Sarbanes-Oxley (SOX)

The Migration from Project to Process

Practical Actions for Getting Started

Jim DeLoach, Managing Director

November 7, 2006
## The Results So Far?

<table>
<thead>
<tr>
<th>Year</th>
<th>Opinions Filed</th>
<th>Adverse Opinions</th>
<th>Restated Opinions</th>
<th>Effective to Non-Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year 1</td>
<td>3,710</td>
<td>591 (15.9%)</td>
<td>90 (2.4%)</td>
<td>59 (10%)</td>
</tr>
<tr>
<td>(period ending prior to 11/15/05)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Year 2</td>
<td>2,895</td>
<td>194 (6.7%)</td>
<td>89</td>
<td>283 (9.5%)</td>
</tr>
<tr>
<td>(period ending 11/15/05 to 1/31/06)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Source:** AuditAnalytics.com – May 2006
SEC's Internal Control Weaknesses Remain

WASHINGTON -- …The Government Accountability Office said three material weaknesses in the SEC's internal controls, which were found in an audit of the SEC's 2004 financial statement, remained in place when the government-watchdog agency did its audit of the SEC's 2005 results.

….identified problems with computer security, tracking of fines and penalties, and preparation of financial results.

…. for some SEC line items, detailed information supporting the balances and underlying transactions weren't readily available and were hard to retrieve.

It recommended the agency beef up its financial-management office and procedures.

SEC Chairman Christopher Cox said his goal is to fully resolve material weaknesses involving financial-statement preparation and penalty tracking in fiscal year 2006, which ends Sept. 30.
First-year costs of Section 404 compliance were significant, ranging from .06% of revenues for companies in excess of $10 billion to 2.65% of revenues for companies with revenues of under $100 million.

Over 12% of first adopters reported material weaknesses, with an impact on shareholder value of generally less than 3%.

Approximately 70% of material weaknesses were related to financial accounting issues; another 14% of the issues pertained to personnel matters relating to poor segregation of duties, inadequate staffing; remaining disclosures related to IT controls, control environment or other matters.

First-year Section 404 compliance was not a model of efficiency.

– Some adopters waited too long to begin
– Standard-setters issued guidance during Q3
– Interpretations of standards differed among all parties involved
## Calendar Years 2001–2005 Restatements

### Restatement Issues (percentages based on total restatements)

<table>
<thead>
<tr>
<th>Year</th>
<th>Total Restatements</th>
<th>Restatement Issues</th>
<th>Debt, quasi debt, warrants, equity (BCF) issues</th>
<th>Deferred, stock-based, comp issues</th>
<th>Lease, legal, FAS 5 contingency issues</th>
<th>Revenue recognition issues</th>
<th>FAS 109 tax expense, benefit, deferral issues</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2005</strong></td>
<td>1541</td>
<td>Unique filers</td>
<td>1385</td>
<td>319</td>
<td>179</td>
<td>283</td>
<td>210</td>
</tr>
<tr>
<td></td>
<td></td>
<td>% of Year's Total</td>
<td>42.6%</td>
<td>20.7%</td>
<td>11.8%</td>
<td>18.7%</td>
<td>13.8%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>% of Category Total</td>
<td>42.0%</td>
<td>51.8%</td>
<td>44.4%</td>
<td>66.4%</td>
<td>31.5%</td>
</tr>
<tr>
<td><strong>2004</strong></td>
<td>763</td>
<td>698</td>
<td>123</td>
<td>81</td>
<td>61</td>
<td>153</td>
<td>85</td>
</tr>
<tr>
<td></td>
<td></td>
<td>% of Year's Total</td>
<td>16.1%</td>
<td>10.6%</td>
<td>8.0%</td>
<td>20.1%</td>
<td>11.1%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>% of Category Total</td>
<td>21.1%</td>
<td>20.0%</td>
<td>20.1%</td>
<td>14.1%</td>
<td>23.0%</td>
</tr>
<tr>
<td><strong>2003</strong></td>
<td>587</td>
<td>546</td>
<td>67</td>
<td>65</td>
<td>51</td>
<td>128</td>
<td>77</td>
</tr>
<tr>
<td></td>
<td></td>
<td>% of Year's Total</td>
<td>16.2%</td>
<td>11.4%</td>
<td>11.1%</td>
<td>8.7%</td>
<td>22.0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>% of Category Total</td>
<td>16.5%</td>
<td>10.9%</td>
<td>16.1%</td>
<td>11.8%</td>
<td>19.4%</td>
</tr>
<tr>
<td><strong>2002</strong></td>
<td>412</td>
<td>378</td>
<td>51</td>
<td>41</td>
<td>25</td>
<td>93</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td></td>
<td>% of Year's Total</td>
<td>11.4%</td>
<td>12.4%</td>
<td>10.0%</td>
<td>0%</td>
<td>23%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>% of Category Total</td>
<td>11.5%</td>
<td>8.3%</td>
<td>10.2%</td>
<td>0%</td>
<td>14%</td>
</tr>
<tr>
<td><strong>2001</strong></td>
<td>316</td>
<td>203</td>
<td>56</td>
<td>37</td>
<td>0</td>
<td>81</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td></td>
<td>% of Year's Total</td>
<td>8.7%</td>
<td>17.7%</td>
<td>11.7%</td>
<td>2.8%</td>
<td>25.8%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>% of Category Total</td>
<td>8.9%</td>
<td>9.1%</td>
<td>9.2%</td>
<td>2.1%</td>
<td>12.2%</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td><strong>3619</strong></td>
<td><strong>3300</strong></td>
<td><strong>616</strong></td>
<td><strong>403</strong></td>
<td><strong>434</strong></td>
<td><strong>636</strong></td>
<td><strong>405</strong></td>
</tr>
<tr>
<td><strong>% Total of all Restatements</strong></td>
<td></td>
<td></td>
<td><strong>17.0%</strong></td>
<td><strong>11.1%</strong></td>
<td><strong>12.0%</strong></td>
<td><strong>18.4%</strong></td>
<td><strong>11.2%</strong></td>
</tr>
</tbody>
</table>

Source: AuditAnalytics.com – as of April 25, 2006
Total number of Financial Restatements could increase by as much as 25% from 2005 to 2006 if this pace (year to date) continues

Source: AuditAnalytics.com – as of June 9, 2006
For companies who filed a financial restatement and had a clean 404 opinion from their auditors, there was a 184% greater likelihood that they would also be involved in securities class action litigation, as compared to those who had an adverse 404 opinion.

Source: AuditAnalytics.com – as of May 30, 2006
So, Where’s the Good News in all of This?

Good Sarbanes-Oxley Section 404 Internal Controls Corresponded with Higher Share Price Movement

SOX Year 2 Efforts Didn’t Get the Job Done

What We Know:

• Costs still exceed benefits
• Personnel are tired
• "Catch up" on important things was a priority
• Resource shortages continue to be acute
• Angst in the auditor relationship – auditors are tightening their approach
• It still takes longer than anticipated
• # of key controls is still THE cost driver
• Sole reliance on independent tests of controls remains THE "high cost" approach
SOX "Project to Process" – What are we talking about?

- SOX "Project to Process" is about the transition from an ad hoc project, which most first adopters experienced in Year 1, to a sustainable, cost-effective and value-added process over time.

- How do companies make "Project to Process" happen?
  - Think longer term giving consideration to the following:
    - Will the internal control structure continue to perform as significant changes occur?
    - Given the increased level of transparency within the financial reporting processes, do value-add opportunities exist?
    - Is the organization confident it is aligning the compliance process with a risk-based approach?
  - Make the right choice
  - Create value while improving sustainability
Create Value While Improving Sustainability – Overview

**ORGANIZATIONAL INFRASTRUCTURE**
- Re-evaluate prior year risk assessment
- Redefine scope of independent controls testing
- Re-assess testing emphasis
- Align Internal Audit plan with 404 test plan
- Review software options for documentation and workflow

**ACCOUNTABILITY & RESPONSIBILITY**
- Improve 404 and integrate 302 infrastructure
- Re-evaluate Year 3 certification process
- Manage critical relationships
- Improve and integrate enabling technologies
- Transform IAD program

**CHANGE RECOGNITION PROCESS**
- Institutionalize compliance
- Manage critical relationships
- Transform IAD program
- Optimize controls
- Re-engineer business processes

**ADD'L OPPORTUNITIES FOR IMPROVEMENT**
- Actively manage change
- Design Change Recognition Process
- Identify and Prioritize Improvement Opportunities
- Integrate with other risk management activities

**Implement self-assessment program**
Key to Cost-Effectiveness: Balancing the Sources of Evidence

- **Manual**
- **Detective**
- **Ad hoc**

**OPTIMIZE CONTROLS**

- **Systems-based**
- **Preventive**
- **Managed**

**Self-Assessment**

- Monitoring
- Automated Controls Testing
- Testing of Manual Controls

**Self-Assessment**

- Entity-Level Monitoring
- Process-Level Monitoring
- Testing of Automated Controls
- Testing of Manual Controls

**COST**

**SUSTAINABILITY**
• The role of technology or automation in regulatory compliance can be broken down into two parallel tracts:
  – Automation of the internal control environment
  – Automation of the compliance process
• Sustainability, reduction in costs, and improved value to the organization require advances in both.
• Significant advances can be made for many companies through better leverage of already acquired applications and tools.
The Evolution of Compliance Technology

- Integration of compliance frameworks, tools and data
- Portal access to personalized risk management information
- Proactive risk identification and evaluation

Enterprise Risk Management

Continuous Control Monitoring & Improvement

Control & Assessment Automation

Automation of Certification Process

Document Internal Controls

Value

Time

© 2006 Protiviti Inc.
The maturity of an organization’s IT processes goes hand-in-hand with its ability to implement automated controls and realize compliance and operational benefits.
### Critical Applications Supporting Financial Reporting

- Application 1
- Application 2
- Application 3
- Application 4
- Application 5
- Application 6
- Application 7
- Application 8
- Application 9
- Application 10
- Application 11
- Application 12
- Application 13
- Application 14
- Application 15

### IT General Control Processes

1. Define IT Strategy and Organization
   - 1.1 Develop and Maintain the IT Strategy
   - 1.2 Define and Manage the IT Organization
   - 1.3 Develop and Maintain the IT Governance Structure
2. Manage Security and Privacy
   - 2.1 Security / Privacy Strategy and Communication
   - 2.2 Administer Security (Add, Change, Delete Users)
   - 2.3 Manage Security Incidents
   - 2.4 Monitor Regulatory Compliance
3. Deploy and Maintain Solutions
   - 3.1 Manage Systems Development Life Cycle (SDLC)
   - 3.2 Develop and Maintain Application Interfaces
   - 3.3 Manage Application Changes
4. Manage IT Infrastructure
   - 4.1 Manage Data Center Operations
   - 4.2 Manage Technical Infrastructure
   - 4.3 Performance Planning and Monitoring
5. Manage IT Assets
   - 5.1 Manage IT Asset Requests
   - 5.2 Manage IT Asset Procurement
   - 5.3 Accounting for IT Asset Management
   - 5.4 Manage IT Asset Deployment
   - 5.5 Monitor IT Assets
   - 5.6 Manage Software Licensing and Compliance
   - 5.7 Manage Hardware Maintenance Agreements
   - 5.8 Manage Third-Party Agreements
   - 5.9 Manage IT Asset Retirement
6. Support End Users
   - 6.1 Manage Incidents
   - 6.2 Manage Problems
   - 6.3 Manage Service

### Assessment of Design and Operational Effectiveness

- **Number Processes for Documentation and Risk / Control Analysis:**
  - **240 Processes**
- **Controls to Test:**
  - **1,920 Controls**
- **Level of Effort:**
  - **15,360 Hours**

**Note:** Assumed 8 controls per process, 8 hours per control test for purposes of illustration.
Critical Applications Supporting Financial Reporting

Application 1
Application 2
Application 3
Application 4
Application 5
Application 6
Application 7
Application 8
Application 9
Application 10
Application 11
Application 12
Application 13
Application 14
Application 15

IT General Control Processes

4.1 Define IT Strategy and Organization
  4.1.1 Develop and Maintain the IT Strategy
  4.1.2 Define and Manage the IT Organization
  4.1.3 Develop and Maintain the IT Governance Structure

4.2 Manage Security and Privacy
  4.2.1 Security / Privacy Strategy and Communication
  4.2.2 Administer Security (Add, Change, Delete Users)
  4.2.3 Manage Security Incidents
  4.2.4 Monitor Regulatory Compliance

4.3 Deploy and Maintain Solutions
  4.3.1 Manage Systems Development Life Cycle (SDLC)
  4.3.2 Develop and Maintain Application Interfaces
  4.3.3 Manage Application Changes

4.4 Manage IT Infrastructure
  4.4.1 Manage Data Center Operations
  4.4.2 Manage Technical Infrastructure
  4.4.3 Performance Planning and Monitoring

4.5 Manage IT Assets
  4.5.1 Manage IT Asset Requests
  4.5.2 Manage IT Asset Procurement
  4.5.3 Accounting for IT Asset Management
  4.5.4 Manage IT Asset Deployment
  4.5.5 Monitor IT Assets
  4.5.6 Manage Software Licensing and Compliance
  4.5.7 Manage Hardware Maintenance Agreements
  4.5.8 Manage Third-Party Agreements
  4.5.9 Manage IT Asset Retirement

4.6 Support End Users
  4.6.1 Manage Incidents
  4.6.2 Manage Problems
  4.6.3 Manage Service

Assessment of Design and Operational Effectiveness

Number Processes for Documentation and Risk / Control Analysis:
  16 Processes

Controls to Test:
  128 Controls

Level of Effort:
  1,024 Hours

Note: Assumed 8 controls per process, 8 hours per control test for purposes of illustration.
Attain and Maintain

**Control Maturity**
- Control Automation
- Control Reliability
- Prevent / Detect Ratio

**Process (Maintain)**
- Turnover
- App Changes
- Process Changes
- Reorganization
- New Business Unit

**Cumulative Cost**
- Control Execution
- Internal / External Testing
- Remediation
- Tools / Implementation
In Summary - - It’s Time to Shift the Dialogue

<table>
<thead>
<tr>
<th>Institutionalize the Existing Internal Control Structure</th>
<th>Improve the Quality of the Internal Control Structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Leave financial reporting processes as is</td>
<td>• Improve process quality, time and cost performance</td>
</tr>
<tr>
<td>• Apply manual “find and fix” controls with unacceptable error rates</td>
<td>• Improve the processes upstream to eliminate defects at the source</td>
</tr>
<tr>
<td>• Underutilize configurable controls</td>
<td>• Optimize configurable controls</td>
</tr>
<tr>
<td>• Design and implement test plans around EXISTING controls</td>
<td>• Design and implement test plans around IMPROVED controls</td>
</tr>
<tr>
<td>• Apply a quantitative, coverage approach to scoping</td>
<td>• Apply a risk-based approach to scoping</td>
</tr>
<tr>
<td>• Test most of the controls tested last year</td>
<td>• Optimize key controls and rotate independent tests in low risk areas</td>
</tr>
<tr>
<td>• Apply detailed testing almost exclusively to validate effectiveness</td>
<td>• Also apply self-assessment and entity- and process-level monitoring</td>
</tr>
<tr>
<td>• Focus risk assessment on financial reporting risks</td>
<td>• Focus risk assessment more broadly on business risks (ERA)</td>
</tr>
</tbody>
</table>

“PASS/FAIL”

“PROCESS CAPABILITY”
At Protiviti, we believe the companies that most effectively understand and manage their risk are the companies that most often succeed. Or as we like to say…

Know Risk. Know Reward.™