

The Top Down Group



Sarbanes-Oxley and Internal Audit:

A overview to SOX 404
compliance

Definition of Internal Audit

■ "an independent, objective assurance and consulting activity designed to **add value and improve an organization's operations**. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and **improve the effectiveness of *risk management, control, and governance processes***."

Responsibilities of Internal Audit

- Assist in oversight of Sarbanes Oxley Compliance
- Communicate with Management concerning the overall internal control structure while maintaining independence
- Act as a liaison between external auditors and management
- Should have full access to all functions, records, property and personnel, as well as to the audit committee
- Monitor and assess management's awareness and consideration of risk
- Develop an audit plan to ensure efficient operations and systems
 - Perform operational audits of different areas based on a formal Risk Assessment of the Company (prepared by Internal Audit)
- Update the Audit Committee on people, processes and controls at the Company
- Perform any investigative work at the request of Management/Audit Committee

Section 404 of the Sarbanes-Oxley Act (SOX)

- Requires an “Internal Control Report” at the end of every year that states:
 - It is Management’s responsibility to establish and maintain a system of internal controls governing financial reporting
 - Management’s opinion on the effectiveness of the financial reporting controls
 - Sufficient evidence to support its opinion
- * Requires an attestation report by external auditors
- Management’s assertions of controls over financial reporting
- Results of their testing of key controls over financial reporting and other key aspects of the Act

Committee Of Sponsoring Organizations (COSO) Framework for Internal Controls:

- Section 404's "adequate structure and procedures" correlates to the five key components of the COSO framework for internal controls:
 - ❖ Control Environment - tone of the organization, foundation of the components of internal control.
 - ❖ Risk Assessment - identification, evaluation of relevant risks to the achievement of Company's goals; forms basis for how risks should be managed.
 - ❖ Control Activities - policies and procedures to help ensure that Management's directives are carried out.
 - ❖ Information & Communications - timely, efficient exchange of information that enables people to carry out their responsibilities.
 - ❖ Monitoring - process that assesses the quality of internal control performance over time.
- * KEY: All five components must be in place for an adequate control environment.**

What does all this mean to your Company?

- Only that we have to make sure you are consistently performing control activities that you are already probably doing.
 - Control activities are the policies and procedures that help ensure management directives are carried out. They help to ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions.
 - Some examples of control activities:
 - Signature Approvals (timesheets, job orders, invoices, journal entries, purchase orders, etc.)
 - Authorizations (evidenced by signature)
 - Verifications (evidenced by signature)
 - Reconciliations (signed, supported and filed)
 - Reviews of operating performance (QTD Variance analysis, budget to actual, etc.)
 - Segregation of duties
 - Whistle blower hotline
- * Key – Control activities eliminate the “Enron excuse.”
 (“I knew nothing about it!”)**

So how do we get started?

I. Prepare an Top Down, Risk Based assessment of your company

A. Document the overall control environment at the Company.

- ✓ Requires interviews with key personnel.
- ✓ Helps develop a sense of the corporate culture and overall "tone at the top."
- ✓ Describes the Company's activities that address each of the five components of a Control environment. (I.e. What sort of environment do we have?)
- ✓ Details any fraud prevention mechanisms we have in place.
- ✓ Enables Management to assess the scope of the project.
- ✓ Allows external auditors to gauge Management's opinion the Control environment and consider the risk of the company.

*** Key – Starts the process by getting people to think about the Control Environment.**

II. Document Processes that affect Financial Statements

- * Processes usually include: Financial Close, Payroll, Accounting for Fixed Assets, Inventory, Purchasing and payment, etc.
- I. Prepare a flowchart or narrative that describes the process from beginning of the cycle until it affects the financial statements.
- II. Develop a "Control Matrix" for different activities in each process that includes:
 - I. Control objective for the activity (bank reconciliations)
 - II. Risk of not performing the control (theft/underreporting cash balances)
 - III. Control activity: When do we prepare bank recs? How do we prevent theft of cash? Who prepares it? Who reviews it? Etc.
 - IV. If we don't have a control activity for a certain control objective, it's considered a DESIGN deficiency.
- III. Interview process owners (i.e. the "preparer" of bank recs) to document the control activities we perform
- IV. Identify "Key" Control activities that MUST happen in a sound control environment
- * **Key – The process owners, not Internal Audit, perform and monitor these controls activities.**

III. Test your "Key" Controls

- I. Management testing normally occurs twice during the year - Phase I and Phase II.
- II. Testing is often performed by Internal Audit, or some other independent source (outside consultants or internal employees unassociated with the process being tested.)
 - i. Phase I (usually earlier in the year) establishes the control is functioning as designed.
 - ii. Phase I testing may involve: Sampling 30 invoices to ensure of evidence of approval/review; Reviewing 10 Journal Entries to ensure adequate support and evidence of review; Sampling 20 timesheets to see if employee and supervisor have signed.
- III. All sampled evidence must be copied and footnoted to support management's conclusion about the effectiveness of controls.
- IV. A control that does not perform as designed is considered OPERATING Deficiency
- V. Testing work is then reviewed by External Auditors to aid in their assessment .

*** Key – Our documentation claims we perform a control activity. Testing Proves (or disproves) it.**

IV. Remediate any Design or Operating Deficiencies

- I. There will ALWAYS be some testing exceptions (operating deficiencies). No such thing as 100% effective controls where human interaction is involved.
- II. Management must attempt to remediate all testing exceptions or control deficiencies.
- III. Responsibility of Process Owner/Supervisor to remediate exceptions or fix control deficiencies
- IV. Phase II testing will focus on:
 - I. Sampling a smaller size or Just inquiring and observing control activity.
 - II. Evaluating and testing Remediation items (Phase I testing exception or Control Deficiencies.)
- V. Any deficiencies NOT remediated by year end MUST be evaluated by Management when preparing its final assessment of Internal Controls for SOX 404.

*** Key – Correct Operating and Control Deficiencies**

V. Evaluate outstanding deficiencies

- I. Formally evaluate each deficiency to determine it's "seriousness."
Three types of deficiencies
 - Control Deficiency – Normal deficiency, immaterial to financial statements
 - Significant Deficiency – A "more than inconsequential" but less than material deficiency. A serious control deficiency exists in a process.
 - Material Weakness – A material control deficiency exists which does not allow the external auditors to rely on Company's control environment. Must be disclosed to investors.
- II. The SEC requires management to report on effectiveness of I/C as of a point in time rather than a span. A material weakness occurring earlier in testing is not reportable if remediated and operating long enough by year end.
- III. Determining when a significant deficiency becomes a material weakness is based on two components: significance & the probability a F/S error would occur and not be detected by compensating controls.

Some Key Focus Areas

- Entity Level Controls.... Tone assessments
 - Scoping analysis... what are the significant accounts/processes
 - Spreadsheet controls
 - Reconciliation procedures
 - Journal entry review/support
 - SAS 70 evaluation methodology
 - Fraud prevention and safeguarding methodology
 - Audit Committee responsibilities/documentation
 - Control deficiency evaluation methodology
- * Key- YOUR key role as a Control owner**
1. Accurate description of process and control activities when being interviewed.
 2. Completeness of information and timely response to requests
 3. Remediate Testing exceptions/Control Deficiencies
 4. Stay involved/Think about your job and how it relates to SOX

Effect of a Material Weakness

- Companies reporting a material weakness experienced a 4% drop in stock price relative to the Market in just two months! (CFO Magazine, July 21, 2005)
- Most deficiencies were personnel segregation and experience.....controls over journal entries and closing process, reconciliations.....procedures controlling QC over reporting, design/review of policies and evidence.
- Deficiencies by Industry... highest in software and service firms, then in descending order manufacturing, health care, pharmaceuticals, financial services and electronics.
- SEC - Companies with material weaknesses need to fully disclose the circumstances so investors can evaluate the underlying factors as to why it happened.
- SEC - Asked investor groups to issue guidance on how a material weakness will impact their evaluations of a company.
- Not all material weaknesses to be viewed as equally significant.....to investors decision processes.... some may have a greater or lesser impact.
- Regard will be given to the fullness of management disclosure, underlying cause of the material weakness and managements actions to address it.

The Top Down Group: What we can do for your company

- The Top Down Group specializes in custom tailoring a SOX compliance program for each client, making sure the benefits of sound internal controls outweigh the costs and effort.
- SOX compliance doesn't have to be complicated, time consuming or expensive, it just needs to be tailored correctly for each company.
- The Top Down Group will:
 - ❖ Work with your company to understand the business, the processes and the control environment.
 - ❖ Develop a SOX plan just right for your company and your budget, enabling you to focus on running your business.
 - ❖ Prepare a top down, risk based approach to your SOX compliance project, focusing on scalability and materiality.
 - ❖ Prepare a project plan, timeline and testing strategy for the project.
 - ❖ Guide you step by step on documenting, testing and assessing your control environment and ensure a repeatable, efficient process, year after year.

Timothy J. Simkiss background

- Timothy J. Simkiss, CPA founded the Top Down Group after several years of consulting and public company internal audit experience in diverse industries ranging from utilities, telecommunications, professional services, consulting, biomedical, distribution and pharmaceutical.
- Responsibilities have included
 - ❖ Sarbanes Oxley compliance
 - ❖ Due diligence audits
 - ❖ Enterprise risk assessments
 - ❖ Reviews / operational efficiency audits
 - ❖ Documenting of finance and accounting policies and procedures.
- Mr. Simkiss holds a Master's of Finance, a Bachelor's of Science, and has been a Certified Public Accountant since 1999.
- Mr. Simkiss is a member of the Institute of Internal Auditors and the Financial Executives Networking Group.