OBJECTIVES

- History
- What is a SOC report?
- Differences between SOC 1 and 2
- When to request and accept each
- What should be included in each
- What to ask as you read
WHAT IS SOC?

SOC – originally “Service Organization Controls”
SOC – 2016 updated to “System and Organization Controls”
SOC – not to be confused with “Security Operations Center”
SOC – not to be confused with “SOX” (aka Sarbanes-Oxley)
WHAT IS A SOC REPORT?
WHAT IS A SOC REPORT?

What is a SOC report?
A SOC report is intended to provide an independent opinion on various types of internal controls at service organizations or on discreet “systems”.

What is a service organization?
An organization that provides services to another organization
Example: Payroll processing company
Example: Claims processing company
Example: Software as a Service provider
WHAT IS A SOC REPORT?

The Players.....

*Service organization* – the entity that provides services to a user organization that are part of the user organization’s information system

*User organization* – the entity that has engaged a service organization to perform certain functions

*User auditor* – The auditor who reports on the financial statements of the user organization
A HISTORY LESSON

April 1992 – AICPA issues SAS 70 in response to pressure from service organizations that were being overwhelmed by audits

• Allowed one internal control review to be performed on service organization to examine all of the areas required to meet SAS 55 requirements

• Resulting service auditor's report (aka SAS 70) can be distributed and relied upon by all of the financial statement auditors of the service organization’s clients
A HISTORY LESSON

May 2011 - AICPA issues SSAE 16

- “SSAE 16 is the new SAS 70”
- SOC 2 and SOC 3 introduced after SOC 1 (SSAE 16)
- Confusion abounds!!!

When did you first hear about SOC reports?
Who can tell me the difference between SOC 1 and SOC 2?
“NEW” STANDARDS FOR THIRD PARTY AUDITS
SOC 1 – SSAE 16 – intended for ICFR
SOC 2 – AT 101 - based on pre-defined controls “principles”:
• Security
• Availability
• Processing Integrity
• Confidentiality
• Privacy
SOC 3 – Condensed and abbreviated SOC 2 report
• Includes auditor opinion and Management’s assertion
• AICPA seal can be displayed
• General availability
April 2016 - AICPA issues SSAE 18

- Consolidation of SSAE 16 and many other SSAEs
- Intended to be the standard for many different types of attestation report
- Confusion abounds!!! (Again)
So is it now a SSAE 18 report?

**NO!!!!!!**

SSAE 18 is the name of the standard under which the report is produced. The name of the report is a SOC report, or more specifically, SOC 1, SOC 2 or SOC 3
<table>
<thead>
<tr>
<th></th>
<th>Who are Users?</th>
<th>Why?</th>
<th>What?</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC 1</td>
<td>Management, user entities, and user auditors</td>
<td>Financial statement audit (ICFR)</td>
<td>Controls relevant to user entity ICFR</td>
</tr>
<tr>
<td>SOC 2</td>
<td>Management, user entities, Regulators, others</td>
<td>GRC programs, cybersecurity programs, compliance, due diligence</td>
<td>Controls relevant to Security, Availability, Processing Integrity, Confidentiality, Privacy</td>
</tr>
<tr>
<td>SOC 3</td>
<td>Any reader with a need for confidence in controls</td>
<td>General release, “GoodHousekeeping seal of Approval”</td>
<td>Same as SOC 2</td>
</tr>
</tbody>
</table>
CURRENT STATE

- SOC 1 - Report on Controls at a Service Organization *Relevant to User Entities’ Internal Control over Financial Reporting*
- SOC 2 - Report on Controls at a Service Organization Relevant to *Security, Availability, Processing Integrity, Confidentiality or Privacy*
SOC 1 - Report on Controls at a Service Organization Relevant to User Entities’ Internal Control over Financial Reporting

Services provided by a service organization are relevant to the audit of a user entity’s financial statements when those services and the controls over them affect the user entity’s information system. A service organization’s services are part of a user entity’s information system if the services affect any of the following:

- The classes of transactions in the user entity's operations that are significant to the user entity’s financial statements
- The procedures within both IT and manual systems by which the user entity’s transactions are initiated, authorized, recorded, processed, corrected as necessary, transferred to the general ledger, and reported in the financial statements
- The related accounting records, supporting information, and specific accounts in the user entity’s financial statements used to initiate, authorize, record, process, and report the user entity’s transactions
- How the user entity’s information system captures events and conditions, other than transactions, that are significant to the financial statements
- The financial reporting process used to prepare the user entity’s financial statements, including significant accounting estimates and disclosures
- Controls surrounding journal entries, including nonstandard journal entries used to record nonrecurring, unusual transactions, or adjustments
CURRENT STATE

- **SOC 2 - Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy**
  - **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.
  - **Processing integrity** - System processing is complete, accurate, timely, and authorized.
  - **Confidentiality** - Information designated as confidential is protected as committed or agreed.
  - **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 CICA.
POP QUIZ

- True or False?
  SOC 1 and SOC 2 are both examples of SSAE 18 reports

- True or False?
  For the SOC reports that your organization receives, your organization is the service organization.
Customer auditor wants SSAE 16 or SOC “X”

Procurement relies on auditor

Service organization wants business

Service auditor wants the business
How to Read SOC 1

- Review control objectives – are they applicable?
- Review control activities – do they support the control objectives?
- What’s missing?
  - e.g. – if change controls are important due to custom software being used, are they covered?
- Remember: the service organization determines what controls are important to the user.
Sample review

III. DESCRIPTION OF THE ServOrg SYSTEM USED TO MANAGE AND CONTROL CASH MANAGEMENT AND ACCOUNTING SOLUTIONS SERVICES .............................................. 5
Overview of Services Provided ....................................................................................... 5
Description of Relevant Transactions Processed ............................................................. 5
Control Environment Elements ....................................................................................... 7
Risk Assessment .............................................................................................................. 9
Monitoring ...................................................................................................................... 9
Information and Communication Systems ....................................................................... 9
Description of General Control Activities ..................................................................... 9
Physical Security ........................................................................................................... 9
Logical Security ............................................................................................................. 10
Network Security ......................................................................................................... 10
Data Integrity and Security .......................................................................................... 11
Security Violation Monitoring and Reporting ............................................................... 12
Change Management .................................................................................................... 12
Data Backup and Recovery .......................................................................................... 13
Organization and Administration .................................................................................. 14
Description of Application Control Activities ............................................................... 14
New Client Set Up and Implementation ....................................................................... 14
Incoming Fund Controls ............................................................................................... 15
Fund Processing Controls ............................................................................................ 16
Outgoing Fund Controls ............................................................................................... 17
Complementary User Entity Control Considerations ................................................... 18
Sample review

Control Objective 6 – Controls provide reasonable assurance that data integrity is maintained through various stages of processing in accordance with user specifications.

<table>
<thead>
<tr>
<th>Controls specified by ACME</th>
<th>Tests performed by Big 4, LLP</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IT Director is solely responsible for maintaining all archive and backup systems.</td>
<td>Inquired and reviewed archive and backup policies and procedures with the IT Director</td>
</tr>
<tr>
<td>Reports are generated detailing job statistics and exceptions, if any, for daily backup</td>
<td>Examined a sample of backup reports for successful completion of backup jobs.</td>
</tr>
<tr>
<td>procedures for each server.</td>
<td></td>
</tr>
<tr>
<td>Media tapes are used to execute the backup procedures</td>
<td>Verified the condition of the on-site media tapes.</td>
</tr>
<tr>
<td>Offsite storage is provided by Iron Butterfly Data Services, Inc.</td>
<td>Examined acknowledgement receipts from the offsite storage provider.</td>
</tr>
<tr>
<td>Conclusion: No exception noted.</td>
<td></td>
</tr>
</tbody>
</table>
Sample review

**B: Facility and Environmental Protection Control Objective** — Controls provide reasonable assurance that DC facilities housing customer equipment are engineered and monitored such that each element of the computing environment is compliant with customer contractual specifications.

<table>
<thead>
<tr>
<th>Controls specified by ACME</th>
<th>Tests performed by Big 4, LLP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>B1</strong> Power management, fire detection and suppression, and temperature and humidity control equipment is in place to provide ongoing environmental protection.</td>
<td>Observed the environmental protection units (power management, fire detection and suppression, and temperature and humidity control) in place at the IO’s facilities. Selected a sample of environmental protection units placed in critical data center locations and noted that these units were operating as designed.</td>
</tr>
<tr>
<td><strong>B2</strong> Building Management System(s) (BMS) are used to monitor all environmental controls and alert data center staff of any potential issues.</td>
<td>Observed the existence and operation of a building management system used to monitor environmental protection units placed throughout critical areas of the facility.</td>
</tr>
<tr>
<td><strong>B3</strong> IO staff performs and logs daily visual checks of power, environmental, and other system controls including battery and fuel monitoring systems.</td>
<td>Selected a sample of facilities monitoring logs and noted that monitoring was performed for power, environmental and other system controls of the facility.</td>
</tr>
</tbody>
</table>

Conclusion: No exception noted.
How to review SOC 2

- Are all appropriate TSCs covered?
  - E.g. – if information confidentiality is important to your arrangement with the SO, is it covered?
- Are any criteria identified as N/A? Do you as a user agree?
- Are all elements included?
How to review SOC 2

Elements that should be included:

i. The types of services provided

ii. The components of the system used to provide the services, which are the following:
   
   (1) *Infrastructure*. The physical and hardware components of a system (facilities, equipment, and networks).
   
   (2) *Software*. The programs and operating software of a system (systems, applications, and utilities).
   
   (3) *People*. The personnel involved in the operation and use of a system (developers, operators, users, and managers).
   
   (4) *Procedures*. The automated and manual procedures involved in the operation of a system.
   
   (5) *Data*. The information used and supported by a system (transaction streams, files, databases, and tables).

iii. The boundaries or aspects of the system covered by the description

iv. How the service organization’s system captures and addresses significant events and conditions\(^\text{19}\)

v. The process used to prepare and deliver reports and other information to user entities and other parties

\(^\text{19}\) For example, the setup of access rights for new users of the system.
## Sample review

<table>
<thead>
<tr>
<th>Controls specified by ACME</th>
<th>Tests performed by Big 4, LLP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3.2:</strong> Procedures exist to restrict logical access to the defined system including restriction of access to offline storage, backup data, systems, and media.</td>
<td>This criterion is not applicable due to the fact that the scope of the examination is limited to the entity’s colocation services.</td>
</tr>
<tr>
<td><strong>3.4</strong> Procedures exist to protect against unauthorized access to system resources.</td>
<td>A user ID and password is needed to access system resources. Login sessions are terminated after six consecutive unsuccessful login attempts.</td>
</tr>
<tr>
<td><strong>3.13</strong> Procedures exist to provide that only authorized, tested, and documented changes are made to the system.</td>
<td>This criterion is not applicable due to the fact that the scope of the examination is limited to the entity’s colocation services.</td>
</tr>
</tbody>
</table>

Conclusion: No exception noted.
User Entity Controls

This section of a SOC report describes other internal controls that should be in operation at user organizations to complement the control structure policies and procedures at the service organization. User auditors should consider whether the listed controls have been placed in operation at user organizations. Examples of User Entity Controls:

- Clients are responsible for ensuring that changes to processing options are appropriately authorized, implemented, and approved.
- Clients are responsible for reviewing reports that are prepared and distributed on an ad-hoc or scheduled basis that relate to claims payments and eligibility status.
- Clients who submit or manage eligibility are responsible for the accuracy of the data, the complete transmittal of the data, and the need to maintain all applicable encryption protocols on their end.
- Clients who maintain eligibility are responsible for enforcing new hire eligibility rules. SO will enforce rules as provided to us by the client at the time of client installation.
- Providers, who submit claims, either electronically or via paper, are responsible for providing complete information in order for the claim to be processed without manual intervention.
True or False?

A SOC 1 report from a service organization that has no exceptions assures that controls are adequate and operating effectively.
You are getting ready to sign a contract for a new Payroll application that is offered via the cloud (SaaS). They utilize a third party colocation facility for their application offering.

- Do you need to request a SOC report?
- If so, which one?
David Barton

Six Concourse Parkway
Suite 1700
Atlanta, GA 30328
678-602-4400

@itcontrolsfreak – twitter
itcontrolsfreak.wordpress.com - blog