

Sarbanes-Oxley Compliance: Managing Technology Controls

WATCHIT PROGRAMS

WatchIT delivers experience to the desktop.

Our programs feature industry executives and experts who share insight and understanding on the latest technology issues, real-world solutions, and their business impact.

Knowledge, advice, best practices: you get all this and more from WatchIT.

This program's Track: Game Plan

INTRODUCTION

The Sarbanes-Oxley Act is the single most important piece of legislation affecting public corporations since the U.S. securities laws of the early 1930s. Through implementing the rules of the SEC, the act charges managers of public companies with the task of certifying that they have an operational system of internal controls over financial reporting.

Through the creation and issuance of standards by the Public Company Accounting Oversight Board, registered public accountants will have to audit their control environment to attest to management's assertions that they have an operational system of controls. Significant deficiencies found will be reported to the audit committee, and material weaknesses will result in an adverse opinion, even if management remedies the weakness.

To this end, IT executives need to understand internal control theory and ensure that they have taken the necessary steps to comply with the act. Companies with a market capitalization of greater than \$75 million have until August 15th of 2004 to comply. Small and mid-cap companies have until June 15, 2005.

Every IT manager must understand what they need to do to comply with the internal control requirements of the act. This includes planning for the attestation by the public accountants, and ensuring that controls continue to operate after they leave. This program is designed to do just that.

Welcome to the WatchIT Game Plan program, Sarbanes-Oxley Compliance: Managing Technology Controls. I'm Scott Green, global head of Audit and Compliance at Weil, Gotshal & Manges, a law firm with 17 offices in nine countries and a leader in the practice of corporate governance.

I am also the author of the best-selling Manager's Guide to the Sarbanes-Oxley Act: Improving Internal Controls to Prevent Fraud.

After passage of the Sarbanes-Oxley Act, I recognized that it would require all managers to document, assess and monitor their control environment, yet few managers have ever been trained to perform a control assessment.

My book is designed to present control concepts in a jargon-free manner and back them up with real life examples of fraud to provide clarity, context and understanding. The book is a helpful companion to the technical content of this program, as many examples are ripped from the headlines of our nation's media, and are stories with which we are all familiar.

I also teach Finance and Banking at Hofstra University's Zarb School of Business. As a well-known lecturer and author on the subjects of management controls and fraud, I have written many technical articles and consulted for a number of major companies throughout the years. I hope to bring that knowledge to you today.

In viewing this presentation and utilizing supporting resources and materials, you will learn:

- ~ Why understanding the Sarbanes-Oxley Act is critical to your organization;
- ~ How it impacts information technology departments;
- ~ How to comply with provisions of the act; and
- ~ What you need to do to prepare for a review from your registered public accountants.

Your investment in this training will help ensure that your department:

- ~ Meets the requirements of the act; and
- ~ Contributes to an overall unqualified opinion from your external auditors.

AGENDA

Our agenda will discuss the following topics:

- ~ The Sarbanes-Oxley Act: an overview;
- ~ The COBIT roadmap and its nine separate phases for compliance;
- ~ The benefits, pitfalls and impact of the compliance process; and
- ~ A brief conclusion.

VALUE-ADDED RESOURCES INCLUDED WITH THIS PROGRAM

If you are viewing this program via the Internet or on a CD-ROM, you'll have access to:

~ The program transcript;

~ Links to related Web sites, books, articles, and relevant vendor information.

THE SARBANES-OXLEY ACT: AN OVERVIEW

In this first section, we'll present an overview of the Sarbanes-Oxley Act.

WorldCom, Enron, Adelphia, Global Crossing and the list of public companies that failed in 2001 and 2002 goes on and on. The failure of these companies shook the very foundation of investor confidence in our public markets.

Congress passed the Sarbanes-Oxley Act of 2002 with the goal of rebuilding investor confidence and protecting capital markets. They recognized that requiring strong internal controls was an important component of this confidence building.

Section 404 of the act addresses this component by mandating an annual evaluation of internal controls and procedures for financial reporting and by requiring management to assess and certify the effectiveness of these controls. It also requires a company's external auditor to complete a separate report that attests to management's assessment of the effectiveness of internal controls and procedures for financial reporting.

In short, the external auditor must perform testing to validate management's assessment of the internal control structure. If a material weakness is found by the auditors, new guidance requires that the auditor issue an adverse opinion. So our objective is to ensure that we have a strong system of internal control that we can demonstrate to our auditors.

To properly analyze our system of internal control, the adoption of a framework to guide us through all of the necessary analytical steps is paramount. The SEC has required that a system of internal controls must conform to a recognized and accepted framework. And it has specifically cited the Committee of Sponsoring Organizations of the Treadway Commission (or COSO) framework as meeting their criteria.

Because of this endorsement, many organizations will use COSO to perform their company-wide evaluation. This framework is now widely accepted as the standard by which all control systems are measured. It consists of components that comprise the overall system of controls, which apply to the entity as a whole.

THE COBIT ROADMAP

In this section, we'll explore the COBIT roadmap and its nine separate steps for compliance.

Since most IT managers are not trained in the art of internal control, they need more examples and detailed guidance to help identify, document and evaluate controls than COSO provides. To address this, the IT Governance Institute created Control Objectives for Information and Related Technology, or COBIT.

COBIT is an IT governance framework that provides both entity level and activity level objectives. It maps to the COSO framework and, therefore, is used by many IT professionals to evaluate their systems of internal controls. Today, we will rely on the proven COBIT roadmap for compliance, which consists of nine separate phases:

- ~ Planning;
- ~ Risk assessment;
- ~ Identifying significant accounts and controls;
- ~ Documenting control design;
- ~ Evaluating control design;
- ~ Evaluating operational effectiveness;
- ~ Determining material weaknesses;
- ~ Documenting results; and
- ~ Building sustainability.

Each of these detailed phases conforms to the COSO framework, but in terms that are more relevant to IT managers.

The COBIT Roadmap – Phase 1: Planning

Let's start with planning. While scoping the project may seem simple at first, this is actually one of the most difficult stages. General IT controls cut across geographic and business processes, yet not all processes are relevant.

At this stage, an understanding of how the financial reporting process works is critical. This understanding will help identify those key systems and subsystems that need to be evaluated.

Any systems that initiate, record, process or report financial information should be included within the scope of the project. For example:

- ~ Payroll systems feed compensation and tax information to the financial statements.
- ~ Shipping systems identify important cut-off points for revenue recognition purposes.
- ~ Asset registers feed the balance sheet.
- ~ Payment systems feed expense data.

All of these systems, not just general ledger systems or consolidation packages, need to be included in the review.

As a starting point, take your systems inventory and identify which contribute to financial reporting processes. This can be done by identifying significant financial accounts, and working backwards to the systems that feed these accounts.

It is likely that significant accounts have already been identified by a SarbOx compliance team or the finance department. Add to your list any other systems that help management monitor their risk or otherwise contribute to financial statement disclosures.

The COBIT Roadmap – Phase 2: Risk Assessment

Once we have identified our population of systems, we need to perform a risk assessment. Risk assessment requires that we determine both the likelihood and impact of potential adverse events. For each system in our scope, we will first assess whether the potential for a control failure is more than remote, and second, the impact to the organization if a control break actually occurs.

Examples of risks that could adversely impact financial reporting include events that:

- ~ Impact the availability, timeliness, quality, confidentiality or integrity of information;
- ~ Bypass or override automated authorization controls;
- ~ Bypass or exploit access rights to IT systems and related applications; or
- ~ Impair recovery controls that support business continuity.

Organizations with multiple locations also must assess risk associated with these various processing locations. When evaluating a location, one must consider:

- ~ How dependent is the location on IT?
- ~ How does the organization view the risk associated with this location? and
- ~ How harmonized are the systems and processes? Unique systems increase the risk that control objectives may not be met.

Once we have performed our risk assessment, we can prioritize our systems and locations for review. We are then ready to identify significant accounts and controls.

The COBIT Roadmap – Phase 3: Identify Significant Accounts and Controls

There are generally two categories of information system control activities recognized by both COSO and COBIT:

~ There are general controls that apply to all information systems and support the secure and continuous operation of the entire entity; and

~ Application controls which are designed to prevent or detect unauthorized transactions.

Entity level, or general controls, primarily relate to the overall control environment and risk assessment. They set the tone for the effectiveness of all other controls.

Those that support the quality and integrity of information and mitigate risks will require assessment. This is because auditors pay particular attention to general controls due to their importance in the overall system of control. Therefore, external auditors will judge such subjective measures as:

~ Tone from the top IT management;

~ Integrity, ethical values and competence of management;

~ Management's philosophy and operating style;

~ Delegation of authority and responsibility;

~ IT policies and procedures;

~ The quality and skill of employees; and

~ Oversight provided by management.

COBIT Control Objectives: Five Domains

There are a number of specific COBIT control objectives that you can utilize to perform a self-assessment of your general controls. These general control objectives are sorted into five domains, and these domains are:

~ Plan;

~ Acquire and maintain;

~ Deliver and support;

- ~ Monitor and evaluate; and finally
- ~ An evaluation of your application controls.

Let's look at each of these domains in further detail so that we understand what we will need to do to address their related objectives.

COBIT Control Domains: Plan

The planning domain addresses such organizational items as:

- ~ Developing the strategic plan;
- ~ Defining the information architecture;
- ~ Defining the IT organization;
- ~ Communicating plans;
- ~ Managing human resources;
- ~ Ensuring compliance with external requirements;
- ~ Assessing risk; and
- ~ Managing quality.

Auditors will look for documentation and other evidence that adequate planning occurs in the IT department.

If you have not already done so, prepare a strategic plan that aligns business objectives and IT strategies as well as identifies what IT must do to support the business. Auditors will not only read your plans, but will assess whether the plans have been adequately communicated to other stakeholders in the organization.

When reviewing the information architecture, the auditors will also look for evidence that the organization makes certain that information will be captured and communicated timely and in good form.

They will evaluate if controls for the completeness, accuracy, validity and authorization of information have been defined, and information classified in accordance with security and privacy policies.

Management will prepare definitions for information capture, processing and reporting controls which include completeness, accuracy, validity and authorization objectives.

The auditors will then evaluate how well management has defined, implemented and maintained security levels for different data classifications.

When defining the IT organization and relationships, ensure that there are clear organizational responsibilities, job descriptions and control over IT assets. Auditors will evaluate if IT personnel have sufficient experience and authority to execute their assigned responsibilities. Be prepared to produce:

- ~ Organizational charts;
- ~ Job descriptions; and
- ~ Evidence that employees have key competencies to do their jobs.

In order to communicate management plans, make certain that policies and procedures are present detailing how IT operations will be governed. Auditors will ensure that there is a process in place to regularly update policies and procedures, as well as determine if there is an effective process in place to investigate and address a breach of policy.

The IT organization must also manage human resources so that there is sufficient cross-training or other controls to respond to job changes and terminations without impairment to the control environment. A position depth chart can be a particularly effective method for demonstrating the ability to respond to resource events. Develop a response to the question of succession and cross-training.

Also, when ensuring compliance with the external requirements objective, your department must also have an effective process for monitoring changes to the regulatory environment and ongoing compliance with the Sarbanes-Oxley Act. Make sure that your policies and procedures reflect how you continue to monitor your control environment.

Prepare to share both entity and activity level risk assessment frameworks used in the IT organization. This will be easy if you are following the COBIT framework.

Auditors will evaluate if the risk assessment is effective by reviewing:

- ~ Assessment elements;
- ~ The qualitative and quantitative outputs; and
- ~ Resulting implementation of cost-effective controls to mitigate exposure to risks on a continuing basis.

Demonstrate your commitment to quality control. Regularly conduct and document the results of:

- ~ Regular control self-assessments;
- ~ Internal audits; and

~ Quality control procedures.

COBIT Control Domains: Acquire and Maintain

Next we will cover the acquire and implement domain. The acquire and implement domain focuses on the procurement, implementation and maintenance of technology hardware, software and services. These objectives cover:

- ~ The acquisition and maintenance of application software and technology infrastructure;
- ~ Development and maintenance procedures;
- ~ The preparation of change control procedures; and
- ~ Actually managing change.

Proper design, acquisition and deployment of application software ensure alignment with business objectives. Design interfaces with other software are a critical activity that, done poorly, could compromise the complete and accurate reporting of financial information.

Auditors will review the system development life cycle methodology to determine that it effectively results in secure applications that provide processing integrity. Be prepared to provide this methodology as well as evidence that it is used effectively.

Additionally, when acquiring and maintaining technology infrastructure, procedures should be implemented in such a way that the design, acquisition, building and deployment of technology systems properly supports applications and communications.

Auditors will look at the security of the data and the stability of the system architecture. Be prepared to provide metrics that indicate system stability and otherwise demonstrate how you are able to keep data secure.

To develop and maintain procedures, produce – for every part of information system development or modification – a user reference and support manual. Auditors will likely review this documentation for key systems.

Also, develop detailed change control procedures. Good CIOs make certain that new systems are not moved into production unless appropriately tested, accredited and approved.

Every step in this process should be documented with the expectation that the external auditors will review the documentation. This is a key area assured to get their attention. They will expect that there are separate servers for testing programs and a methodology for moving new code into production. Be prepared to prove to them that this is indeed occurring.

Finally, there must be procedures to document, prioritize and execute requests for managing change. Systems and emergency maintenance should also be documented and available to meet this objective. Produce evidence that these processes are operational.

COBIT Control Domains: Deliver and Support

The next domain covers delivery and support services. The deliver and support domain consists of providing secure, continuous, accurate, uninterrupted technology service to the organization. The objectives in this domain include:

- ~ Define and manage service levels;
- ~ Manage third party service levels;
- ~ Ensure continuous service;
- ~ Ensure system security;
- ~ Educate and train users; and
- ~ Manage configuration, problems and incidents, data, facilities, and operations.

In short, this domain contains a lot of the day-to-day duties that many of us take for granted. In the new Sarbanes-Oxley world, however, it is not enough that we execute our duties, we need to have the supporting evidence to demonstrate our competence.

You can do this by defining and managing service levels. Well-managed IT departments develop key performance indicators that reflect the quality of technology service delivery as a procedure performed in the normal course of business. Regular reporting of these indicators is evidence that management monitors service levels. Have your KPI (key performance indicator) reports ready.

Also, manage the third party service level. It is becoming more and more common for IT departments to outsource certain services to third party vendors. It is important that you are able to demonstrate proper oversight of these vendors.

By documenting the qualification of vendors and monitoring their activities against predetermined standards, management will be able to prove oversight of vendors. Maintain documentation regarding the selection criteria of vendors and how they are evaluated, in addition to any actual evaluations performed.

Managing peak performance and growth capacity is an important deliver and support objective. Throughput thresholds should be periodically tested and bottlenecks identified. Produce documentation of the testing results and remediation plans where recording growth or peak activity could be constrained by systems.

Proper business continuity and disaster recovery planning ensures continuous service. Auditors will evaluate whether the plan is current and includes all:

- ~ Critical applications;
- ~ Third party services;
- ~ Operating systems;
- ~ Personnel; and
- ~ Supplies.

They will also want to ensure that off-site recovery facilities have been successfully tested within the past year. Have the documented planning, execution and results of such testing on hand.

Demonstrate that your systems are secure. This is done by implementing both physical and logical controls that prevent unauthorized access.

Produce procedures for the granting of access rights to systems. Also prove that granted rights are periodically reviewed to make sure that there are no conflicts or that changes in job responsibilities have not negated the business purpose for certain rights.

Be in a position to prove that:

- ~ Firewalls;
- ~ Intrusion detection; and
- ~ Vulnerability assessments

... are available where appropriate. Public accountants will evaluate these items and ensure that security is actively monitored.

Management should also be able to demonstrate that they adequately educate and train users by providing continuous education that includes:

- ~ Ethics;
- ~ System security;
- ~ Confidentiality; and
- ~ Integrity standards.

You can produce a training syllabus with corresponding attendance records to display your commitment to education.

Auditors will also assure themselves that the enterprise can meet the managing configuration objective of this domain. They will ensure that:

- ~ Rogue software is not introduced into the environment;
- ~ System infrastructure – such as switches, routers, firewalls, network operating systems, servers or other related devices – are configured to prevent unauthorized access; and
- ~ Virus prevention procedures exist throughout the enterprise.

Organize your:

- ~ Policy-based management tools;
 - ~ Policies and procedures;
 - ~ Management reports; and
 - ~ Other evidence you can provide
- ... to support this request.

There should also be documented procedures for managing problems and incidents that fall outside of normal operations. If installed and operational, help desk software will help provide incident reports and related activity to clear this objective; otherwise, manual logs may suffice. Make sure that your escalation procedures are defined and operational.

Auditors will also search for evidence that the IT organization meets the manage data objective of the deliver and support domain. The manage data objective includes the controls and procedures used to support information integrity, including its completeness, accuracy, authorization and validity.

Such techniques as:

- ~ Processing totals;
- ~ Edit checks;
- ~ Bound checks;
- ~ System-to-system reconciliations;
- ~ Physical data inventory procedures; and so on

... are utilized to meet this objective.

For each process, log or otherwise highlight these areas for the auditors so that they do not have to search for them.

Also, when managing facilities, be prepared to show how the organization physically restricts access to all but authorized personnel and provides environmental controls.

Electronic keys are a terrific preventative control that normally can yield reports that display employee access levels and entry denials. Such reports can be used to prove that access restrictions are functional. Auditors will also assess data center environmental factors such as:

- ~ Fire suppression;
- ~ Uninterrupted power supply;
- ~ Air-conditioning; and
- ~ Elevated floors.

Finally, auditors will look for evidence that operations are properly managed. This objective is met by:

- ~ Monitoring key performance indicators;
- ~ Managing shift changes; and
- ~ Ensuring the documentation of standard procedures for IT operations.

COBIT Control Domains: Monitor and Evaluate

The fourth general control domain, monitor and evaluate, consists of objectives that, as the name suggests, help the organization continuously assess their system of controls and notifies management of any degradation in the effectiveness of the system.

The first objective of this domain is simply to monitor. This can be done by comparing key performance indicators to benchmarks gleaned from both internal and external sources.

The second is to assess internal control – through both control self-assessment procedures as well as independent audits. Gather evidence that deviations found from these procedures are reported to senior management and corrected.

Finally, the third objective is to obtain independent assurance through independent system and internal control reviews. Independent evaluation eliminates any intentional or unintentional bias and may result in better practices.

COBIT Control Domains: Evaluation of Application Controls

The last domain addresses application controls. The COBIT framework approaches application controls by business cycle. The sales, purchasing, monetary, inventory, asset management and

human resource cycles are each contemplated separately. But the objectives and questions used to evaluate each cycle are similar.

For each cycle, you can ask these questions to evaluate completeness, accuracy, validity and authorization controls. This is the same approach I take in my book, *Manager's Guide to the Sarbanes-Oxley Act*. For each cycle or process, ask yourself "How do you know?" questions. For instance, how do you know:

- ~ That transactions are properly approved and within authorization limits?
- ~ Are unauthorized transactions rejected?

By answering the question, you have either identified a control or a weakness. Let's ask the other questions that will identify controls and weaknesses.

How do you know:

- ~ That all transactions are captured by the system and recorded in the proper period?
- ~ Is there a method to identify missing transactions?

How do you know that:

- ~ Transactions cannot be erroneously entered twice;
- ~ Information enters the system accurately;
- ~ Information is fed to other systems completely and accurately;
- ~ Automated calculations are performed accurately;
- ~ Value is received for assets given; and
- ~ Database information is current and changes to master files are authorized and performed accurately, completely and timely?

How do you know that:

- ~ Aged receivables are monitored;
- ~ Transactions are classified properly; and
- ~ Recorded amounts accurately reflect physical quantities and values of assets?

How do you know that:

- ~ Impairment to assets are identified and recorded in the proper period;

- ~ Defective assets are identified and rejected or returned to the source;
- ~ Estimates and assumptions used for non-routine transactions are reasonable; and
- ~ Transactions conform to company policy?
- ~ Are there exception reports to identify outliers?

How do you know that:

- ~ No one has attempted to access your applications inappropriately;
- ~ There are no fictitious employees or vendors;
- ~ Time and attendance records are accurate; and
- ~ Goods, services, information and other assets reach their intended destination?

Regardless of business cycle, the answer to each of these questions identifies a control. If one cannot describe “how they know,” then a potential control weakness has been identified that must be addressed.

Both controls and potential weaknesses need to be documented so that they can be reevaluated in relation to the overall control design. To ensure completeness, all significant financial accounts identified by the enterprise should be mapped to each of the business cycles.

As discussed earlier, it is likely that these significant accounts have already been identified by financial personnel or any SarbOx working group. By accounting for all significant accounts and evaluating all business cycles that contribute data, management can gain comfort that the design and operational assessments will be comprehensive.

That concludes the identify significant accounts and controls section of the roadmap.

The COBIT Roadmap – Phase 4: Document Control Design

Now let's discuss the fourth phase: document control design. The Public Company Accounting Oversight Board was established under the Sarbanes-Oxley Act “to oversee the audit of public companies that are subject to the securities laws, and related matters.” In short, they now have regulatory oversight of the accounting profession, where the profession used to be self-regulated, with oversight from the SEC.

The Board has indicated that inadequate documentation, by itself, can be a deficiency in internal control that could rise to the level of a material weakness. Even some of the most control-aware organizations do not have their control structure documented. Under the new rules, this is no longer acceptable.

For many, preparing and evaluating this documentation will be the most expensive SarbOx compliance activity. Many companies have hired teams of consultants and purchased documentation systems to perform this required task.

As we experienced in the Identify Significant Accounts and Controls section of our roadmap, documentation can take many forms, including, but not limited to:

- ~ Policy manuals;
- ~ Process models;
- ~ Flow charts;
- ~ Job descriptions;
- ~ Documents; and
- ~ Forms.

No single form of documentation is required, and the extent of documentation will vary depending upon the size, nature and complexity of the organization.

A cottage industry in documentation applications has also risen to address some of these needs. Some of the tools I am most familiar with include:

- ~ Paisley Consulting's Focus; and
- ~ Protiviti's proprietary software.

However, there are a number of vendor solutions to help coordinate a department's documentation needs. You need not purchase a system; in fact, most companies document their controls manually using spreadsheets and other standard desktop software applications.

Regardless of whether an automated tool is used or not, available documentation should be evaluated, updated and discussed with the external auditors early in the process so that deficiencies can be addressed before a formal evaluation of the control structure is performed. The documentation should support the approach the department takes to reduce the risk that IT prevents the business from achieving its objectives.

At the transaction level, documentation will include how transactions are initiated, recorded, processed, and reported. At a minimum, this documentation will contain:

- ~ A description of the processes and related subprocesses;
- ~ A description of the risk associated with the process or subprocess, which includes an analysis of the impact and probability of occurrence;

- ~ A statement of the control objective designed to reduce the risk of the process or subprocess to an acceptable level;
- ~ A description of the control activities designed and performed to satisfy the control objective;
- ~ A description of the approach followed to test the existence and operational effectiveness of the control activities; and
- ~ Conclusions reached about the effectiveness of the controls, as a result of testing.

The documentation will also reflect all of the relevant processing procedures – whether they are routine or non-routine – as well as the business owner of the system or data.

The COBIT Roadmap – Phase 5: Evaluating Control Design

At this point, the fifth phase in our roadmap, senior management must evaluate the ability of the control program to reduce IT risk to an acceptable level.

Not all controls are created equal. For instance, system-based preventive controls are more effective than detective controls, as they are implemented at the source of the risk, while detective controls reside further downstream and will alert you only after a problem has occurred.

Furthermore, system-based controls are more reliable than manual controls. Additionally, some controls rely on other controls to function effectively. So it is important that, at this stage, the organization steps back and evaluates the reliability of the control system.

If reliability is optimized – in other words, there are effective automated preventative and detective controls throughout a well-documented process, and the health of those controls is monitored by highly aware and knowledgeable personnel – then the organization has met their objective.

If less reliable controls are present, such as manual detective controls, then other methods will need to be designed into the control structure that will provide an added measure of control. For instance, if system-to-system reconciliations are not automated, periodic self control assessment or internal audit of the manual reconciliations should be performed to ensure that degradation of this control has not occurred.

The COBIT Roadmap – Phase 6: Evaluating Operational Effectiveness

Once the control design has been deemed acceptable, the continuing effectiveness of the documented controls must be confirmed. Walkthroughs can be a particularly effective and efficient method to understand and evaluate if procedures are conforming to design. Walkthroughs consist of “walking” a transaction through the process, from initiation to final reporting in the financial statements, accumulating evidence of operating controls along the way.

Once the process is confirmed as operating as designed:

- ~ Ongoing control self assessments;
- ~ Test counts of physical assets;
- ~ Independent review of system reconciliations; and so on

... will help provide evidence that the controls continue to operate as intended.

At a minimum, external auditors will test the general IT controls of the organization, so testing these controls should always be of the highest priority. Less significant application controls may be tested less frequently, but management should nevertheless ensure that application controls continue to function normally.

The COBIT Roadmap – Phase 7: Determining Material Weaknesses

When the IT team has identified a control deficiency, whether in design or operation, the team will first determine if there are compensating controls that protect the enterprise. If a compensating control exists, the team must then decide if they want to continue to rely on that control, or take remedial action to implement a properly functioning and operational control. If the deficiency precludes reasonable assurance that the financial statements are materially correct, remedial action must be taken as a priority.

The COBIT Roadmap – Phase 8: Documenting Results

During the evaluation phase, results of tests performed need to be documented, as the external auditors will review these results as a part of their assessment of the management's assertions. Ideally, this documentation should culminate in a single report that demonstrates the overall reliability, quality and integrity of IT systems.

The COBIT Roadmap – Phase 9: Building Sustainability

The final phase of the COBIT roadmap is building sustainability. Sustainability can be institutionalized through:

- ~ Repetitive testing at prescribed points in time;
- ~ Regular control self assessments;
- ~ Proper change control processes and oversight;
- ~ The monitoring of key performance indicators which reflect the health of significant control points, and so on.

Sustainability is the same as standard operating procedure. When activities that support the control structure are rote and an everyday occurrence, then you have met this objective.

THE BENEFITS, PITFALLS AND IMPACT OF THE COMPLIANCE PROCESS

In this section, we'll examine the benefits, pitfalls and impact of the compliance process.

There is little doubt that implementing this framework will be a significant project, regardless of the size of the enterprise. Many of the larger companies have combined internal resources and external consultants to form project teams designed to quickly document and assess the system of controls.

The number of hours spent by these companies is staggering. According to Financial Executives International, large companies are reporting spending in excess of 35,000 hours to comply with the internal control requirements of Sarbanes-Oxley.

These are not the only costs. According to the Public Accounting Report, audit fees for large companies have increased 38% on average. This is even before the internal control provisions of the act have taken effect.

However, these costs are not discretionary. Public companies have no choice but to comply. An adverse audit opinion could be devastating to a company.

On the other hand, the benefits to doing this right include:

- ~ Better organizational communication;
- ~ Greater confidence in the system of internal control;
- ~ A bona fide reason to support spending scarce capital on projects that have a strong control component; and
- ~ In the end, job security.

The coming few months will be busy for IT departments as they pull together their SarbOx compliance programs. For those that do not build automated monitoring tools into their programs, ongoing costs will continue to burden their enterprise until these investments are made.

If sufficient investment is made up front to build sustainability into the system of internal controls, many of the hours and dollars invested will be one-time expenditures.

For most companies, SarbOx compliance will become standard operating procedure, embedded and inseparable from normal operating activity. The focus will then return to strategic issues and better ways to make a mousetrap.

CONCLUSION

In this final section, we'll provide some concluding thoughts.

The passage of the Sarbanes-Oxley Act is arguably the most important legislation impacting public corporations since the 1930s. Because the CEO and CFO will be held accountable for their system of internal controls, significant investments have been made by public companies to comply with Section 404 of the Sarbanes-Oxley Act.

Large companies have spent heavily to comply with the act. With such a heavy investment, it is imperative that companies stay on course and achieve the needed result.

The material presented today can be used as a checklist to ensure that all deliverables are contemplated. If I can leave you with some parting words of advice, it is to:

- ~ Start early;
- ~ Plan for contingencies; and
- ~ Prepare for your auditors.

Compliance with SarbOx will likely take more time than is evident on day one of the project. Unplanned issues will arise and certain tasks will take longer than estimated. Additionally, by being prepared for your auditors, you start off on the right foot by demonstrating knowledge and command of your control environment.

FOR ADDITIONAL INFORMATION

If you have been viewing this program via the Internet or on CD-ROM, please click on the Resources tab for additional information on this topic.

Thanks for viewing the WatchIT Game Plan program: Sarbanes-Oxley Compliance: Managing Technology Controls. I'm Scott Green. If you have any questions or comments, please e-mail us at: experts@watchit.com.

LEGAL INFORMATION

All trademarks or registered trademarks are the properties of their respective owners.

WatchIT.com™ does not endorse and is not affiliated with any of the vendors referenced in its products or on its Web site

By providing links to other sites, WatchIT.com™ does not guarantee, approve or endorse the information or products available at these sites, nor does a link indicate any association with or endorsement by the linked site to WatchIT.com™.

Unauthorized reproduction of this program or its supporting material is forbidden without the express written permission of WatchIT.com™ and constitutes a violation of Title 17, US Code, Sections 501 and 506.

For additional information, see (if available):

~ CD Help page "readme.txt File"

~ CD Help page "Legal Information"

~ Legal information at the WIT Web site: <http://www.watchit.com/copyright.cfm>