Who Is Schneider Downs?

- Top-60 public accounting firm in the United States. We have clients worldwide, but our primary service area includes OH, PA, MI and WV.
- Headquartered in Pittsburgh, PA; second office in Columbus, OH.
- Highly specialized risk advisory services team with heavy experience in third-party risk management, SOC reporting, internal audit outsourcing, cybersecurity, etc.
- Our team has combined experience working on more than 500 service auditor examinations.

Who Are We – Dan Desko

- CISA, CISSP, CTPRP (Certified Third Party Risk Professional)
- 12 years of experience, part in IT, part in security and risk consulting
- Currently, Senior Manager of Risk Advisory Services at Schneider Downs
- SD SOC practice leader, manager of multiple SOC engagements
- Experience in delivering vendor risk management services to multiple industries (healthcare, education, financial services, etc.)
- Current ISACA Pittsburgh Chapter President
- Serves on multiple committees for the Shared Assessments Group.
Who Are We – Troy Fine

- CISA, CPA, CITP (Certified Information Technology Professional)
- Eight years experience as a business intelligence consultant and a security and risk consultant
- Currently, Manager of Risk Advisory Services at Schneider Downs
- Areas of Focus – SOC 1 and 2, SOX, HIPAA, HITRUST, ISO27001, PCI
- Member of the AICPA's CITP Credential Committee
- Ohio State Alum

Goals For Today

- Cover the SOC Report Basics
  - Types of reports
  - Types of service organizations
- Understand the Impact of SSAE 18
- Understand the Impact of SOC 2 Updates
- Understand the Major Components of a SOC Report and How to Review
- Share Lessons Learned

SOC Report Basics

<table>
<thead>
<tr>
<th>Report</th>
<th>Type of Report</th>
<th>Additional Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC 1</td>
<td>System and/or Financial Reporting</td>
<td>Detailed report for systems and financial controls specified by the service organization.</td>
</tr>
<tr>
<td>SOC 2</td>
<td>System and/or Financial Reporting</td>
<td>Detailed report for systems and financial controls specified by the service organization.</td>
</tr>
<tr>
<td>SOC 3</td>
<td>Security, Availability, Processing Integrity, and Confidentiality</td>
<td>Detailed report for systems and identified areas with controls specified by the service organization.</td>
</tr>
<tr>
<td>SOC 4</td>
<td>Security, Availability, Processing Integrity, and Confidentiality</td>
<td>Same as above without disclosing detailed controls and testing.</td>
</tr>
<tr>
<td>SOC 5</td>
<td>Security, Availability, Processing Integrity, and Confidentiality</td>
<td>Same as above without disclosing detailed controls and testing.</td>
</tr>
</tbody>
</table>
SOC Report Basics

• **Type 1** – Report on the suitability of design of controls
• **Type 2** – Report on the suitability of design and operational effectiveness of controls
• Report Types
  – SOC 1, Type 1
  – SOC 1, Type 2
  – SOC 2, Type 1
  – SOC 2, Type 2
  – SOC 3

SOC Report Basics

• Types of services organizations (SOC 1)
  – Bank Trust Department
  – Claims Processor
  – Investment Management Firm
  – Payroll Providers
  – Third-Party Administrators
  – Hosted Financial Management Systems

SOC Report Basics

• Types of services organizations (SOC 2)
  – SaaS Providers
  – Application Hosting Provider
  – Cloud Storage Provider
  – Cloud Code Management Software
  – Cloud Document Management Solutions
  – Email Hosting Provider
  – Cloud Data Analytic Solutions
  – Data Centers
  – Cloud Help Desk Management Software
  – Cloud Customer Relationship Management Solutions
SOC 2+ Reports

- Service auditor can express an opinion on both the AICPA’s Trust Services Criteria “plus” additional subject matter (ISO27001, HITRUST, PCI, NIST 800-53, etc.)
- Report must contain a modified assertion by management of the service organization
- Service auditor’s opinion must be modified for the additional compliance framework

SOC 2+ HITRUST Example

- AICPA and HITRUST collaborated to develop and publish guidance to streamline performing SOC 2+ HITRUST engagements
- Work products include:
  - Mapping of CSF to Trust Services Principles and Criteria
    - Security
    - Confidentiality
    - Availability
- SOC 2+ HITRUST Reporting Template
- Practitioner document with frequently asked questions

Why a SOC 2+ Report?

- Benefits to report issuers:
  - Time and cost savings
  - Gain efficiencies
- Benefits to report recipients:
  - Use one report to meet their requirements
  - Testing performed one time by the same audit firm
  - Common format that they are used to seeing
  - Easily map SOC 2 criteria to additional subject matter
SSAE 18 Overview

• Supersedes SSAE 16 and AT 801
• Effective date
  – SOC reports dated on or after May 1, 2017
• No significant changes
  – May require adjustments to management’s description
  – May require service auditor to adjust testing approach

Impact on Service Organizations

• Enhances requirement for monitoring subservice organizations
• Required to provide additional evidence to support completeness and accuracy of information provided to service auditor
• System description must include complementary subservice organization controls

Impact on Service Auditors

• Internal audit more clearly defined
• Requires evaluation of completeness and accuracy of evidence provided by service organization
• Obtaining an understanding of the service organization’s system and assessing the risk of material misstatement.
SOC 2 Update

• TSC (Trust Services Criteria)
  – The underlying subject matter for a SOC 2 report.
• Effective Date
  – SOC reports issued on or after June 15, 2018
• Key changes
  – Restructures and aligns the TSC with the COSO 2013 framework
  – Renames the Trust Services Principles and Criteria
  – Restructures and adds supplemental criteria to better address cybersecurity risks in engagements using the TSC
  – Adds points of focus to all TSC

COSO Principle Example

DEFG
COSO Principle 27: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

The following points of focus, specific to the COSO 2013 framework, highlight important characteristics relating to this criterion:

• Business Risk — Management and the board of directors, in an appropriate, timely manner, respond to reports of deficiencies and trends and take actions as necessary.
• Security Risk — Deficiencies are communicated by parties responsible for taking corrective action within an appropriate, timely manner and the board of directors, as appropriate.
• Access Control Deficiencies — Management tracks whether deficiencies are remediating in a timely basis.

Supplemental Criterion Example

DEF
COSO Criterion 27: Ensure that access to data, applications, and systems is in accordance with applicable policies, procedures, and standards. The following points of focus, specific to engagements using the trust services criteria, highlight important characteristics relating to this criterion:

• Entity Access to Data — Ensures that access to data is in accordance with applicable policies and procedures. This is achieved through the use of physical security and other controls, such as access controls for data centers, network access controls, and other administrative controls.
• System Access Policy Controls — The appropriate degree of trust in systems, such as access controls for data centers, network access controls, and other administrative controls, is maintained.
• System Access Controls — The appropriate degree of trust in systems, such as access controls for data centers, network access controls, and other administrative controls, is maintained.
• User Access Policies Controls — The appropriate degree of trust in systems, such as access controls for data centers, network access controls, and other administrative controls, is maintained.
**Control Environment**

- **CC1.1 - COSO Principle 1:** The entity demonstrates a commitment to integrity and ethical values.
- **CC1.2 - COSO Principle 2:** The board of directors demonstrates independence from management and exercise oversight of the development and performance of internal control.
- **CC1.3 - COSO Principle 3:** Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
- **CC1.4 - COSO Principle 4:** The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
- **CC1.5 - COSO Principle 5:** The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

**Communication and Information**

- **CC2.1 - COSO Principle 13:** The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
- **CC2.2 - COSO Principle 14:** The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
- **CC2.3 - COSO Principle 15:** The entity communicates with external parties regarding matters affecting the functioning of internal control.
Risk Assessment

- **CC3.1 - COSO Principle 6:** The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

- **CC3.2 - COSO Principle 7:** The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

- **CC3.3 - COSO Principle 8:** The entity considers the potential for fraud in assessing risks to the achievement of objectives.

- **CC3.4 - COSO Principle 9:** The entity identifies and assesses changes that could significantly impact the system of internal control.

Monitoring Activities

- **CC4.1 - COSO Principle 16:** The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

- **CC4.2 - COSO Principle 17:** The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Control Activities

- **CC5.1 - COSO Principle 10:** The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

- **CC5.2 - COSO Principle 11:** The entity also selects and develops general control activities over technology to support the achievement of objectives.

- **CC5.3 - COSO Principle 12:** The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
Supplemental Criteria

- Logical and Physical Access Controls (CC6.1-CC6.8)
  - Section 5 of current Common Criteria
- System Operations (CC7.1-CC7.5)
  - Section 6 of current Common Criteria
- Change Management (CC8.1)
  - Section 7 of current Common Criteria
- Risk Mitigation (CC9.1-CC9.2)
  - Section 3 of current Common Criteria

Additional Criteria

- Availability
  - No significant changes
- Confidentiality
  - Only two additional criteria
    - Identification
    - Disposal
- Processing Integrity
  - No significant changes
- Privacy
  - No significant changes

Review of a SOC Report

- Our experience has shown that users of SOC reports are very inconsistent in their approach to reviewing them.
- There are several critical key points to review in any SOC report.
- Five Main Sections (Typically)
  - Independent Service Auditor’s Report
  - Management’s Assertion
  - Description of the System
  - Tests of Operating Effectiveness
  - Other Information Provided by the Service Organization
**Goal of a SOC Review**

- Evaluation of the SOC report should be a key element in determining whether the service organization presents risk to the user entity and assist in quantifying the level of risk.
- Based upon the results of the report evaluation, determine whether additional audit procedures are required to be performed at the service organization to further quantify the risk or obtain additional comfort over the control environment.
- Are risks significant enough to require further discussion with service organization senior management or evaluation of alternative providers.

**Independent Service Auditor’s Report**

- This is the first section of the SOC report and provides a wealth of good information.
- This section provides the auditors opinion on whether the controls were suitably designed and operating effectively to meet the control objectives or the Trust Services Principles and Criteria.
Independent Service Auditor’s Report

• Items to review in Section I:
  – Report period
  – Services covered by the report
  – If a SOC 2, the Trust Services Principles or additional criteria included within the report
  – Who the service auditor is (reputation)
  – Sub-service organization involvement
  – Type of opinion (qualified vs. unqualified)

Management’s Assertion

• Management of the service organization is required to provide the service auditor with a written assertion that states the following:
  – Fairness of the presentation of management’s description of the service organization’s system
  – Suitability of the design of the controls included in the description
  – The operating effectiveness of those controls (for Type II engagements)

Description of the System
Description of the System

• Sufficiency of information provided to gain an understanding of the system
  – Are there significant parts of the system that are not included that are pertinent to the services being offered?
• End user control considerations (EUCCs)
  – Best practice dictates mapping these to internal controls within the organization to ensure proper coverage

Tests of Operating Effectiveness

• Sufficiency of the controls that were tested
  – Determine if gaps exist
• Sufficiency of the applied testing methodology
• Noted exceptions/deficiencies and the impact on services being provided
  – Management’s responses to exceptions, are they acceptable, do they mitigate the risk effectively, etc.

Other Information Provided by the Service Organization

• This section of the report is optional and is not audited.
• May include:
  – Information related to management’s responses to exceptions.
  – Information related to other initiatives at the service organization.
  – Information related to business continuity and disaster recovery is often illustrated in this section.
Compare to Prior Year Report

• To provide added context, compare the results of the prior year assessment to the current year
  – Did the opinion change?
  – Were exceptions remediated according to management responses?
  – Were similar or different exceptions identified in the prior year?
  – Did the number of exceptions increase or decrease from prior year?
  – Were any new significant events described that would give you concern?

Review Lessons Learned

• Our experience reviewing SOC reports on behalf of our clients (as the user auditor) has provided many lessons learned.
  – Scope of report provided doesn’t match services procured.
  – Report period is not relevant.
  – Testing performed does not meet level of rigor we would expect to satisfy control objective or criteria.
  – Heavy inquiry-only procedures.
  – Gap in report period for subsequent reports.
  – Non-statistical sampling methods.
  – Numerous exceptions on controls perceived to be high risk without modification of opinion.
  – SOC report provided for a sub-service org only (e.g. the datacenter utilized by your vendor).

Questions

Daniel J. Desko, CISA, CISSP, CTPRP, MBA
Senior Manager, IT Risk Advisory Services
Phone: 412-697-5285
Email: ddesko@sdcpa.com

Troy Fine, CPA, CITP, CISA
Manager, IT Risk Advisory Services
Phone: 412-697-6370
Email: tfine@sdcpa.com