SOX Refresh: It’s Time for a Change!

Kevin Rohrbach
Todd McCavit
TODAY’S SPEAKERS

Todd McCavit
Managing Director, Protiviti
IAFA

Kevin Rohrbach
Managing Director, Protiviti
IAFA
INTRO STORY

The Missing Person Who Joined Her Own Search Party

""
KEY INSIGHT

"One of the more interesting trends we have seen in our SOX research over the past decade is that the level of cost and effort has not decreased in any meaningful way for organizations. This would certainly not be in the expectation for those that have been involved in the process post PCAOB AS5 (over the last 10 years or so years) but it’s the reality today."
2019 KEY FINDINGS – SOX SURVEY

- SOX compliance costs are trending down, although they remain significant.
- Overall, SOX compliance hours continue to rise, with some significant variations.
- The use of automated controls testing is increasing, as is interest in deploying advanced technologies to enhance SOX compliance efficacy.
- More organizations are leveraging outside resources.
- Cyber security continues to influence SOX efforts.
Despite efforts and expectations to the contrary, the hours and level of commitment dedicated to SOX compliance have not decreased notably over the past decade.

External auditors’ scrutiny of compliance capabilities continues to change and intensify, largely due to the PCAOB’s ongoing refinement of auditing standards and related oversight activities in service of its mission to protect investors and the public interest by promoting informative, accurate and independent audit reports.

While it remains difficult to keep the SOX compliance burden constant — let alone reduce the hours and costs involved in the endeavor — the best opportunity to do so is through automation and the introduction of new SOX compliance approaches.
How has the internal control over financial reporting (ICFR) structure changed since SOX 404 (b) was required for your organization?

SOX compliance activities most impacted by the results of an External Auditors PCAOB inspection results.

- Systems reports and IPE
- IT considerations
- Evaluating deficiencies
- Cyber security controls
- Using the work of others (e.g. Internal Audit)
- Evaluating outsourced processes including SOC reports
PCAOB INSPECTION RESULTS

• PCAOB issued 153 inspection reports in 2018 and 45 through 6/20/19 for 2019.

• Eleven domestic firms were inspected annually in 2018
  – Six global network firms which audited 99% of total market capitalization of issuers from 2014 - 2016: BDO, Deloitte, E&Y, Grant Thornton, KPMG, PwC.
### INSPECTION OBSERVATIONS

#### AUDIT DEFICIENCIES

The most frequent audit deficiencies continue to be in the key areas of internal controls over financial reporting, assessing and responding to risks of material misstatement, and auditing accounting estimates. The 2018 results also indicate continued deficiencies around engagement quality reviews.

#### CYBERSECURITY

In approximately 10% of audits inspected, the company had experienced a cybersecurity incident. Auditors generally considered the incident in their risk assessments and modified their audit procedures to address the potential impact on relevant controls and the data generated by the company’s information technology systems.

#### SOFTWARE ASSISTED AUDIT

PCAOB gained insights into software audit tools used by firms and tools that are under development. These tools were used primarily as part of risk assessment and typically involved analysis of large volumes of transactions, such as revenue and journal entry testing.

#### NEW ACCOUNTING STANDARDS

Audit firms have revised their audit methodologies and conducted trainings around the new accounting standards. Firms continue to have regular interaction with management on the implementation of the new accounting standards.
INSPECTION IMPACT ON YOUR ORGANIZATION

The inspection process doesn’t just impact the audit firms but as the below results show, there is a downstream effect on companies and their associate SOX compliance costs. The selected items are the top three areas where companies have experienced the greatest impact to their costs.

- **Testing system reports and other information produced by entity (IPE)**
  - 24% Extensive
  - 26% Substantial
  - 29% Moderate
  - 14% Minimal
  - 7% None
  - **79% moderate or greater cost impact!**

- **IT considerations**
  - 17% Extensive
  - 29% Substantial
  - 37% Moderate
  - 9% Minimal
  - 8% None
  - **83% moderate or greater cost impact!**

- **Testing review of controls**
  - 15% Extensive
  - 28% Substantial
  - 33% Moderate
  - 17% Minimal
  - 7% None
  - **76% moderate or greater cost impact!**
GET THE BASICS RIGHT

Data Request - Generation:
• Timely, organized, easily accessible, accurate data request generation

Validate Controls are operating:
• Management should generally not be surprised by IA and external audit findings

Data Request Fulfillment:
• Assign someone to gather data requests and validate them

Use external audit templates:
• Maximize reliance and efficiency of your external auditor by using their templates
TESTING - TRY SOMETHING DIFFERENT

Test earlier

Test more often
PLANNING - TRY SOMETHING DIFFERENT

Plan earlier

Plan Strategically
Next-generation internal audit and, by extension SOX compliance 2.0, is about encouraging innovative thought into the audit process. In all aspects of internal audit, including but certainly not limited to SOX compliance work, we need to think about where we may be able to do things differently. Divergent thinking should be encouraged. We need to welcome disruption.
NOW EMERGING: SOX COMPLIANCE 2.0

The SOX compliance 2.0 technology toolkit is large. RPA, advanced analytics, AI, data visualization, GRC tools, process mining.

Data is the lifeblood of SOX compliance 2.0. The use of these tools hinges on data access and governance.

The entire compliance lifecycle is ripe for disruption and innovation.


Advance tools test a higher number of complete data sets, with far more exceptions likely to be identified.
### INCREASED USE OF TECHNOLOGY ENABLED TOOLS

<table>
<thead>
<tr>
<th>GRC / Workflow Tools</th>
<th>Process Mining</th>
<th>Robotic Process Automation</th>
<th>ITGC Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Creating a fully electronic SOX compliance process with real time documentation communication, and reporting</td>
<td>• The use of machine learning and artificial intelligence to construct how a process actually occurs based on application data</td>
<td>• Use of software tools, managed by appropriate business teams, to automate SOX compliance functions by executing rules-based tasks</td>
<td>• Cyber security tools that also benefit SOX compliance. Tools that assist with managing privileged access, passwords, user access, etc.</td>
</tr>
</tbody>
</table>
What is Process Mining?

Process Mining uses AI and machine learning to extract existing data from an organization’s IT systems to visually reconstruct how processes actually perform. The data shows what is actually happening and creates a complete process map.

How Can Process Mining Be Used In SOX?

• Automate the walkthrough process – replace interviews with advanced analytics and review process based on 100% populations.

• Data tells us what is actually happening – automatically identify process variants and complexities, identifying areas that do not comply with intended process design.

• Support risk assessment activities – identify “hot spot” areas, drive audit focus

• Make findings more impactful by quantifying the impact of non-conformance and benefits of adherence to consistent process.
HOW A CLOUD-BASE TOOL CHANGED SOX!

Client Problem

A large Oil & Gas producer was looking to move away from the manual SOX compliance process that had been in place since its IPO. At the time the company was using Microsoft Excel and Visio along with Adobe as its main tools for executing its SOX program. The organization’s control and process owners did not have the proper visibility into the controls and documentation that they were responsible for and the testing cycles were managed via a series of spreadsheets, email and shared drives. This led to a lack of insight of responsible control owners and inefficient manual efforts. The company evaluated the available tools in the market via a selection process and ultimately implemented AuditBoard.

Desired Enhancements

1. **Completely Electronic Compliance Process** – The Company’s Internal Audit group wanted to move away from relying on Microsoft Office products and into an environment that was 100% electronic and cloud based for all aspects of the compliance process.

2. **Seamless Communication** – The organization needed to have seamless and real time communication between the organizations Process Owners, Internal Audit team and External Audit team regarding the real time visibility into the state of controls, document requests, testing status, etc.

3. **Enhance the Experience of the Process Owners** – Real time communication with Process and Control Owners via a tool, workflow management, document repository for all requests and testing support, and the ability to maintain and update SOX documentation and controls in real-time across process map, narratives, RCMs testing lead sheets and dashboards.

Value Delivered

Through the implementation of AuditBoard’s SOXHub and Workstream modules the company was able to move its entire SOX compliance process into a cloud-based tool and the Internal Audit team is now able to manage the entire process via the tool including:

- Updating all documentation in a single place and have it flow through to all areas in the tool from narratives to RCMs to testing lead sheets
- Managing real-time status reporting, dashboards and integration with Microsoft O365 and PowerBI
- Managing documentation requests via Workstream, communicate with Process and Control Owners in real-time via the tool and provide support to the External Audits digitally as work is completed
- Enabling the company’s Process Owners with real-time visibility to their controls, testing status and results as well as allowing them to make updates as needed through out the year
- Facilitating the quarterly sub-certification process in the system via Workstream

© 2019 Protiviti – Confidential. An Equal Opportunity Employer M/F/Disabled/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
HOW OPTIMIZING CYBERARK HELPED REMEDIATE SIGNIFICANT IT CONTROL ISSUES!

**Client Problem**
A company was struggling to address security risks related to their management of privileged users. The customer had purchased CyberArk but were not getting value out of the deployment. After several years of issues, the issues were escalated for not adhering to existing access control policies around privileged access and failing to rotate passwords on privileged accounts. Finally, the existing set up was not configured appropriately to provide a back up of their privileged account data, meaning this data was at risk for data loss in the event of a system failure.

**Desired Enhancements**
1. PAM related industry best practices and industry standards implemented.
2. Access controls defined, communicated, and enforced around password policies and password management.
3. Privileged accounts for SOX systems put into a vaulted and managed state.
4. Managed accounts set for auto-rotation of passwords.
5. Disaster recovery implemented to develop preparedness and testing plan/schedule to execute procedures for failover in case of disaster.

**Value Delivered**
1. Roles around tool administration were redesigned and documented.
2. Customer’s procedures for reviewing privileged access improved.
3. Improved communication and coordination with account owners, safe owners and privileged users around the privileged account management process.
4. Within 3 months all SOX relevant privileged accounts were remediated and either moved into CyberArk’s PAM tool and into a vaulted and managed state or entitlements that made the account privileged were removed.
5. Training and Education sessions for CyberArk team and CyberArk end-users developed and delivered.
6. Disaster recovery procedures to ensure failover capabilities for CyberArk system availability (access to privileged account credentials) remediated.
7. Disaster recovery backup hardware installed and configured.
Face the Future with Confidence