of this will become clear in subsequent chapters. Here is a quick rundown on XYZ Sprockets' IT infrastructure.

### Server Room

XYZ Sprockets' server infrastructure is as follows:

- Windows 2000 departmental file servers, one each for Finance, Marketing, and HR
- Active Directory for authentication

### Desktops

Here's a look at XYZ Sprockets' desktop inventory:

- Eighty employees in the main office running Windows 98, Windows 2000, and Windows XP
- Ten Windows XP laptops, Microsoft Office, Visio, and Project for desktop applications
- Outlook for e-mail client
- Internet Explorer
- Norton AntiVirus

## Outsourced Services

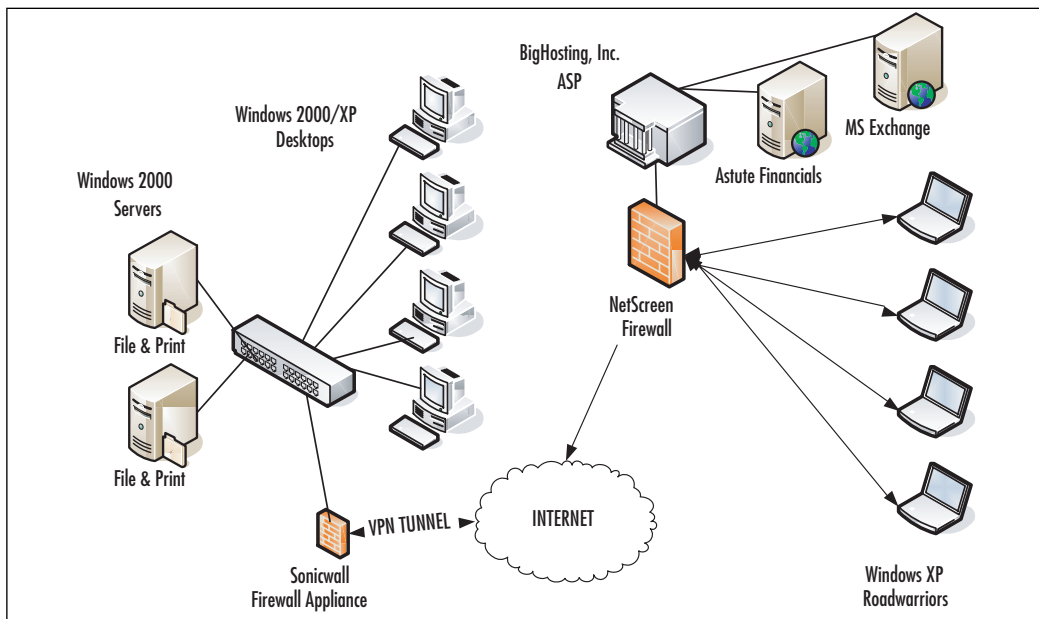
XYZ Sprockets has elected to outsource the following services to BigHosting Inc. to facilitate a small, in-house IT organization:

- VPN services
- Financials in-house developed
- E-mail
- Internet access
- Telecommunications

## Outsourced Services

Figure 2.1 diagrams XYZ Sprockets' networking infrastructure.

**Figure 2.1** XYZ Sprockets' Network Topology



Based on XYZ Sprockets' environment, the list of Control Objectives shown in Table 2.5 could be applicable for the company's SOX compliance. As the majority of the Planning and Organization Control Objectives are related to management function, there is generally little opportunity to reduce the required number of actions.

However, if you review the subsequent domains, note that various Control Objectives have been left off. The missing Control Objectives were not omitted, but rather intentionally left off, as they did not apply to XYZ Sprockets' specific environment. The logic behind customizing the Control Objectives to a specific environment is discussed in subsequent chapters.

**Table 2.5** Control Objectives Applicable for SOX Compliance at XYZ Sprockets

Domain	Removed Control Objective
Planning and Organization	N/A
Acquire and Implement	1, 2, and 10
Delivery and Support	5 and 10
Monitor and Evaluate	6

## Planning and Organization

1. Management prepares strategic plans for IT that align business objectives with IT strategies.
2. Management obtains feedback from business process owners and users regarding the quality and usefulness of its IT plans in the ongoing risk assessment process.
3. An IT planning or steering committee exists to oversee the IT function and its activities.
4. The IT organization ensures that IT plans are communicated to business process owners and other relevant parties across the organization.
5. IT management communicates its activities, challenges, and risks on a regular basis with the CEO and CFO.
6. The IT organization monitors its progress against the strategic plan and reacts accordingly to meet established objectives.
7. 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.
8. IT management has defined information classification standards in accordance with corporate security and privacy policies.

**48 Chapter 2 • SOX and COBIT Defined**

9. IT management has defined, implemented, and maintained security levels for each data classification. These security levels represent the appropriate (minimum) set of security and control measures of each classification and are reevaluated.
10. IT managers have adequate knowledge and experience to fulfill their responsibilities.

## Acquire and Implement

1. The organization has an acquisition and planning process that aligns with its overall strategic direction.
2. The organization acquires software in accordance with its acquisition and planning process.
3. Procedures exist to ensure that system software is installed and maintained in accordance with the organization's requirements.
4. Procedures exist to ensure that system software changes are controlled in line with the organization's change management procedures.
5. IT management ensures that the setup and implementation of system software do not jeopardize the security of the data and programs stored on the system.
6. 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.
7. Procedures exist and are followed to ensure that infrastructure system changes are controlled in line with the organization's change management procedures.

## Delivery and Support

1. Selection of vendors for outsourced services is performed in accordance with the organization's vendor management policy.
2. A framework is defined to establish key performance indicators to manage SLAs, both internally and externally.

3. IT management ensures that, before selection, potential third parties are properly qualified through an assessment of their ability to deliver the required service and their financial viability.
4. Third-party service contracts address the risks, security controls, and procedures for information systems and networks in the contract between the parties.
5. 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.
6. A designated individual is responsible for regular monitoring and reporting on the achievement of the third-party service level performance criteria.
7. A regular review of security, availability, and processing integrity is performed for SLAs and related contracts with third-party service providers.
8. IT management monitors the performance and capacity levels of the systems.

## Monitor and Evaluate

1. Performance indicators (e.g., benchmarks) from both internal and external sources are defined, and data are collected and reported regarding achievement of these benchmarks.
2. IT management monitors its delivery of services to identify shortfalls and responds with actionable plans to improve.
3. IT management monitors the effectiveness of internal controls in the normal course of operations through management and supervisory activities, comparisons, and benchmarks.
4. Serious deviations in the operation of internal control, including major security, availability, and processing integrity events, are reported to senior management.
5. Internal control assessments are performed periodically, using self-assessment or independent audit, to examine whether internal controls are operating satisfactorily.

**50 Chapter 2 • SOX and COBIT Defined**

6. 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).

## Sustainability Is the Key

It is critical that SOX compliance be viewed as an ongoing process rather than a one-time event. In cases where you will need to revise, develop, and implement new procedures and controls, it will be vital to your continuing success that these procedures and controls are sustainable. Rest assured that the auditors will return periodically and will want to review evidence of the effectiveness of your ongoing controls—you must walk the walk.

In instances when you will need to revise, develop, and implement new procedures, keep the following in mind:

- Can the frequency of review be maintained (weekly, monthly, bimonthly quarterly, yearly, etc.)?
- How much evidence of review will be maintained, and how will it be stored?
- How disruptive will the review process be to daily functions?
- Can review evidence be systemically produced?
- How much of the review process can be automated?

In conclusion, it is possible for an IT organization, even a small one, to use COBIT to attain SOX compliance. However, you will need to customize and scale the COBIT controls to best fit your environment.

**TIP**

Keep Control Objectives as simple as possible and automate wherever possible. Get buy-in for new controls or documented processes from business units as soon as possible. IT staff will initially have to re-enforce new controls or processes with business units to facilitate the necessary behavioral change.

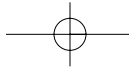
Finance and IT organizations of publicly traded companies should be familiar with audits or the need to have, even undocumented, procedures required to manage key IT processes. However, to comply with SOX, the Finance and IT organizations of publicly traded companies will be required not only to formalize and document these processes but also to increase the number and granularity of their audit concerns.

Again, while Finance and IT organizations of publicly traded companies should be familiar with audits, those audits have traditionally been of a cursory nature and typically only covered the following areas:

- Program change control
- Segregation of duties in Finance and IT
- Lack of user access controls and their periodic review
- Weak password controls
- Shared administration access rights

However, to comply with SOX, Finance and IT organizations of publicly traded companies will find that the areas of the audit process have increased (see the next section), and the nature and the complexity of the audit process have changed. No longer will an informal or even a loosely documented procedure suffice; rather, proof will now be the cornerstone to an organization's passing its SOX compliance. To pass SOX compliance, an IT organization will have to show proof of formal documentation, management buy-off and sign-off, and effectiveness of the implemented controls. These controls include:

- Periodic review of effectiveness of controls
- External security controls
- External security change management controls
- File and folder security
- Control of access to sensitive financial data in nonproduction systems
- Testing the backup and restore process
- Physical access controls
- Rapid response to employee and contractor terminations
- Process for reporting, investigating, and resolving security problems
- Data retention policy



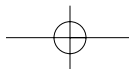
52 Chapter 2 • SOX and COBIT Defined

**TIP**

---

The primary focus of the SOX IT audit will be information security, program change, and data backup and recovery. Where possible, build on what you have, even if the process is not documented or formalized. Processes currently outside the scope of SOX are business continuity planning and operations that do not impact integrity/ access /reporting of financial data.

---



## Summary

In this chapter, we discussed how Congress enacted the Sarbanes-Oxley Act of 2002 in an effort to prevent financial scandals such as those that occurred at Enron and MCI. We also discussed how although Congress had the best of intentions when they enacted the Sarbanes-Oxley Act of 2002; there are some fundamental issues with how the Act was drafted:

- No IT-specific wording for IT compliance
- Section 404 and 302 appear to overlap
- De facto standard for SOX (COBIT) does not scale based on a company's size

Based on the aforementioned issues, we established that small to medium-sized companies will face unique challenges in their effort to pursue compliance of Sarbanes-Oxley Act of 2002. Given the unique challenges with which small to medium-sized companies will have to contend, their ability to leverage SOX and position it with executive management will be critical to their success.

We continued by delving into how the Sarbanes-Oxley Act of 2002 and COBIT came to be synonymous, and how different standards exist, but COBIT has been most widely adopted by audit firms. From there, we learned the six components of COBIT and the four COBIT domains. We continued by drilling further down by defining an Entity Level, a Control Objective, and the difference between the two. Building on the section on COBIT, we established that while the COBIT guidelines are good, standard operating procedures (SOPs) for an IT organization, it is impractical for any company to implement all of the COBIT guidelines as written. From there, we developed a fictitious company to demonstrate how, with planning and knowledge of an environment, the COBIT guidelines could be culled into something more doable and manageable.

## Solutions Fast Track

### SOX Overview

- The Sarbanes-Oxley Act of 2002 affects how public companies report financials and significantly impacts IT.

**54 Chapter 2 • SOX and COBIT Defined**

- ☑ Sarbanes-Oxley compliance requires more than documentation and/or establishment of financial controls; it also requires the assessment of a company's IT infrastructure, operations, and personnel.
- ☑ Requirements of the Sarbanes-Oxley Act of 2002 do not scale based on the size or revenue of a company.
- ☑ Small to medium-sized companies (IT department) will face unique challenges, both budgetary and with personnel, in their effort to comply with the Sarbanes-Oxley Act of 2002.
- ☑ A vast majority of companies will view SOX compliance as a Finance initiative and may not involve IT, or limit IT's involvement to the project's periphery.
- ☑ Limited perception of SOX compliance may make it difficult for CFOs, CIOs, and IT Directors to position SOC compliance with executive management.
- ☑ The SOX compliance process will provide CFOs, CIOs, and IT Directors the opportunity to forge stronger alliances with the business units.

## Why IT COBIT?

- ☑ There is no specific mention in Section 404 as to what IT needs to do to comply with Sarbanes-Oxley.
- ☑ A company can use various predefined standards for defining and documenting their internal controls—ITIL (IT Infrastructure Library), Six Sigma, COBIT—or develop their own.
- ☑ The adoption of the COBIT guidelines and practices as a de facto standard is likely because they are platform independent.
- ☑ There are approximately 300 generic COBIT objectives, grouped under six COBIT Components.
- ☑ Entity Level Control consists of the policies, procedures, practices, and organizational structures.
- ☑ Control Objective is a statement of the desired result or purpose to be achieved.
- ☑ The control is effective in preventing, detecting, or correcting risk.

- ☑ The operating effectiveness of the control activity is adequately evaluated on a regular basis.
- ☑ The standards and assertions required to execute the control are clearly understood.
- ☑ Deficiencies are identified and remedied in a timely manner.
- ☑ The performance of the control can be documented.
- ☑ The controls, policies, and procedures are documented.
- ☑ COBIT is comprised of four Domains:
  - ☑ Planning and organization
  - ☑ Acquisition and implementation
  - ☑ Delivery and support
  - ☑ Monitoring

## Are the Developers of COBIT Controls Crazy? Is This Practical?

- ☑ COBIT controls may appear to any CEO, CFO, or IT Director a daunting task, and that the developers of the controls must be crazy.
- ☑ Whether the task of implementing COBIT controls is daunting will depend on how much effort is put into filtering the COBIT controls.
- ☑ The largest and best run organization would not be able to implement all the controls as defined by COBIT.
- ☑ The keys to culling down COBIT controls center on a couple of questions:
  - Which controls are appropriate to your environment?
  - Of the appropriate controls, which will maximize your efforts?

## Sustainability Is the Key

- ☑ It is critical that SOX compliance be viewed as an on-going process, rather than a one-time event.
- ☑ Auditors will return periodically and will want to review evidence of the effectiveness of your on-going controls—you must walk the walk.
- ☑ Where you will need to revise, develop, and implement new procedures, keep the following in mind:
  - ☑ Can the frequency of review be maintained (weekly, monthly, bimonthly quarterly, yearly, and so on)?
  - ☑ How much evidence of review will be maintained, and how will it be stored?
  - ☑ How disruptive will the review process be to daily functions?
  - ☑ Can review evidence be systemically produced?
  - ☑ How much of the review process can be automated?

## Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to [www.syngress.com/solutions](http://www.syngress.com/solutions) and click on the “Ask the Author” form. You will also gain access to thousands of other FAQs at ITFAQnet.com.

**Q:** Where can I find additional information on COBIT?

**A:** There is a vast amount of information on the Internet about COBIT. We recommend the following sites as a good place to start:

- **Information Systems Audit and Control Association** [www.isaca.org](http://www.isaca.org)
- **IT Governance Institute** [www.itgi.org/](http://www.itgi.org/)

**Q:** Is it necessary that I use the COBIT guidelines?

**A:** No. You can follow any predefined standard, or even use your own. However, bear in mind that choosing to use a standard with which your audit company is unfamiliar will extend your compliance process and jeopardize failing compliance.

**Q:** Can I implement all the COBIT guidelines?

**A:** Yes, if you have an unlimited budget and unlimited resources.

**Q:** Can SOX compliance be achieved without any automation?

**A:** Yes, but since auditors generally prefer evidence of a control to be system generated, you might find it extremely difficult.

