

Thinking Outside the SarbOx: Operational Controls for Sarbanes-Oxley 404 Compliance

**By: Maureen McAllister C.P.A.
McAllister Consulting L.L.C.**

OVERVIEW

This module describes how standard operational controls, typically operating outside of the accounting arena, are useful in demonstrating Sarbanes-Oxley 404 compliance.

The Sarbanes-Oxley legislation of 2002 created specific requirements for public companies relative to their internal controls over financial accounts and reporting. Among other requirements, public companies are required to assess their internal controls periodically, to help assure investors and other stakeholders that financial data are reliable. Internal controls are the procedures, practices, checks-and-balances that help ensure the financial data and associated reports fairly represent the financial condition of the firm.

This module focuses on operational controls as a significant source of objective evidence to support management's assertion of effective internal controls. The ISOxsm approach, described in this module, utilizes evidence from expanded audits of the Quality Management System (e.g., ISO 9001) to support those management's assertions. This approach saves time and money and has other benefits.

To aid learning, key concepts are summarized at the top of most pages. Details follow. Consult the last page for additional assistance.

Learning Objectives

- Recognize the connection between operational controls and the related financial controls
- Appreciate how these operational controls provide evidence in support of Sarbanes-Oxley section 404 compliance
- Understand where to find this evidence outside of the accounting arena, especially in organizations that have formal management systems in place, like ISO 9001
- Learn how the “ISOxsm” internal audit approach blends the auditing of operational controls with similar activities in an ISO system, saving time and money while providing objective evidence of 404 compliance.

Operational controls are those systems, procedures, checks-and-balances that operate as the firm executes its major activities. For example, a firm will have controls in place to ensure assets are safeguarded:

- controls over the purchasing and physical receipt of goods and services
- systems to ensure that only trained and competent personnel perform work
- transactional controls over inventory disbursements, shipping, and invoicing

Many operational controls feed directly into systems that generate financial data. A purchase requisition, once approved, becomes a purchase order, a liability, a payable, and ultimately, a cash outflow.

Operational controls, when properly designed and functioning effectively, provide objective evidence that the related financial data are reliable.

To get at these operational data, however, a firm's accounting personnel usually need to look beyond their own arena of responsibility. These operational controls often are the responsibility of operations, engineering, sales/marketing, materials management, HR, and other functions.

In organizations that have a formal management system, such as ISO 9001, these systems, procedures, and controls are already established, documented, implemented, and audited.

The ISOxsm approach to Sarbanes-Oxley (SOx) 404 compliance utilizes these controls to provide supporting evidence for the effective functioning of related financial controls. For example, an audited ISO 9001 system shows compliance to basic controls over the purchasing and receiving practices of a firm. By taking this evidence, and extending the ISO auditing “upstream” and “downstream” into the related financial controls, the firm can show a proper flow that results in sound, reliable inventory balances.

This blended approach is known as: “ISO” + “SOx” = ISOxsm

ISOxsm merges the ISO audit with other internal audits performed by the finance/accounting personnel. Efficiencies result.

The Learning Path

- The Driving Force: Sarbanes-Oxley Section 404 compliance
- Operational Controls Outside of Accounting: The ISO Management System Model
- Utilizing management system controls for 404 compliance
- Internal Auditing: A Focal Point for Integrated ISO and SOx Compliance
- ISOxsm in Context
- Next Steps

This module follows a simple path to explain the effective usage of ISOxsm audits in support of SOx 404 compliance. Cost-effective SOx 404 compliance is the key driving force behind ISOxsm.

Management systems like ISO 9001 have easily-identifiable operational controls because the ISO standard requires these controls in pursuit of its' primary objective: customer confidence. The connections between ISO operational controls and related financial controls are then described in terms of the COSO model of internal controls and the PCAOB's Auditing Standard No. 2 requirements.

ISOxsm focuses on internal auditing, a requirement of all ISO management systems. This module provides examples of how this is done, including a sample "walk through" structure and sample audit questions from a blended ISOxsm audit.

The ISOxsm approach to demonstrating compliance must be viewed in the larger compliance context. The SEC and PCAOB are still working on implementation. Moreover, operational data are only part of the compliance puzzle. Many controls are outside the scope of an ISOxsm internal audit. While it doesn't fulfill all compliance needs, ISOxsm helps hold down costs by gaining efficiencies and avoiding redundancies.

Next steps offer practical guidance on launching an ISOxsm audit program.

The Driving Force: Sarbanes-Oxley Section 404 Compliance

- See www.sec.gov for specifics
- Rebuilding investor/market confidence in the face of examples of accounting irregularities and loss of stakeholder value
- Emphasizing the underlying systems and procedures to help ensure credible financial data
- Preventing fraud and unintentional errors
- Encouraging a “culture” of ethics and compliance with standard operating procedures
- Various abbreviations; examples: “SarboX” or “SOx”

The U.S. Securities and Exchange Commission oversees Sarbanes-Oxley compliance as part of its broader mission of regulating public companies.

The Sarbanes-Oxley legislation of 2002 was meant to put teeth into the internal controls over financial data and reporting. It was designed to rebuild investor/market confidence badly shaken by the Enron and other debacles.

In a nutshell, Sarbanes-Oxley placed a lot more responsibility on both firm management and the public accountant auditors to “get it right”. The assessment and auditing of internal controls related to financial reporting are supposed to help prevent fraud as well as unintentional errors/omissions by ensuring that proper internal controls are in place and operating correctly.

As part of this, Sarbanes-Oxley is looking to encourage a culture of good corporate governance from the top to the bottom of every public company. High ethical standards and a high regard for adherence to established procedures should pervade an organization. In fact, its impact is so sweeping that Sarbanes-Oxley issues are often in the mass media, where it has become known by a variety of acronyms: “SarboX” and “SOx” are just a couple.

Internal Controls.....Or You Can't Test Everything

- See www.coso.org for the most widely accepted model of internal control in the accounting community
- Internal Controls as the 24/7 safeguards against errors, omissions, and fraud
- Emphasis on SOPs, checks and balances, and similar safeguards
- Elements of internal control (from COSO):
 - Control Environment
 - Risk Assessment
 - Control Activities
 - Information and Communication
 - Monitoring

Emphasis on Management's responsibility to ensure that internal controls exist and are effective at both the entity-level and the activity-level

The business and accounting communities have long recognized the importance of internal controls in generating reliable financial statements. The Committee of Sponsoring Organizations (see www.coso.org) has a long-established and highly-regarded model for internal controls. Known as the COSO model, it has five elements of internal control:

- control environment
- risk analysis
- control assessment
- information and communication
- monitoring

COSO has more recently issued a broadened model of risk management which consists of eight elements.

Both models help management to design an effective internal controls system. Importantly, these controls must exist at both the entity-level and the activity-level. Some controls, like establishing the proper policies and communication channels, are put in place by management and should operate throughout the firm. Other controls, over transactions like purchasing, receiving, shipping, and invoicing, must operate at the activity level. Both types of controls are necessary.

There is a balance between the strength of controls and the auditing/testing required to ensure that the resulting financial data are reliable. The stronger the internal controls system, the more confidence in the financials. Auditing and testing can be adjusted accordingly. In fact, 100% testing of financials is as unrealistic as 100% inspection of product to look for defects.....no amount of "looking" will catch every possible problem.

SOx places responsibility for assessing effective design and implementation of internal controls squarely on the shoulders of senior management. SOx requires that the CEO and CFO assess internal controls and make assertions about these controls in their public financial statements.

Financial Controls and Operational Controls

- Definitions:
 - Financial
 - Operational

Operational Controls as the foundation for many financial controls

Operational controls help create the proper control environment throughout the organization

Earlier we saw how operational controls often exist outside of purely accounting functions (e.g., on the receiving dock) and tend to align with day-to-day activities of the firm. Typically, these exist within other functional areas, some geographically remote from the accounting activities. In a sense, this makes them all the more important, as they may be overseen by individuals with little or no responsibility for financial data.

For simplicity, operational controls can be thought of as those controls, wherever in operation, that relate to the basic business purposes of the firm and are not strictly an accounting activity. Financial controls are those that related more directly to the preparation of financial statements and may have little impact on or visibility to day-to-day business activities. Good examples are controls that relate to depreciation calculations, consolidating entries, and accounting estimates.

In many situations, operational controls are the foundation of many financial controls. For example, a good set of receiving and incoming inspection controls help ensure that raw material inventory figures are reliable. Allowance calculations for slow-moving and obsolete inventory are more credible with proper operational controls in place.

Good internal controls also help create the proper control environment, one of the five essential elements of internal control in the COSO model. The discipline and rigor associated with written procedures, carried out by competent personnel, help “set the tone”. COSO’s activity level (receiving controls) and the entity level controls (written procedures enforced by management) operate in tandem.

Operational Controls Outside of Accounting: The ISO Management System Model

- Compliance to management system standards
- ISO 9001 and its derivatives
- Emphasis on preventing vs. detecting errors
- Stress on corrective action when errors do occur
- Safeguard the customer (and indirectly, all stakeholders)
- Registration to management system standards: objective evidence
- Usefulness for SOx 404 compliance

Operational controls can take on additional strength and credibility when they are part of an overall management system like ISO 9001. ISO 9001 is a quality management system standard to which many firms become registered. Registration involves an outside third party (a “registrar”) periodically evaluating the compliance of operational controls vs. the ISO 9001 standard. This standard is issued by the International Organization of Standardization, an organization of national bodies headquartered in Switzerland, and functioning to facilitate international trade (among other things).

The ISO 9001 standard is not industry-specific, but it has industry specific “sister” standards including ISO/TS 16949 for automotive, AS 9100 for aerospace, and others. These share many commonalities related to operational controls. These standards emphasize the importance of internal controls to prevent failures and to institute correction and corrective action when errors/omissions do occur.

These standards are written especially with the customer in mind. However, all stakeholders, including investors, benefit when a firm operates in a systematic, controlled manner. Beyond this, all stakeholders can take comfort from the objective evidence of controls afforded by an ISO audit. ISO compliance requires internal auditing. Routine surveillance audits by an ISO registrar are also required. Both types of audits provide objective evidence of compliance to the ISO requirements, and also document non-conformances. Formal corrective action is mandatory for these deficiencies.

A management system like ISO 9001 is useful in supporting management’s assertions about the effectiveness of internal controls as required by SOx 404. Evidence from these internal controls may also be of use in the public accountant’s audit of internal controls, as required by SOx.

ISO 9001: A Very Brief Overview

- International standard
- Focus on customer requirements and satisfaction
- Requires that key business processes and certain activities be documented, with appropriate recordkeeping of actual results
- Emphasizes preventing error and failures by a consistent, disciplines adherence to approved internal procedures
- Stresses monitoring and measurement of key business processes to access performance against requirements
- Requires auditing as both a self check and by accredited third parties
- Is orchestrated by a designated ISO Management Representative
- Drives management involvement and oversight, especially via the Management Review process

ISO 9001 is an international standard focused on customer requirements and satisfaction. In a sense, the customer is analogous to the investor. In some industries, customers actually demand that their suppliers be ISO registered. Both customers and investors stand to benefit when the firm operates within a well-designed internal control system.

ISO systems have documented processes, identifying the key inputs, activities, and outputs of each Process (e.g., the quoting process, the product engineering process, etc.) Interfaces between processes are also identified (their “sequence and interaction”).....similar to what is audited in a walk-through of interrelated transactions. Process results are monitored. Where processes do not achieve their goals (“planned results”), correction and corrective action are required.

The requirements of ISO are stated as “shalls” within the standard. For example, the ISO standard states that the firm shall have a documented procedure for handling and controlling non-conforming product (“rejects”) and goes on to define the topics that procedures must cover.

Among the “shalls”, the ISO standard requires on-going internal auditing. The results of audits (both internal and registrar) must be reported to and reviewed by senior management.

The ISO system is headed-up by a designated ISO Management Representative. This representative is often the executive in charge of operations or quality assurance, but may be any of the organization. His/her primary duty is to establish and oversee the quality system, report results to Top Management, and promote awareness of customer requirements, internally and with other stakeholders. Importantly, the ISO Management Representative can become an ally in 404 compliance. The Management Review activity, periodic reviews of plans and results, is required by ISO and helps ensure management’s involvement in the quality management system.

The ISO 9001 standard is available in the United States through the American Society for Quality (ASQ) or the American National Standards Institute (ANSI).

Operational Controls: Entity Level and Activity Level

- ISO “shalls” (requirements) align with the internal controls related to significant accounts and assertions
- ISO requirements align with both entity and activity level controls and with COSO elements
- Both levels of control are important for ISO compliance
- ISOxsm utilizes the connection between ISO requirements and internal controls to create a consolidated or “blended” internal audit program.

	Control Environment	Risk Management	Control Activities	Communications and Information	Monitoring
Entity Level Controls	<p>Quality policy (5.3)</p> <p>Quality objectives (5.4.1)</p> <p>Defined major business processes with metrics (4.1, 8.2.3)</p> <p>Job descriptions (5.5.1)</p> <p>Commitment to competency (6.2.2)</p> <p>Organization charts (4.1)</p> <p>Management Review (5.6)</p>	<p>Defined and documented major business processes and related sub-processes and transactions (control points) (4.1, 4.2.2)</p> <p>Business-level planning (e.g., budgeting (5.4.2)</p> <p>Product-level planning (e.g., APQP; FMEA, etc.) (7.1)</p>	<p>Control activities embedded within documented processes (all of section 7)</p> <p>Defined linkages between processes (4.1, 4.2.2)</p> <p>Task-specific work instructions controlling Production (7.5.1)</p> <p>General IT controls (4.2.3, 4.2.4, 6.3)</p>	<p>Awareness of company-level data (e.g. quality policy; customer requirements) (5.5.3)</p> <p>Training (6.2.2)</p> <p>Feedback on customer issues (5.1, 5.2, 8.2.1)</p> <p>Communication on QMS performance and effectiveness (5.5.3)</p>	<p>Major process monitoring and measurement (8.2.3)</p> <p>Internal Auditing (8.2.2)</p> <p>Management Review, including a variety of data to be monitored (5.6)</p>
Activity Level Controls	<p>Defined methods for the setup and maintenance of key data:</p> <ul style="list-style-type: none"> - customer master - product master - vendor master <p>(4.2.4, 6.3)</p> <p>Procedures defining specific task, responsibilities, authorizations, etc. (5.5.1)</p>	<p>Authorizations for control/risk points (points of “hand-offs”), embedded in key processes:</p> <ul style="list-style-type: none"> - order review sign-offs - product/ECN controls - purchase order review - etc. (all of section 7) <p>Limitations on “near cash” activities (e.g., scrapping product; purchases) (7.4, 8.3)</p>	<p>Defined work flows with authorizing documents to control work steps, acceptance of work output, and authorization to ship/invoice (e.g., work orders, requisitions, product acceptance criteria, etc.) (section 7, 8.2.4)</p> <p>Electronic and manual audit trails in related systems (4.2.4, 6.3)</p>	<p>Business systems and communication tools to support the major business processes and objectives – information sharing, which allows individuals to complete their assigned tasks and have evidence (e.g., email) of significant communications (6.3)</p>	<p>On-going monitoring of production/service provision activities, including transactions related to cost (e.g., raw material consumption, scrapped product, etc.) (7.5, 8.2.4) and pricing (e.g., customer order review) (7.2)</p>

Putting the pieces together

Perhaps the hardest part of constructing an ISOxsm internal audit program is understanding how all the “moving parts” mesh together.

Some of the complexity comes from the number of interested parties. At a minimum, these include:

- senior management
- accounting
- the financial internal auditors
- the ISO management representative (if the company is ISO registered)
- ISO internal auditors (ditto)
- functional management
- the public accountants
- investors
- the SEC, and specifically, the PCAOB.

Whoever heads up the ISOxsm internal audit program will need to work with these, and possibly other stakeholders, to produce an audit program that is beneficial.

The remainder of this module focuses on how one can put together all the pieces to please all the stakeholders.

First, we need to address two issues that are not directly part of the ISOxsm internal audit program but need to be clarified:

1. Is the ISOxsm approach valid and useful for an organization that is not ISO registered?
2. How do the internal controls, which are the starting point of an ISOxsm internal audit, relate to the requirements of PCAOB?

ISOxsm in the Non-ISO organization: Is it still applicable?

- ISO-type operational controls typically exist in many non-registered organizations
- Reflect good operating procedures, even if not documented
- ISO provides a template/yardstick for operational controls, even where there is no intent to become ISO registered

Operational controls exist in many non-registered companies. Most public accounting firms or financial institutions (e.g., providing loans to a public company) would look for basic controls.....separation of duties, checks and balances in authorizations, etc.

In many smaller organizations, duties and responsibilities tend not to be documented, and the separation of duties is constrained by the limited number of personnel. Such companies often do not have written procedures, no formal reporting structure (organization chart), and looser controls over who is authorized to do what.

Nonetheless, the ISOxsm approach is applicable in a non-ISO firm. Taking the ISO “shalls” (requirements) and seeing how these align with existing controls in the non-ISO firm can create a template for possible deficiencies to investigate.

Consider the ISO requirement for how a company handles nonconforming product. (An ISO registered firm must a documented and implemented procedure for controlling how “rejects” are handled so the rejected items do not get used or shipped to customers accidentally. See ISO 9001, section 8.3.) Such controls normally include how these rejects are physically segregated, recorded in the perpetual inventory system, scrapped, scrap recovery, etc. Whether documented or not, controlling nonconforming product as required by ISO just makes good business sense.

ISO vs. significant Financial Accounts and Assertions related to Internal Control:

The controls defined in the PCAOB's Auditing Standard No.2 include:

- controls over initiating, recording, processing the reporting significant accounts and disclosure-related assertions
- controls over the selection and application of accounting policies
- antifraud programs and controls
- controls on which other controls are dependent (e.g., general IT controls)
- controls over significant non-routine and nonsystematic transactions
- specific company-level controls

Auditing Standard No. 2 stipulates significant controls to be tested by Management as part of its review of internal controls. A couple of examples illustrate how ISO systems/data link to controls in these areas:

Controls	ISO Systems/Data
initiating, recording, processing, and reporting	<ul style="list-style-type: none">- quotes to customers- order review/processing- purchases/receipts- inventory transactions- shipping/invoicing
controls on which other controls are dependent	<ul style="list-style-type: none">- documented procedures & policies- training & competency assessment- management review

The relevance of ISO/operational data will depend on the assertions related to the controls being audited. For example, if existence is the assertion being audited, then the ISO practices may be well helpful in demonstrating that only authorized entries are made to inventory accounts.... likewise, when valuation is the assertion. However, if the assertion relates to rights and obligation, then ISO procedures may do little to establish the rights of the company to its stated assets.

This list of controls from AS No. 2 also illustrates where operational controls are probably not part of an ISO system: e.g., controls over the selection and application of accounting policies and controls over significant non-routine and non-systematic transactions.

Constructing an ISOxsm Internal Auditing: The Basic Steps

- The ISOxsm internal audit: An ISO audit of operational controls expanded “upstream” and “downstream” to audit related financial controls
 - Takes the existing internal controls related to financial reporting as the starting point
 - “Filters” the list of internal controls down to only those that are operational
 - Plans the audit program consistent with the directives from management and the public accountants concerning what must be audited and where
 - Constructs audit questions or similar guidance on what to “look at” and “look for” beyond what is normally audited in an ISO internal audit
 - Reports back results in a manner that management can assess the design and implementation effectiveness of internal controls

Internal Auditing is required in any ISO system. The internal audit focuses on each key process and how all the processes are sequenced and interact so as to achieve the organization’s policies and objectives.

As each process is audited, the ISO auditor determines which ISO requirements (“shalls”) apply and looks to make sure that the related control is being met by in actual practice.

The ISOxsm audit is an expanded ISO audit. It starts with the internal controls, filtered so that only operational controls are part of the internal audit.

The overall audit plan reflects what management and the public accountant direct to be audited. For example, if the auditing must encompass facilities responsible for generating at least 65% of the company’s revenue, then the ISOxsm audit plan will likely include the larger facilities that generate more revenue. If certainly deficiencies have been found in the past, those areas/functions are likely to be included.

Questions or other guidance (e.g., a template to fill in) direct the auditor to look for or look at specific items. Typically, these questions take the auditor “upstream” and “downstream” from the ISO controls into the related financial controls. Specific audit questions checks the control being audited. A walk-through approach built into the sequence of audit questions also checks to see if the flow of operational controls feed effectively into the financial transactions to which they relate.

The ISOxsm audit may also include the substantive “testing” that is traditionally part of a financial audit. Statistically-based sampling can be blended into the ISOxsm audit program if desired.

The findings of an ISOxsm audit are reported separately from the results of the ISO non-conformances. Typically, audit questions are structured so a “yes” response indicates activities are per procedure and no errors/omissions/violations are found. “No” responses are summarized for management review and assessment. Management determines if there is enough evidence, considering the balances of preventive and detective controls, to warrant a conclusion that deficiencies, significant deficiencies, or material weaknesses exist.

Planning the ISOxsm audit: More Planning Considerations

- ISO requirement for process-based auditing
- Auditing the ISO “shalls” within the applicable process audits
- Determining the internal controls aligned with each ISO shall
- Auditing guidance
- Reporting

Planning aligns the internal controls with the related ISO elements. Earlier we saw how control topics laid out in AS No.2 align with ISO data. The audit plan takes this one step further and determines how to “piggyback” the auditing of internal controls with specific ISO “shalls”.

As an example, if a company has identified “Customer Order Review” as a significant business process, it must audit this process as part of its ISO 9001 audit. In planning its ISO audit, it will identify ISO elements applicable to that process. Here, ISO section 7.2.2, “Review of Customer-related Requirements” likely will be included in the ISO audit of this process. In most organizations, this process logically includes internal controls related to revenue accounts, accounts receivables, cash receipts, customer returns and allowances, and the like. It also involves controls over “customer master”, “item master”, and other records.

Starting with the list of internal controls, the ISOxsm audit planner identifies each internal control with a specific ISO element. Any process whose audit includes the 7.2.2. requirements also includes an audit of the related internal controls.

Now comes the decision as to the amount of guidance needed by the internal auditors. Depending on the background and skill level of the internal auditors, the ISOxsm audit planner may further define specific questions and/or tests for the auditors to perform (see below).

The net result of the ISOxsm audit is an audit report, detailing what was audited, the findings, and whether there were any non-conformances (ISO) or deficiencies (SOx) for management review and follow-up. The ISO Management Representative and the CFO, respectively, review these findings before any further determinations are made.

Confidentiality considerations will dictate much of how findings are reported. In general, ISOxsm auditors are not asked to make any judgments about deficiencies or weaknesses. This differs from an ISO audit, where the auditor is making a judgment about whether or not the objective evidence observed supporting ISO compliance. The “stakes” are quite different and the skill level of ISO auditors may be quite different from internal auditors from finance/accounting. These and other consideration will influence how results are reported.

The Role of Accounting in Planning the ISOxsm internal audit

- Making the right organizational contacts
- Providing a list of operational internal controls with which to plan the ISOxsm audit
- Gaining agreement where and when to audit these
- Understanding previously-identified weaknesses and deficiencies
- Competency considerations in structuring the ISOxsm audit

Whoever is responsible for planning the ISOxsm must ensure the right players are involved.

For an ISOxsm audit, it is critical that the accounting function, the CFO, and by extension, the outside public auditors, be involved from the first step.

First, the right organizational contacts are crucial. These depend on the structure of the organization (e.g., divisional vs. centralized), the existence of an internal audit function, the expectations placed on the internal auditors, etc. Often, the Accounting function will take responsibility for liaison with the outside auditors.

Accounting must provide the starting point for the ISOxsm audit: the list of internal controls. While Accounting and the public accountant are very concerned with significant accounts and related assertions, the ISOxsm audit takes the internal controls themselves as the starting point. Typically, Accounting will need to provide a list of these internal controls and guidance on where these need to be audited (e.g., at corporate headquarters vs. a branch or divisional facility). Accounting will usually have agreement with the public accountants on where and how often internal auditing is needed.

Accounting provides essential guidance on what to audit and where. It also can influence the ISOxsm audit content by indicating previously-identified weaknesses and deficiencies. This could impact not only what is audited, but frequency, sample size, etc.

When it comes time to audit, there is a real balance between the competency/skill level required and the specificity of the ISOxsm audit format. If experienced auditors from the internal audit group are used, a more open-ended "walk-through" format may be suitable. If ISO auditors, less-experienced in financial controls are used, then rather specific audit questions may be needed.

As an example, suppose the internal control relates to purchasing controls, specifically the approvals process. An experienced internal auditor may walk-through the entire flow of transactions/events from requisitioning through payment and beyond, requiring very little guidance. The less-experienced ISO auditor may need specific audit questions for each step in the walk-through sequence:

- trace 20 purchase orders "backwards", confirming the requisitions were generated per procedure, including the required signatures/approvals
- look at these 20 purchase orders for evidence of proper issuance per systems controls (e.g., using the pre-numbered manual forms)
- match-up purchase order information vs. Vendor Master information, including terms and unit price, etc.

In short, the audit questions need to be appropriate for the competence of those executing the audit.

An Example of an ISOxsm audit flow

- ISO Section 7.4 (Purchasing), audited within one or several major business processes
- Sequence of the “expanded” ISO audit in “walk-through” sequence
 - Purchasing requirements definition
 - Requisitioning
 - RFQs to potential suppliers
 - Controls over supplier/vendor selection
 - “Vendor Master” setup and controls
 - Purchase order approval and placement
 - Acknowledgement process
 - Revision/Update of purchase orders
 - Purchase materials receipt
 - Approvals to pay
 - Vouching
 - Payment
 - Payables relief
 - Into subsequent accounting activities (e.g., general ledger)

The ISOxsm audit often uses a combination of individual audit questions and “walk through” approach, often following a transaction from start to finish within the process being audited. The specific questions are integrated within the walk through of related transactions. The common denominator is the requirement.....each audit question ties back to either an internal control or to an ISO requirement. In some cases, a single audit question will cover both simultaneously.

As an example, a business typically will have purchasing (ISO section 7.4) embedded within one or more business processes. As section 7.4 requirements are audited in each process, the related internal controls related to the above will also be audited.

Examples of Specific ISOxsm Internal Audit Questions

- Look at a sampling of purchase orders for raw materials, subcontracted services, and capital equipment. Look for evidence that those purchase orders were issued to approved and/or qualified suppliers.
 - Ensure the vendor master information was entered with the proper approval and purchase amount authorization limits.
 - Look for evidence of an adequacy review of purchase information, including information of a commercial nature such as terms and FOB.
 - Look for approval or signatures by authorized parties and trace back the authorization to management policy, electronic controls, etc.
- Walk these transactions upstream/downstream to the physical receipt, receipt entry, accounts payable, vouching, payment, relief of the A/P, and handling of any associated debits (e.g., for items returned to the suppliers)

* As published in *Quality Digest*, April, 2006.

ISOxsm in Context

- The evolving nature of SOx 404 compliance
- The SEC and the PCAOB
- Some implementation issues to date
- How the SEC is addressing concerns

Sarbanes-Oxley 404 compliance is still very much a work in progress. Since its initial implementation with accelerated filers (larger public companies), there has been much discussion about the extent and expense of compliance. The SEC formed a special advisory committee focused on implementation on 404 for smaller and micro-cap companies.....those least able to bear the additional expense and burden of compliance. Their report, issued in April, 2006, acknowledges these concerns and proposes some remedies.

The ISOxsm approach was developed to help companies achieve the benefits of compliance without imposing additional overhead and diverting management attention from other basic business priorities.

Visit www.sec.gov for up-to-date information on 404 compliance requirements and developments.

Once the ISOxsm audit is over

- Management (CEO and CFO) can use the ISOxsm audit results to:
 - Determine next steps including further investigations into potential deficiencies
 - Support the required annual assertions about the effectiveness of internal controls
- The audit plan itself is evidence that management has reviewed the methods of assessing effectiveness and the overall design of the controls as reflected in the documentation and practices being audited.

Management bears the burden of determining the effectiveness of internal controls related to financial reporting and disclosing any material weaknesses. The more thorough the ISOxsm audit plan, auditing, and results reporting, the more management can rely on audit results as objective evidence in support of their assertions about effectiveness. This is further bolstered by the findings from the ISO registrars.

ISOxsm audit evidence for the public accounting firm

- Management will need to decide how best to work with the public auditor to maximize the usefulness of the ISOxsm audit results
- Including the public accountants in ISOxsm audit planning may increase the likelihood of acceptance, allowing them to reduce their auditing and testing
- Auditors ARE allowed to rely on much (not all) of internal work to offset their auditing

Artful planning and execution of the ISOxsm audit could help reduce the time and expense of the public accounting firm auditing of internal controls, as required by SOx.

Early involvement of the public auditors, especially in incorporating their previous findings and areas of concern, improves the chances that the public accounting firm will accept ISOxsm evidence in lieu of some of their own auditing and testing.

Other evidence from an ISO system :

Some Examples

- Evidence beyond internal auditing
- Dominant theme: Day to day operations are standardized and controlled, with documented responsibilities and accountabilities
- Evidence from the on-going operation of the ISO system
 - Management Review
 - Corrective Action System
 - Training and Communications
 - Record Keeping
 - Process Monitoring and Measurement

There is plenty of evidence of internal controls related to financial data from a typical ISO system. We have focused on the internal auditing, but both management and the public accountants may want to dig deeper.

Keep in mind that ISO systems all reflect a structure and discipline useful in demonstrating compliance. Day-to-day operations are standardized and controlled, with documented responsibilities and accountabilities. These controls are reflected in policies, procedures, work instructions, reporting and recording controls, and overall management involvement. The mandated management responsibilities (see ISO section 5 in particular) align with the “control environment” element of internal control.....one that is sometimes difficult to define and test. An ISO system tends to make the control environment much more visible.

What ISOxsm is Not:

- Does not attempt to address non-operational controls (e.g., accounting estimates, consolidating entries, etc.)
- Is not a replacement for good ethics
- Does not take the place of whistle-blower support systems or protections
- Does not establish what the internal controls should be .
- Does not replace what the public accounting firms are required, by law, to do

ISOxsm is a piece in the compliance puzzle, not the whole puzzle itself.

We have focused on the commonality between the ISO operational controls and the related financial controls. We all realize that some financial controls are not based on operational activities. Significant accounting estimates are a good example of this. The reliability of those estimates is usually outside the scope of an ISOxsm audit or existing ISO controls.

In addition, ISOxsm is not a replacement for ethical management or an involved board of directors. It will not prevent fraud, if someone is intent on “tricking” the system.

ISOxsm takes the list of internal controls as its starting point. ISOxsm does not attempt to identify what these controls should be.

ISOxsm certainly does not take the place of what public accounting firms are required, by the Sarbanes-Oxley law, to do. The public accounting firm is still responsible to conduct its own audit of internal controls, although ISOxsm evidence can be relied upon by the auditors to reduce their own testing.....a real potential cost-savings.

Summary

What ISOxsm is: A Practical Approach to Cost Effective Compliance

- The potential benefits revisited
- Extended advantages
 - Avoids duplicative audits
 - Cross-functional coordination
 - Shared responsibility outside of Accounting
 - Integrated, organization-wide corrective action, where necessary
 - Distributes the burden
 - Added credibility with third party registrar evidence

ISOxsm is a Practical Approach to Cost Effective SOx 404 Compliance

ISOxsm will save a company time and money if properly implemented. It lends credibility to management's assertions about the effectiveness of internal controls. It broadens the base of involvement in SOx compliance.

ISOxsm can have some spillover advantages that might not been so obvious at first glance.

- ISOxsm audits can avoid redundant internal audits.....different groups of audits covering the same subjects and causing frustration and irritation amongst those audited.

- Cross function coordination could improve simply as a result of more communication, understanding how an upstream or downstream activity is impacted by what happens elsewhere.

- People, including those outside of accounting, start to feel more accountability for controls

- The formal corrective action system, when used to address problems that impact internal controls, can increase the effectiveness of the solution.....a broader buy-in to fix problems with both operational and financial implications.

- ISOxsm distributes the burden of compliance and hopefully, the benefits of compliance

- The third party ISO registrar audits can increase in importance.....and credibility. Perhaps these audits will be viewed as an organization-wide responsibility (rather than the job of the ISO Management Representative to "get us through this" time after time).

Next Steps

- Where to start:
 - If you're senior management/CFO
 - If you're mid-level accounting management
 - If you're the firm's public accounting auditor
 - If you're the ISO Management Representative
 - If you just need some help.....

If ISOxsm seems like the right next for you, contact McAllister Consulting L.L.C.

By phone: 630-377-7300

By email: info@mcallister-consulting.com

By fax: 630-377-7324

By mail: McAllister Consulting L.L.C.
P.O. Box 760
Wayne, IL 60184