Service Organization Control (SOC) Reports: Lessons Learned From Year Two
Your Presenter Today

- Sue Horn, CISA, CPA
  - Thought leader for Crowe SOC services
Agenda

- Overview of SOC (Service Organization Controls) Reporting Options
- Requirements of SOC Reporting Options for Service Organizations
- Lessons Learned During the Second Reporting Cycle of the SOC Standards: How You Can Improve Your Organization’s Reporting Process Going Forward
- Summary and Conclusion
- Q&A
Reasons for the Change

- Although used internationally for years, SAS 70 reports were issued (or at least signed and supervised) only by U.S. registered firms.
- Statement on Standards for Attestation Engagements (SSAE) 16, “Reporting on Controls at a Service Organization,” is the result of efforts by the Auditing Standards Board of the American Institute of CPAs (AICPA) to clarify its standards and to converge them with IAASB standards.
- Applying Statement on Auditing Standards (SAS) 70, “Service Organizations,” beyond financial reporting
- **AICPA Perspective:** Compliance with SSAE 16 does not result in an organization’s becoming “SSAE 16 certified” or gaining a certificate or designation.
Service Organization Controls (SOC) Reports – Overview

- The AICPA created separate reports on internal controls over financial reporting and reports on other types of controls.

- The AICPA has added reporting options.
  - The three reporting options now are:
    - SOC 1
    - SOC 2
    - SOC 3
  - Also note that AT 101, AT 201, and AT 601 are still in effect.
Types of SOC Reports

SOC 1
• Focused on internal controls related to financial reporting

SOC 2
• Report components similar to SOC 1’s
• Uses trust services principles

SOC 3
• Uses trust services principles
• General use report

SSAE 16 / AT 801
AT 101
## SOC Report Content

<table>
<thead>
<tr>
<th>SOC 1</th>
<th>SOC 2</th>
<th>SOC 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Service auditor’s report&lt;br&gt;• Management’s assertion&lt;br&gt;• Management’s detailed description of systems&lt;br&gt;• Details on the auditor’s tests of controls related to each control objective and results</td>
<td>• Service auditor’s report&lt;br&gt;• Management’s assertion&lt;br&gt;• Management’s detailed description of systems&lt;br&gt;• Details on the auditor’s tests of controls related to each selected trust services principle and results</td>
<td>• Service auditor’s report&lt;br&gt;• Management’s assertion&lt;br&gt;• Management’s summary description of its systems and the boundaries of the systems</td>
</tr>
</tbody>
</table>
Additional Reporting Options

- **AT 101**
  - Report is for entities that wish to report on controls over a specified set of criteria (not limited to financial transaction processing).
  - Report is for general use; report also could be restricted by the auditor.
  - Report may be as of a certain date, cover a time frame, or cover multiple periods.

- **AT 201**
  - Scope of the report is whatever management and the users of the report have agreed to with the auditor.
  - Users must agree to the procedures performed.
  - Distribution is limited to those who have formally agreed to the procedures.

- **AT 601**
  - Report is for entities that wish to report on controls over a specified set of criteria that are defined by an external party (for example, laws and regulations).
  - Use of the report is for general use. Reports also could be restricted by the auditor.
  - The report may be as of a certain date, cover a time frame, or cover multiple periods.
Which Report Should Be Chosen?

SOC Report Decision Tree

Will the report be used by your customers to evaluate controls related to financial reporting or SOX 404 key controls?

Yes -> SOC 1/SSAE 16 Report
No  -> Do your customers need a report on controls related to system security, availability, processing integrity, confidentiality and/or privacy in order to perform proper oversight or vendor management activities?

Yes -> AT 101 Report
No  -> Do your customers have the need to review a detailed description of your control environment, the tests performed by the service auditor, and the results of those tests?

Yes -> SOC 2 Report
No  -> SOC 3 Report
SOC 1 and SOC 2 Report Reviews
Who May Need to Issue a SOC 1 Report

- SSAE No. 16 is applicable when an entity outsources a business task or function to another entity (usually one that specializes in that task or function), and the data resulting from that task or function is incorporated in the outsourcer’s financial statements.

- Some examples of service organizations:
  - Companies that develop and host banking software
  - Outsourced payroll processors
  - Banks offering trust and investment services
  - Medical claims processors
  - Companies that compute commission payments for a sales team
Who May Need to Issue a SOC 2 Report

• Organizations that need to demonstrate how they process transactions and/or data on behalf of their customers
• Organizations that need to demonstrate how their security controls operate
• Organizations that need to demonstrate how their controls related to system availability operate
• Organizations that need to demonstrate how their controls related to data privacy or confidentiality operate
SOC 2 – Trust Services Principles

**Security** – The system is protected against unauthorized access (both physical and logical).

**Availability** – The system is available for operation and use as committed or agreed to.

**Processing Integrity** – System processing is complete, accurate, timely, and authorized.

**Confidentiality** – Information designated as confidential is protected as committed or agreed to.

**Privacy** – Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity’s privacy notice and with criteria set forth in generally accepted privacy principles (GAPP) issued by the AICPA and the Canadian Institute of Chartered Accountants (CICA).
Relationship Among Principles, Criteria, and Controls
Benefits of SOC 2 Reports

- Oversight
- Vendor management programs
- Internal corporate governance
- Risk management
- Reduction in audits performed by user organizations
Quick Recap – SOC Report Sections

SOC 1 and 2 Report Sections

- Service Auditor Opinion
- Management Assertion
- Description of Systems
- Test Results
- Complementary Controls
- Other Information
Quick Recap – Service Organization Responsibilities (SOC 1 and SOC 2)

- Provide a “description of its system.”
- Specify the control objectives and trust services principles of the system and include them in the description of the system.
- Provide a written assertion in the report.
- Have a basis for providing the assertion.
- Identify the criteria used in preparing the description, evaluating whether the controls are suitably designed to meet the control objectives/applicable trust services principles, and evaluating whether the controls are operating effectively.
- Identify the risks that threaten the achievement of the control objectives.
- Design, implement, and maintain controls to provide reasonable assurance that the control objectives and applicable trust services principles will be achieved.
Lessons Learned From Year Two
Lessons Learned: Selection of the Report Type and Coverage Period

Service organizations had less challenges with the report type and coverage selections; however, there were still challenges with SOC 2 reports.

**Recommendations:**

- Select a report type that best fits the user organization’s needs.
  - financial reporting, vendor management, etc.
- Select areas of coverage that user organizations are concerned with.
  - Understand the topics that are important to user organizations.
- Select a time frame that meets the needs of user organizations.
  - SOC 1 Report – six months (required for reliance in conjunction with financial statement audits)
  - SOC 2 Report – at least two months
- Understanding and evaluating the need of a SOC 2 report and the trust principles to be included.
Lessons Learned: *Basis for the Assertion*

Service organizations had better organized and better prepared management assertions and the basis for the assertions however, they are still a work in process.

**Recommendations:**

- The basis for management’s assertion should be in draft format at the beginning of the SOC report time frame.
- Organizations can take several different approaches to develop the basis for their assertion.
  - Organizations may want to ensure that 90% to 100% of the controls supporting the selected control objectives are monitored internally.
  - Organizations may want to ensure that one or two critical controls per control objective are monitored internally.
  - Monitoring procedures may vary from ongoing internal monitoring controls to operating effectiveness testing procedures.
- Management also should develop processes to update the basis tracking documentation frequently.
  - Frequent updates allow management to proactively identify controls weaknesses and to ensure that monitoring procedures are in place.
Lessons Learned: *Risk Assessment*

Service organizations had better documented and more effective risk assessments.

*Recommendations:*

- The risk assessment performed by management should be in draft format at the beginning of the SOC report time frame.

- The risk assessment should be updated during the SOC reporting time frame to reflect changes in risks and monitoring activities.

- Risk identification should be focused on the content covered in the report.
Lessons Learned: *Description of Systems*

Service organizations effectively increased the information included in the description of systems.

**Recommendations:**

- The description of systems should clearly describe the services performed, types of transactions processed, processing flow of transactions, and reporting methods.

- Enough detail should be included in these sections so that user organizations can clearly understand the service provider’s operations and control procedures.

- **A simple rule of thumb might help:** If the service or software application being described were being run internally by the client, what kinds of controls would be in place – and does the service organization have them?
Lessons Learned: Documentation of Significant Changes

Communication of significant changes to service auditors improved as more touch points were taking place.

Recommendations:

- Have standard touch points with the service auditor throughout the time frame to identify significant changes.

- From initiation to completion, ensure that significant changes are documented, so that all critical steps can be captured accurately for evaluation by the users of the report.

Examples:

- A service organization implements a new system to record change-control information to replace its existing system.
- A service organization moves its physical computer systems to a new location.
Lessons Learned: Complementary User Entity Controls

Communication of complementary user entity controls to user organizations improved.

Recommendations:

• Service organizations should thoroughly evaluate the responsibilities of user organizations so that a complete listing of user entity control considerations can be developed.

• In order to develop this listing, service organizations should refer to current company practices and contractual obligations.
Lessons Learned: Subservice Organizations

An increase in the disclosures of subservice organizations occurred in year one of the SOC reporting standards and continues to increase in year two.

Recommendations:

- Service organizations should include additional information in the description of systems to describe how the subservice organizations used by the service provider are monitored.
- Typically, subservice organizations that are critical to a service provider’s environment were carved out of the service provider’s report due to the reporting requirements contained in the standard.
Lessons Learned: *Performing an Interim Visit and Better Organization of Service Auditor Requests*

There has been an increase in requests by clients for interim visits.

**Recommendations:**

- An interim visit helps prevent surprises. Service organizations should consider requesting an interim visit.
  - If controls are broken, it allows organizations to remediate.
    - Note: Any controls identified as broken during the time frame would be reported in the SOC report.
- Request information to be housed in one system/location
Lessons Learned: *Reliance on Internal Audit*

Service organizations continued to look for ways to decrease audit costs and duplication of testing by requesting the service auditor to rely on the work performed by Internal Audit:

*Recommendations:*

- Request that your service auditor evaluate your internal audit program and develop a plan to place reliance on the testing that has already been performed.

- Work performed by Internal Audit can be relied upon to improve efficiency in the audit process.
Summary and Conclusion

**Lessons Learned**

- Service organizations had less challenges with the report type and coverage selections; however, there were still challenges with SOC 2 reports.
- Service organizations had better organized and better prepared management assertions and the basis for the assertions however, they are still a work in process.
- Service organizations had better documented and more effective risk assessments.
- Service organizations effectively increased the information included in the description of systems.
- Communication of significant changes to service auditors improved as more touch points were taking place.
- Communication of complementary user entity controls to user organizations improved.
- An increase in the disclosures of subservice organizations occurred in year one of the SOC reporting standards and continues to increase in year two.
- There has been an increase in requests by clients for interim visits.
- Service organizations continued to look for ways to decrease audit costs and duplication of testing by requesting the service auditor to rely on the work performed by Internal Audit.
Summary and Conclusion

**Predictions and Suggestions:**

- Planning and preparation for the examination is, and will continue to be, critical to the process.
- The process will be less disruptive throughout the audit. The use of technology will be one of the keys to minimizing disruption.
- Multiple types of reports will be provided.
- The number of SOC 2 reports will increase.
- The work of Internal Audit will be used to cut costs.
- More disclosures (such as from subservicers) and additional information will be required.
Questions?
For more information, contact:

Sue Horn
614.365.2236
sue.horn@crowehorwath.com