Comprehensive Consulting Solutions, Inc. – "Business Savvy. IT Smart."®

SOX 404 Internal Controls: How much is enough?

White Paper

Published: September 2005 (with revisions)

Section 404 of Sarbanes-Oxley is effectively the *Forced Implementation of Best Practices*.

Contents

Preface

So, your company is publicly traded or is planning on going public. You have been told to implement Internal Controls to satisfy the requirements of Sarbanes-Oxley Section 404. Many questions may come to mind, such as:

- **How and where do you start?**
- **How can you do this as quickly, efficiently, and cost effectively as possible?**
- **Is it possible to take the easy way out and just purchase a tool to monitor data access?**
- **How can you ensure that this is done right the first time?**
- **How much is enough?**

This White Paper aims to provide helpful guidance and insight into one approach for creating Internal Controls. It is not all-inclusive, but it will help when embarking on this type of effort. Combined with the referenced sources of information it will provide an understanding of what is involved with a project of this nature.

Overview

By now most people have heard about Sarbanes-Oxley (see http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf for the full text of the Sarbanes-Oxley Act) and the impact that it is having on business. The Act was driven by large corporate scandals in the United States (Enron, Tyco, Worldcom, and others) around the time of the Internet Boom, circa 2000. These events resulted in financial loss for employees and investors of these and other companies, mistrust of financial reporting, and general concern regarding the overall impact to the stock market and the economy.

Legislation was created to address these accounting deficiencies and hold key employees - specifically the Chief Executive Officer (CEO) and Chief Financial Officer (CFO) - criminally and civilly accountable for the financial reports of their company. Controls and Audits are the primary means of implementation of the Act.

Section 404 of the Sarbanes-Oxley Act (commonly referred to as "SOX") refers to the "Management assessment of internal controls." This is interpreted by the U.S. Securities and Exchange Commission (SEC) to mean "controls that pertain to the preparation of financial statements for external purposes that are fairly presented in conformity with generally accepted accounting principles as addressed by the Codification of Statements on Auditing Standards §319 or any superseding definition or other literature that is issued or adopted by the Public Company Accounting Oversight Board." (http://www.sec.gov/rules/final/33-8238.htm) **But what does this mean from a practical perspective?**

In practice it will be dependent on the External Auditor (CPA firm contracted by a company) to define what aspects of the overall operations that they feel are *material*, and then to what degree. This will be based on multiple criteria, including their own control objectives. Some identified systems will be deemed critical while others may be deemed supporting. In general the External Auditor can provide guidelines as to their control objectives, but since they are not allowed to audit their own work they will probably not provide much more than that. Your Internal Auditor (employee within your company) must therefore determine the scope of the effort for your particular company. This is really a business perspective of what is important, how important, and what level of risk is acceptable.

Goals of the Act relative to Information Technology

If SOX concerns financial reforms, then what does that have to do with Information Technology (IT)? The obvious answer is that Accounting Systems would be considered "material." That is, a system or process that has real consequences or is of great importance to financial reporting. Even within those systems there can be varying levels of importance based on their overall impact.

But it extends far beyond that in ways that are not always obvious. For example, what about controls over who has access to production data? And how about change control processes for systems and data? Many things previously done informally may now need to follow a defined process. And the basics, such as *segregation of duties*, are now more important than ever.

What about Business Continuity Planning (BCP) / Disaster Recovery Planning (DRP) – sometimes placed under the umbrella of Business Continuity Management (BCM). While BCM is not specifically mentioned in SOX, Section 406(c)(2) requires "full, fair, accurate, ***timely*** [emphasis added], and understandable disclosure in the periodic reports to be filed by the issuer." So while this may only be a supporting objective, it is almost implied as a requirement.

> **"Although the words 'disaster recovery' or 'BCP' are not found specifically in SOA legislation [SOX], the astute board audit committee or chief financial officer (CFO) should realize that an organization must have an effective BCP in place and working in order to attest that internal controls are effective as required by Section 404 of SOA [SOX]." (Robert R. Moeller, Sarbanes-Oxley and the New Internal Auditing Rules, Wiley, 2004)**

As you can see there are some aspects of IT that might not appear relevant at first glance but may indeed be required in order to attest to having adequate controls. The prospect of implementing adequate internal controls in order to comply with SOX 404 can be daunting, but when done properly will provide the appropriate level of control and documentation in a way that is flexible, extensible, and easy to maintain.

Here is a big clue as to what is required for SOX 404 compliance. The U.S. Securities and Exchange Commission has published a Final Rule on Internal Controls (http://www.sec.gov/rules/final/33-8238.htm). Among other things it specifically identified The COSO (The Committee of Sponsoring Organizations of the Treadway Commission) Internal Control – Integrated Framework. Among other things it provides criteria that a company can use to assess their internal controls.

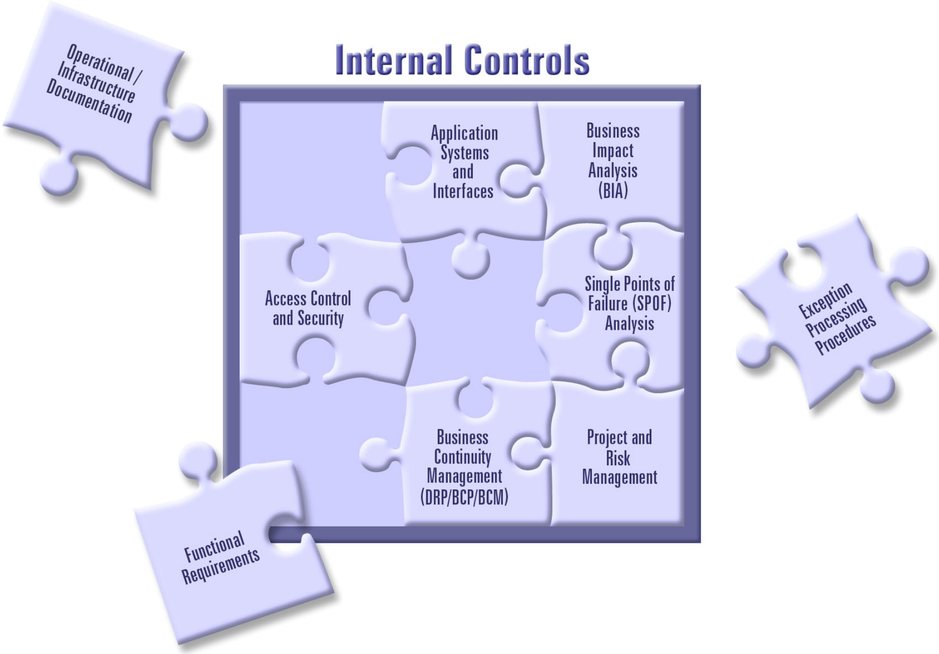
It is also important to understand that Internal Controls are an *ongoing process* - the means to an end and not the end itself at some point in time. Internal Controls provide *reasonable assurance* and not *absolute assurance*. Internal Controls are enacted by people, and are not merely policy manuals and forms. (http://www.coso.org/key.htm) These key concepts are helpful guides for this process.

The COBIT Framework (Control Objectives for Information Technology) from the Information Systems Audit and Control Association (http://www.isaca.org/) is presented from an IT perspective (as opposed to a financial perspective). This framework defines Control Objectives well, breaking them down in a logical, systematic progression. This is the format I personally use when creating internal controls procedures and documentation.

Best Practices – Pieces of the Puzzle

The beauty of this entire effort is that nothing is really new. It is a matter of identifying the key pieces of the puzzle and assembling them in a way that creates the *picture* of control that auditors are looking for. Does this mean that you only need to create the *illusion* of control? Absolutely not! Rather, it means that instead of 'reinventing the wheel' it is possible to start with an understanding of what the auditors will focus on and then work on providing deliverables that meet those expectations. The use of best practices in these key areas will not only help an organization complete this effort efficiently, but will hopefully satisfy the external auditors as well. Always remember that this works best when "driven" by the business, and not by IT.

So, what are the pieces?


Internal Controls
Operational / Infrastructure Documentation
Application Systems and Interfaces
Business Impact Analysis (BIA)
Access Control and Security
Single Points of Failure (SPOF) Analysis
Exception Processing Procedures
Business Continuity Management (DRP/BCP/BCM)
Project and Risk Management
Functional Requirements

Operational & Infrastructure "Systems" Documentation

It is important to understand what "systems" are in use, where they are, and what their purpose is. This includes packaged and customized software, as well as hardware such as the platforms that support the business software, the network, and may include infrastructure information required for business continuity.

When looking at the systems it is important to have answers to the following types of questions:

- What are the dependencies on the various components?
- Who uses them, when, and why? Does this system in any way impact financial reporting? If yes, to what extent?
- Where does the equipment physically reside and who has physical access to these systems?
- Who is responsible for each component of each system?
- Are the environment conditions adequate for the system?

As you can see, this type of documentation provides you with what can be thought of as a *manifest* of hardware and software systems in your environment. This list will also help facilitate the necessary testing of internal controls whenever there are upgrades or new systems (again, hardware and/or software) are implemented.

Application System & Interface Documentation

This step uses as its driver the "systems manifest" that was produced in the previous step. In this step you are determining "what" happens with the data in each system. The following types of questions need to be answered:

- What type of data is stored, processed, or otherwise manipulated by the system in question?
- What are the relationships (if any) between this system and the other systems that have been identified?
- What is the impact of a problem or failure with this system, including possible impact to other systems?
- Is there informal or Ad Hoc access to this system? For example, JDBC/ODBC access from third party tools such as Microsoft Access.

The documentation from this step and from the previous is key to this effort. It will help determine your exposure to risk for the various systems. This information will be used in conjunction with the information from the following steps in order to provide focus to your efforts.

As you are beginning to see, this approach is really a series of interwoven processes – all best practices.

Functional Requirements of Key / Material Systems

What are these systems really supposed to do? Do they meet their objectives? Are they doing more than that? Are you able to map a process group like "Sales Systems" to the various components? Is this a clean mapping or is there ambiguity and/or overlap? Ambiguity can indicate the need for further analysis and validation, while overlap can indicate areas of unnecessary risk. This step provides the top-down view of your systems.

While not part of a SOX effort [see comment on next page], this is a good point to look at Service Level Agreements (SLAs):

- Do you have formally defined SLAs?
- What do they address? Availability and average response time are two common key metrics.
- Are the SLAs reasonable?
- Are they achievable given the current environment?
- Have the SLAs historically been met? If not, why?

Unplanned service outages or poor system response time can lead to the circumvention of standard, approved processes and procedures. Therefore these conditions create conditions for violation of internal controls, which is just another reason why it is important to have an understanding of these types of metrics and agreements.

SLA Comment: For SOX purposes, the assumption is that generic application performance, or controls as implemented, does not create control deficiencies. I've personally heard performance and turn-around time used as excuses for avoiding specific controls. By defining SLAs required from a business perspective and comparing those with actual performance (and ideally gathering metrics for analysis of trends) – tasks that are easier accomplished when conducting detailed analysis, it is possible to avoid those arguments in the future. And as the paper points out, this can identify problems that can lead to people circumventing controls in order to "get the work done."

Regarding the IT Governance Institute's "IT Controls Objectives for Sarbanes-Oxley, 2nd Edition" (http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentFileID=1238), as several readers have done, the service levels that they mention (Figure 20 on page 68, and Figure 21 on page 69) and allude to what I mention above. But, when you look at their Risk Assessment Grid (page 101) you will see this area is listed as discretionary, but not absolutely recommended. My interpretation of this is that it is a recommended best practice (which I fully agree with), but not an absolute necessity. Either way, it is not absolutely required from a pure SOX perspective – unless your External Auditor decides otherwise.

Business Impact Analysis (BIA)

At this point you will have an understanding of your environment that is supported by documentation. Now you need to tie all of the information together and determine the impact of each component relative to specific functional requirements, business goals, and internal controls.

- What is the impact of each system? For example, if the Sales system is unavailable what happens when a customer calls to place an order?
- What are the dependencies among the various systems? When data is exchanged between systems, what is done to prevent the loss of accuracy, precision, and integrity of that data?
- Do these systems have a direct or indirect relationship to financial reporting?
- Could any remote system or interface potentially provide update access to another system or its data?
- Who uses these systems?
- What level of access is required?
- What level of transactional auditing is available?
- Are there manual processes or procedures that could be potentially detrimental?

This purpose of this step is to provide a further understanding of the environment, including the relationship to financial system data and the importance of the system itself. At this point you may find systems or processes that have a potential negative business impact, or where the impact is uncertain. These are areas that almost always deserve further analysis.

Access Control & Security Plan

Everyone cannot have access to everything – that is a given. To put controls in place it is important to understand and document how and why access is granted. This can be done in a number of different ways. For example, access can be restricted by individual users, groups or classes of users, specific applications and many other ways. There could be a mix of control in any environment, especially one that is distributed or decentralized.

Another question is to ask is: What level of granularity is access to data restricted? Can restrictions be applied to specific rows? Certain columns of specific rows? Only at the granularity of an entire table? Worse yet, for an entire database or instance? Controls can only be properly applied when they are designed with the traits and limitations of the systems being used in mind.

Often access will be controlled from many levels. The database schema may allow access to an entire table and the applications provide a further level of granularity, restricting access based on a validated profile. Having this type of documentation is very important, and is a best practice. It can be used with other information, such as the Application & Interface Documentation, to determine areas of weakness and vulnerability. That information is useful in determining if the implementation of the security plan meets the needs of the Internal Controls.

What procedures are in place for adding new employees? What access do they require? Who authorizes this? Do certain types of access require secondary authorization or validation? What training do they need before they physically access production systems? What procedures are in place for revoking access after an employee terminates employment or goes on an extended vacation? What notification is required? Is it complete? Is it timely? How are all of these events documented?

Then there is physical security. Where are the computer systems located? Are they secure? Are they safe from environmental hazards such as water and smoke? Are there safeguards for known risks – such as bolting down equipment in areas prone to earthquakes?

Exception Processing Procedures

Usually the workflow continues without issue, but occasionally there are going to be problems that require some type of manual intervention. In nearly all systems there is a process for addressing this type of issue, although it may not be documented. It is important that events and actions like these are documented (a best practice), and if deemed material to financial reporting then will need to have a control associated with them – even if that control is exception handling. In cases like this, automated controls can be very helpful.

Where this becomes a more significant and serious issue is when exceptions are managed “after the fact”, or outside the scope of the standard applications and processes. For example, is there someone in your organization who routinely “fixes” data? What type of change control process do they use? Who authorizes these changes? Where is the audit trail for this event, including data on the specific changes, maintained? In cases like this there is clearly a need to fix the root cause of the problem and then implement controls for future changes.

Having a rigid, standardized process is a helpful control. It should provide the necessary audit trail (such as the data before and after the change) evidence as well as documentation of the reason / need for the request and the appropriate review and approval. All of this information / documentation should then be stored in a persistent repository.

In one environment our group acted as the control. End users requested specific data changes or fixes. A helpdesk ticket was generated for this request. A programmer was assigned to develop queries in a representative test environment to satisfy the request. They would update the helpdesk ticket, attaching the queries and the test results. A business analysis would review the test output to validate that the work performed met the requirements of the original request, and that there were not new problems generated by this change. They would update the ticket and once it was ready it would be sent to a business manager for approval. Once it was approved we had authorization to proceed. We would review the queries and then run them in production. The queries had the before and after-image of the data being manipulated. The complete logs were attached to the helpdesk ticket, the requesting user was notified of completion of the task, and the ticket was closed.

Single Points of Failure (SPOF) Analysis

This type of analysis is used to help identify risk and quantify the impact of any possible risk event. It is a best practice from a general business perspective (what are the weakest links in the chain?), but relative to Internal Controls it can help point out deficiencies relative to specific controls. This should look at systems, processes, and even specific people. What are the risks for each specific environment? What is the impact of a risk event? Should the risk be transferred, mitigated, eliminated, or ignored? This type of analysis will help make that determination. When viewed in the context of the other documentation that has been generated so far it will provide direction and justification for what needs to be done.

Business Continuity Management

Disaster Recovery Planning (DRP) is the planning, preparation, and procedures necessary for the restoration of systems, infrastructure, and data. This is traditionally what companies did to protect one of their most important assets – data. But, that failed to completely address ongoing business operations. Business Continuity Planning (BCP) took Disaster Recovery a step further to allow the business to continue key operations after a disaster. Therefore, a BCP is dependent on a DRP. Now this often falls under the umbrella term "Business Continuity Management" (BCM), more accurately reflecting the ongoing process nature of this work.

Many people will state, "SOX doesn't care whether or not a business concern is able to continue as long as it reports that fact correctly." While there is no pure requirement for any type of disaster recovery or business continuity planning, it is indeed implied. As mentioned earlier, SOX Section 406(c)(2) requires "*full, fair, accurate, timely, and understandable disclosure in the periodic reports required to be filed by the issuer.*" So, how do you insure the completeness and timeliness of this reporting? Business Continuity Planning is an important part of the answer.

Project & Risk Management

The practice of professional project management can really help drive the SOX 404 effort. Someone with experience and proven expertise (such as a PMI certified Project Management Professional, or PMP) who understands how to decompose a complex process into manageable components and coordinate activity is invaluable. Has all work been accounted for? Are the right people working on the right pieces at the right time? Are there dependencies between tasks? Is Risk being managed? Is there effective communication and documentation? Again, this is a best practice for any large effort, especially one as visible as SOX.

This also creates an opportunity for Independent Validation & Verification, a process that utilizes outside expertise to validate that the planning and efforts are complete and will deliver the desired results. Expertise from various areas is usually leveraged to not only look at what is being done, but also how it is being done. This can save time and money if problems are identified early, and will provide an additional level of comfort for Management.

A good Project Manager will also document important events, such as detailed meeting minutes that include information about issues, positions and opinions, decisions made, etc. This information could prove invaluable when working with Auditors, especially since an External Auditor can rely on the work of others. Justification about the scope and the level of specific controls can be provided using this historical information.

As an aside, the question may arise whether a Project Manager is truly responsible for SOX on a day-to-day basis. It is my opinion that they are. In addition to SOX being a part of the requirements for a project, every Project Manager should understand that their projects could impact financial reporting in both direct and indirect ways. Therefore, it is incumbent upon them to perform their due diligence regarding SOX and to plan for SOX resources and reviews within the scope of their project.

Do all companies require the same level of detail?

No. The U.S. Securities and Exchange Commission issued a statement (http://www.sec.gov/info/accountants/stafficreporting.htm) that included the following directives:

- The purpose of internal control over financial reporting
- Reasonable assurance, risk-based approach, and scope of testing and assessment
- An overarching principle of this guidance is the responsibility of management to determine the form and level of controls appropriate for each organization and to scope their assessment and testing accordingly. One size does not fit all and control effectiveness is affected by many factors.

The Internal Auditor for your organization should seek advice from the External Auditor regarding the appropriate level of detail for a typical organization of this size, and then present recommendations to Management for final approval. When done properly this should not violate the SECs auditor independence requirements. Keep in mind that the External Auditor will let you know what types of questions or activities are “out of bounds.”

Is there a recommended approach?

The SEC has provided recommendations based on their experience to date. They suggest a top-down (process, not system) and risk-based approach to implementing internal controls. The tools and best practices described in this white paper will help you accomplish this.

The real trick is finding the right balance. Working closely with your Internal Auditor at an early stage will help to define the scope of your efforts. Some systems can be easily be deemed out of scope for the SOX 404 effort. For example, a website residing on an isolated server that does not provide any type of transactional feeds or access to production systems. The reason for this decision should be documented for future reference.

Once you've determined what is clearly out of scope then start looking at what remains. The pieces of the puzzle described in this document will help determine what is material versus what is supporting, and will help identify risks to those systems. From there you can work with the Internal Auditor and Management to define the level of controls that are necessary for your specific organization. Each piece of the puzzle builds upon the previous piece, and before long you have a complete picture of what you need to accomplish. This avoids wasted time and effort and positions your project for success.

Next you need to look at the types of controls. Keep in mind that everything within the scope of these systems needs to follow a control process – but the level of control will vary based on several factors (e.g., size of the company, impact to financial reporting, etc.) Some controls will be preventive while others will be detective. Controls should also provide a mix of compliance testing with substantive testing (analytical procedures). Automated controls are always preferable to manual controls since they are easier to validate.

Regardless of the type of control you will be required to periodically test the control and maintain evidence of the tests. Often the sample size will require that you produce evidence of testing over multiple periods so it is important to safeguard those results as you would safeguard any other asset in your organization. Create a test plan that includes repository management of test results!

Is there anything else? A change management system is truly essential to all aspects of internal controls. Configuration changes, hardware and software upgrades, data changes, network changes, etc. all need to be tracked. The "system" (could be manual, not necessarily an expensive automated system) needs to be able to track various types of events at different levels of granularity. Data for a network configuration change will differ from data for a "production data fix." Even programming changes and the associated binary / executable file implemented in production should be tracked. It is also possible to use this change management system to manage your testing evidence. It doesn't have to be fancy but does need to be consistent, complete, and secure.

Are you ever really done?

Unfortunately, no. This is a process and must be thought of that way. There will be an ongoing need to update and validate the process and supporting documentation. Proving that the controls are complete and sufficient is a part of this comprehensive process. And as good as things are today there are bound to be changes tomorrow. Periodic review of the controls, execution of pre-approved tests to validate that the controls are effective, and documentation of these efforts are an ongoing task.

Because of this it is important to develop a system of tracking the controls and their tests. It should be capable of:

- Storing several generations of the controls and their test output
- Easily enhancing the control
- Using integrated change control mechanisms for the review, validation, and approval of all changes
- Reporting on changes

It's a matter of perspective…

This is a classic case of "is the glass half-empty or half-full?" Many companies will view Sarbanes-Oxley as a bane for their business. But it really is an opportunity, resulting in many positive benefits.

- Standardization and simplification of computing environments
- Automation of manual processes
- Removal of unnecessary risk items
- Improved efficiencies of systems leading to improved performance and reduced operating costs
- Documentation that is comprehensive and useful, removing the "urban legend" dimension of some environments

It provides the opportunity to improve the understanding of your environment, leading to better support and fewer problems. These factors directly relate to the total cost of ownership of a system. There is clearly value to doing this right.

Summary

If you've looked at the various references cited within this white paper you will understand that this can be a challenging task at best. Understanding what is required, having a solid plan of action, and then leveraging skilled resources will help to achieve the ultimate goal of implementation of the necessary internal controls for your business. The focus is on doing what is necessary and doing it right.

Lighthouse – Helping to Navigate the Fog of Compliance™

Just as a lighthouse provides guidance for Mariners, our Lighthouse™ Service will provide the guidance that your organization needs to effectively and efficiently navigate the waters of compliance. We cut through the fog of complex frameworks and help you navigate to your desired destination.

It can be complicated knowing exactly what is required, and to what level of detail. One size does not fit all, and a software product will be unlikely to provide the level of internal controls that auditors want to see.

What is the answer? Expertise of Business, Management, and Technology. A defined process to guide the effort that utilizes proprietary software tools to facilitate and expedite the effort. This combination approach provides the level of results that your organization requires, saving time and money by avoiding unnecessary work. Effort is focused where it is needed.

Please contact us to see how we can help your organization navigate the fog of compliance.

About the Author

Chip Nickolett, MBA, PMP is the President of Comprehensive Solutions. The *pieces of the puzzle* listed in this white paper are all areas that he and his team have focused on for years. Chip helped implement SOX internal controls for a legacy ERP system at a large global company using this approach. For more information please see http://www.Comp-Soln.com/chipn.html.

Let Us Help You Succeed!

Call today to discuss ways that Comprehensive Solutions can help your organization save money and achieve better results with your IT projects. We provide the ***confidence*** that you want and deliver the ***results*** that you need.

View our “SOX Internal Controls” Brochure

View our “Project Management” Brochure

Back to White Papers
Back to Services

Comprehensive Solutions
4040 N. Calhoun Road
Suite 105
Brookfield, WI 53005
U.S.A.

Phone: (262) 544-9954
Fax: (262) 544-1236

This document is provided for informational purposes only, and the information herein is subject to change without notice. Please report any errors herein to Comprehensive Consulting Solutions. Comprehensive Consulting Solutions, Inc. does not provide any warranties covering and specifically disclaims any liability in connection with this document.

All product names referenced herein are trademarks of their respective companies. Use of these names should not be regarded as affecting the validity of any trademark or service mark.