VOLUME 1

PriceWaterhouseCoopers ©
Sarbanes-Oxley Section 404 – An Introduction


The final rules will be effective for fiscal years ending on or after June 15, 2004 for SEC registrants with a public float $75 million; other than foreign private issuers; or for fiscal years ending on or after April 15, 2005 for other registrants, which includes small businesses and foreign private issuers.

Under Section 404, SEC registrants will be required to include with their annual filing:

• A statement of management’s responsibility for establishing and maintaining adequate internal control over financial reporting;
• A statement identifying the framework used by management to evaluate the effectiveness of internal control;
• Management’s assessment of the effectiveness of internal control as of the end of the company’s most recent fiscal year end; and
• A statement that the company’s external auditor has issued an attestation report on management’s assessment.

Canadian companies will be impacted by the new regulations in two ways. Foreign private issuers will be required to meet the new requirements starting in fiscal 2005. In addition, Canadian inbound subsidiaries of SEC registrants may be impacted by the new regulations for the 2004 fiscal year, based on the parent’s assessment of the materiality of the subsidiary, in terms of the company’s overall internal control structure.

The level of effort required by the audit team to conduct the attestation will depend primarily on the thoroughness of management’s own assessment, and the level to which it is formally documented. Therefore, it will be beneficial and necessary for management and the auditor to work closely together to prepare for these requirements. In addition, while the extended implementation period may now cause some companies to re-evaluate their current readiness plans, the reality is that companies will ultimately need to address the requirements of this section, and they should not wait until the last minute for preparation. The extension provides companies with the opportunity to address control weaknesses prior to going “live” with the required 404 reporting requirements, including the possibility of performing a “dry run” before the deadline.

Action Plan – A Suggested Timeline

<table>
<thead>
<tr>
<th>Major Project Activities</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Jul - Sept</td>
<td>Oct - Dec</td>
<td>Jan - Mar</td>
</tr>
</tbody>
</table>

- Project Initiation
- Documentation and Evaluation
- Remediation of Identified Gaps
- Attestation “Dry Run”
- Assertion and Attestation

A Roadmap for an entity to develop a Section 404:

1. Risk Assessment
2. Map Financial Statements line item to cycles/controls
3. Agree upon key risks and controls
4. Document existing processes (detailed flowcharts and narratives)
5. Identify controls in place
6. Gap Analysis
   • Identify weaknesses
   • Assess impact
   • Identify compensating controls
    • Fill gaps
7. Test controls for effectiveness
8. Gap Analysis
9. Deliver completed package

Some companies will be required to address substantial documentation of controls, including formal policy and manuals, etc. Most will not have completed the formal plan to address this.
The following conditions are necessary for an entity to be “auditable” under Section 404:

- Management accepts responsibility for the effectiveness of control
- Controls are suitably designed and implemented to achieve the control objective (reliability of financial reporting) using established criteria
- Control objectives and related controls need to be appropriately documented
- Management assesses the effectiveness of internal control over financial reporting and reports thereon (on both the design and operating effectiveness of controls)

Some companies may already have substantial documentation of their internal controls, including internal audit files, formal policy and accounting procedures manuals, etc. Most companies, however, will not have completed a comprehensive evaluation of their internal controls across the organization. In addition, the existing documentation may not be adequate to meet the demands of SOX 404. As such, virtually all organizations will require a formal plan to address the new regulations.

**Audit of Financial Statements versus 404 Controls Attestation**

**Audit of Financial Statements**
- Understanding and consideration of internal controls only to the extent necessary to develop the audit approach
- Overall objective is an opinion on the financial statements, not to opine on internal controls
- Internal control reports have been very rare in practice and are the subject of different attestation standards

**Section 404 Attestation**
- 100% controls-based approach. No comfort from substantive/analytical procedures
- Must evaluate and test controls across business and functional areas to opine on effectiveness (broader and deeper)
- Lack of errors, or material adjustment, historically, in financial statements is not de-facto evidence onto itself, of an appropriate internal control structure
The COSO Controls Framework

Monitoring
- Assessment of a control system's performance over time.
- Combination of ongoing and separate evaluation.
- Management and supervisory activities.
- Internal audit activities.

Control Environment
- Sets tone of organization-influencing control consciousness of its people.
- Factors include integrity, ethical values, competence, authority, responsibility.
- Foundation for all other components of control.

Risk Assessment
- Risk assessment is the identification and analysis of relevant risks to achieving the entity’s objectives—forming the basis for determining control activities.

Information & Communication
- Pertinent information identified, captured and communicated in a timely manner.
- Access to internal and externally generated information.
- Flow of information that allows for successful control actions from instructions on responsibilities to summary of findings for management action.

Control Activities
- Policies/procedures that ensure management directives are carried out.
- Range of activities including approvals, authorizations, verifications, recommendations, performance reviews, asset security and segregation of duties.

Internal Control Framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) was charged in the mid-1980's with the responsibility of defining an effective framework for systems of internal controls. Since its publication in 1992, the COSO framework has become widely accepted as the benchmark for establishing and assessing a structure for internal controls.

Section 404 reporting requires that management’s evaluation of internal controls be based on a suitable, recognized control framework that is established by experts using “due process”; a process which includes the broad distribution of the framework for public comment. COSO is recognized as an example of an acceptable framework that would meet these criteria. The definition of internal control used in the final regulations also makes reference to the COSO framework. Accordingly, it is widely agreed that the COSO framework will become the established benchmark for Section 404 reporting.

Under the COSO framework, “internal control” is defined as a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

COSO identifies five components of control (control environment, risk assessment, control activities, information and communication, and monitoring) that need to be in place and integrated to ensure the achievement of each of these three objectives. In preparing for Section 404 reporting, management will need to consider controls which address all five of these components.
Assessing Controls

The most effective way to meet the enhanced legal requirements of Section 404 will depend on the size, nature and complexity of the entity, including the quality of business processes and internal control systems. Accordingly, it is recommended that an evaluation of the controls and procedures be made by developing an internal control “maturity analysis” (see diagram below). An internal controls maturity analysis can make it easier for a company to evaluate how its existing control structure impacts the level of effort required to meet its control reporting requirements. In addition, the level of maturity can have a significant impact on the level of additional effort that will be required by management and the external auditor to meet SOX 404 requirements, which would require a level of at least “monitored” for significant controls.

Internal Controls Maturity Framework

- **Level 1 – Unreliable**
  - Unpredictable environment where controls are not designed or in place
- **Level 2 – Informal**
  - Controls are designed and in place but are not adequately documented
  - Controls mostly dependent on people
  - No formal training or communication of controls
- **Level 3 – Standardized**
  - Controls are designed and in place
  - Controls have been documented and communicated to employees
  - Deviations from controls may not be detected
- **Level 4 – Monitored**
  - Standardized controls with periodic testing for effective design and operation with reporting to management
  - Automation and tools may be used in a limited way to support controls
- **Level 5 – Optimized**
  - An integrated internal control framework with real time monitoring by management with continuous improvement
  - Automation and tools are used to support controls and allow the organization to make rapid changes to the control activities if needed

Companies with multiple business segments, geographic locations, or reporting units will need to determine which locations are relevant. Consideration should be given to the financial significance of the location, in terms of the potential for a material error, and the ability of the entity to commit the overall organization to financial risk. Specific risks that should be considered would include major systems changes, management turnover, a major acquisition, or a volatile business environment.

Individual locations or business units that are not individually significant may, when aggregated with other units, result in a group that could create a material misstatement. In this case, consideration should be given to whether there are entity-wide controls over this group of units that may provide comfort. The following diagram provides guidance on testing for companies with multiple locations:

Multi-Location Testing Consideration

- Is the location or business unit individually important? Yes
- Are there specific significant risks? Yes
- Are there locations or business units that are not important even when aggregated with others? No
- Are there document and entity-wide controls over this group? Yes

<table>
<thead>
<tr>
<th>Location Testing Consideration</th>
<th>Decision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Evaluate documentation and test significant controls at each location or business unit</td>
</tr>
<tr>
<td>No</td>
<td>Evaluate documentation and test controls over specific risk</td>
</tr>
<tr>
<td>Yes</td>
<td>No further action required for such units</td>
</tr>
<tr>
<td>Yes</td>
<td>Evaluate documentation and test entity-wide controls over group</td>
</tr>
<tr>
<td>No</td>
<td>Some testing of controls at individual locations or business units required</td>
</tr>
</tbody>
</table>
Section 404 Preparedness and Attestation

**Key Elements**

- **Project Initiation and Planning**
  - Form project charter: scope, objectives, core team
  - Develop project plan: milestones, deliverables
- **Risk Assessment and Prioritization**
  - Conduct risk assessment: identifying, prioritizing risks
- **Documentation**
  - Prepare inventory of existing documentation
  - Develop new documentation as needed
- **Evaluation**
  - Evaluate existing controls: assessment of gap analysis
  - Develop remediation plan: for identified gaps
- **Attestation of Internal Controls**
  - Complete 404 attestation: document assertions
- **Continuous Improvement**
  - Establish continuous improvement plan: for ongoing monitoring

**Deliverables and Work Projects**

- **Project Charter**
- **Project Plan**
- **Training Plan**
- **Communications Plan**
- **Project Team**
- **Inventory of existing documentation**
- **Templates**
- **Action Register**
- **External control evaluation findings**
- **Remediation plan**
- **Management reviews**
- **Attestation report**

Project Methodology

In evaluating internal controls for the Sarbanes-Oxley 404 certification process, PwC recommends an implementation plan for management that addresses the following critical tasks:

1. Form a project team to allocate responsibilities, assess resources, decide on an approach, and establish timing
2. Collect data on the current controls environment, by assessing areas of risk and reviewing existing practices
3. Prepare an inventory of existing and available documentation
4. Evaluate internal controls and prepare a gap analysis to identify areas of concern requiring further follow up
5. Remediate the identified gaps and validate that these areas have been fully addressed
6. Continue to monitor progress of remediation efforts towards sign-off of 404 assertions by management

The table above further indicates the key elements of a Section 404 project plan, and identifies responsibilities for both management and the external auditor.