Service Organization Control (SOC) Reports and Cyber Security Maturity Model

IIA Lunch and Learn Session
23rd March 2016
Contents

► Role of SOC Reports

► SOC 1 Reports

► SOC 2 and 3 Reports

► Recent Developments
  ► SOC 2+
  ► Cyber Attestation

► Cyber Security Maturity Model
Role of SOC Reports
SOC 1 and SOC 2

► SOC 1
  ► A report on controls at a service organization relevant to a user entity's internal control over financial reporting
  ► Effectively, an external audit
  ► Type I and Type II reports available

► SOC 2
  ► A report on controls at a service organization relevant to security, availability, processing integrity, confidentiality and / or Privacy
  ► Uses the Trust Services principles and criteria
  ► Type I and Type II reports available
Role of SOC reports
SOC 3

► SOC 3
► Covers the same scope as SOC 2.
► Based on Trust Services principles and criteria.
► Does not include a description of the service auditor’s tests of controls and results. Also, the description of the system is less detailed than the description in a SOC 2 report.
► A seal can be issued on a service organization’s website. The Canadian Institute of Chartered Accountants (CICA) administers a seal program for these engagements (if the CPA is licensed for the seal by the CICA).
► The use and distribution of the report is NOT restricted.
SOC 1 Reports
Purpose and scope

► Purpose of SOC 1 is to report on the internal controls of the service organization in relation to the financial statements

► Scope is defined by the service organization; should include all services that have a financial impact

► Type I and Type II reporting options available

► The use of these reports is restricted to the management of the service organization, user entities of the service organization and user auditors.
SOC 1 Reports

Attestation standard

- Prepared in accordance with *Statement on Standards for Attestation Engagements* (SSAE) No. 16, *Reporting on Controls at a Service Organization*, are specifically intended to meet the needs of the managements of user entities and the user entities’ auditors, as they evaluate the effect of the controls at the service organization on the user entities’ financial statement assertions.

- The service organizations determine and define the control objectives and supporting controls which are to be tested by the service auditor.
SOC 1 Reports
Type I and Type II Reports

- **Type I** (relevant to SOC 1 and 2 Reports only)
  - A report on management’s description of the service organization’s system and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date i.e. a ‘point-in-time’ report.

- **Type II** (relevant to SOC 1 and 2 Reports only)
  - A report on management’s description of the service organization’s system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period. i.e. a ‘period-of-time’ report.

- A service organization’s ‘system’ represents five related components, as follows:
  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 programmed and manual procedures involved in the operation of a system (automated and manual)
  5. **Data**. The information used and supported by a system (transaction streams, files, databases, and tables)
To meet the growing needs of ever-expanding technologies, companies who are classified as service organization for SOC reporting, the AICPA put forth the SOC2 framework, a reporting option specifically designed for entities such as data centers, I.T. managed services, software as a service (SaaS) vendors, and many other technology and cloud-computing based businesses.

Within the SOC 2 framework is a comprehensive set of criteria, known as the Trust Services Principles (TSP) that are composed of the following five sections:

1. The **security** of a service organization's system.
2. The **availability** of a service organization's system.
3. The **processing integrity** of a service organization's system.
4. The **confidentiality** of the information that the service organization's system processes or maintains for user entities.
5. The **privacy** of personal information that the service organization collects, uses, retains, discloses, and disposes of for user entities.
SOC 2 Reports
Attestation standard

► These reports are intended to meet the needs of a broad range of users that need to understand internal control at a service organization as it relates to security, availability, processing integrity, confidentiality and privacy.

► These reports are performed using the AICPA Guide: *Reporting on Controls at a Service Organizations Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* and are intended for use by stakeholders (e.g. customers, regulators, business partners, suppliers, directors) of the service organization that have a thorough understanding of the service organization and its internal controls.
SOC 2 Reports
Trust Services Principles and Criteria

► 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 disposed of 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 Canadian Institute of Chartered Accountants.
SOC 2 Reports
Trust Services evaluation categories

► Policies
  ► The entity has defined and documented its policies relevant to the particular principle. (The term *policies* as used here refer to written statements that communicate management's in-tent, objectives, requirements, responsibilities, and standards for a particular subject.)

► Communications
  ► The entity has communicated its defined policies to responsible parties and authorized users of the system.

► Procedures
  ► The entity placed in operation procedures to achieve its objectives in accordance with its defined policies.

► Monitoring
  ► The entity monitors the system and takes action to maintain compliance with its defined policies.
SOC 3 Reports
Differences from a SOC 2

► SOC 3 reports are designed to meet the needs of users who want assurance on the controls at a service organization related to security, availability, processing integrity, confidentiality, or privacy but do not have the need for or the knowledge necessary to make effective use of a SOC 2 report. These reports are prepared using the AICPA / CPA Canada (formerly Canadian Institute of Chartered Accountants) Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. As SOC 3 reports are ‘general use’ reports, they can be freely distributed.

► Unlike a SOC 1 report, which is mainly an auditor-to-auditor communication, SOC 2 Reports are generally a ‘restricted use’ report (at the discretion of the auditor using the guidance in the standard) and SOC 3 Report (in all cases) will enable the service organization to share a general use report that would be relevant to current and prospective customers or as a marketing tool to demonstrate that they have appropriate controls in place to mitigate risks related to security, privacy etc.
SOC 3 Reports
SOC 3 deliverables

SOC 3 reports provide users with:

1. an assertion by management that it maintained effective controls to meet the Trust Services criteria;
2. a short description of the service organization’s system; and
3. a CPA’s examination report on either management’s assertion or on the effectiveness of controls that meet the Trust Services criteria. The fairness of management’s assertion is assessed using criteria in TSP Section 100.

Service organizations may need a general-use report (or seal) instead of or in addition to a SOC 2 report. In addition, a service organization may not wish to provide details of controls in its system description or a description that meets the criteria set forth in the SOC 2 Guide.

In the examination report included in TSP Section 100, the practitioner expresses an opinion on whether the service organization maintained effective controls over its system, based on the criteria in TSP Section 100 that are applicable to the Trust Services principle(s) on which the practitioner is reporting. Because SOC 3 reports are for general use, they can be freely distributed or posted on a website as a seal.
SOC 1, SOC 2, SOC 3 Comparison

System

<table>
<thead>
<tr>
<th>Processing Integrity</th>
<th>Security</th>
<th>Availability</th>
<th>Confidentiality</th>
<th>Privacy</th>
</tr>
</thead>
</table>

SOC 1
- Testing Description
- Opinion
- Assertion

SOC 2
- Testing Description
- Opinion
- Assertion

SOC 3
- Short Desc
- Opinion
- Assertion

Scope of SOC 2 and SOC 3 (Trust Services Criteria)

Users:
- User entity controller
- User entity SOX department
- User auditor

Users:
- User entity security
- User entity compliance
- User entity vendor management
- Regulators
- Prospective user entities

Users:
- General public
What to look for in a SOC Report

Key areas to look for in a SOC Report are:

► Auditor’s opinion and assessment and the scope of the examination – including refs to sub-service organizations

► Service organization’s description of the system, summarizing the services provided, processes and procedures etc. including CUECs

► Control objectives, test of controls and results

► Time coverage of the report
## What is the right SOC for you?
### A service organization’s view

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>SOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Will the report be used by your customers and their auditors to plan and perform an audit or integrated audit of your customer’s financial statements?</td>
<td></td>
<td></td>
<td>SOC 1</td>
</tr>
<tr>
<td>Will the report be used by your customers as part of their compliance with SOx or similar law or regulation?</td>
<td></td>
<td></td>
<td>SOC 1</td>
</tr>
<tr>
<td>Will the report be used by your customers or stakeholders to gain confidence and place trust in a service organization’s systems?</td>
<td></td>
<td></td>
<td>SOC 2 or 3</td>
</tr>
<tr>
<td>Do you need to make the report generally available or seal?</td>
<td></td>
<td></td>
<td>SOC 3</td>
</tr>
<tr>
<td>Do your customers have the need for and ability to understand the details of the processing and controls at a service organization, the tests performed by the service auditor and results of those tests?</td>
<td></td>
<td></td>
<td>SOC 2 or 3</td>
</tr>
</tbody>
</table>
## Comparison of SOC 1, 2 and 3 Reports

<table>
<thead>
<tr>
<th></th>
<th>SOC 1</th>
<th>SOC 2</th>
<th>SOC 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Under what professional standard is the engagement performed?</strong></td>
<td>SSAE No. 16, Reporting on Controls at a Service Organization</td>
<td>AT 101, Attestation Engagements</td>
<td>AT 101, Attestation Engagements</td>
</tr>
<tr>
<td><strong>What is the subject matter of the engagement?</strong></td>
<td>Controls at a service organization relevant to user entities internal control over financial reporting.</td>
<td>Controls at a service organization relevant to security, availability, processing integrity confidentiality, or privacy.</td>
<td>Controls at a service organization relevant to security, availability, processing integrity confidentiality, or privacy.</td>
</tr>
<tr>
<td><strong>What is the purpose of the report?</strong></td>
<td>To provide information to the auditor of a user entity’s financial statements about controls at a service organization that may be relevant to a user entity’s internal control over financial reporting.</td>
<td>To provide management of a service organization, user entities and other specified parties with information and a CPA's opinion about controls at the service organization that may affect user entities' security, confidentiality, or privacy.</td>
<td>To provide interested parties with a CPA's opinion about controls at the service organization that may affect user entities' security, availability, processing integrity confidentiality, or privacy.</td>
</tr>
</tbody>
</table>
## Comparison of SOC 1, 2 and 3 Reports

<table>
<thead>
<tr>
<th>What are the components of the report?</th>
<th>SOC 1</th>
<th>SOC 2</th>
<th>SOC 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A description of the service organization’s system.</strong></td>
<td>A description of the service organization’s system.</td>
<td>A description of the service organization’s system.</td>
<td>A service auditor’s report on whether the entity maintained effective controls over its system as it relates to the principle being reported on i.e. security, availability, processing integrity, confidentiality, or privacy, based on the applicable trust services criteria.</td>
</tr>
<tr>
<td><strong>A service auditor’s report that contains an opinion on the fairness of the presentation of the description of the service organization’s system, the suitability of the design of the controls, and in a Type 2 report, the operating effectiveness of the controls.</strong></td>
<td><strong>In a Type 2 report, a description of the service auditor’s tests of the controls and the results of the tests.</strong></td>
<td><strong>In a Type 2 report, a description of the service auditor’s tests of the controls and the results of the tests.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>In a type 2 report, a description of the service auditor’s tests of the controls and the results of the tests.</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Who are the intended users of the report?</th>
<th>SOC 1</th>
<th>SOC 2</th>
<th>SOC 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditor’s of the user entity’s financial statements, management of the user entities, and management of the service organization.</td>
<td></td>
<td>Parties that are knowledgeable about: • the nature of the service provided by the service organization • how the service organization’s system interacts with user entities, subservice organizations, and other parties • internal control and its limitations • the criteria and how controls address those criteria</td>
<td>Anyone</td>
</tr>
</tbody>
</table>


Recent Developments
SOC 2+

► Service Organizations are under continuous pressure from their customers to confirm compliance to various different regulatory frameworks and continued cyber security risks and concerns.

► Additional client needs are being built into contracts and the service organizations are faced with the challenge of controlling their compliance costs in line with such demand.

► SOC 2+ reports are rapidly emerging as a more effective and efficient option for service organizations that need to communicate internal control information related to other compliance requirements.

► The idea behind SOC 2+ is that the service auditor will express an opinion on both the AICPA’s Trust Services Criteria (i.e. SOC 2 scope) “plus” additional subject matter.

► The ability to report on multiple compliance frameworks simultaneously is what makes a SOC 2+ valuable to both the user and service organizations.
Recent Developments
SOC 2+

The following are approved mappings published by the AICPA for SOC 2+ purposes:

- Trust Services to COBIT5
- Trust Services to COSO 2013 Framework
- Trust Services to ISO 27001
- Trust Services to NIST 800-53 R4
- Trust Services to HiTrust CSF v7
- Trust Services to Cloud Controls Matrix (CCM)
Recent Developments
Cyber Security

- The AICPA has recognized the need for guidance to enable firms to address the marketplace’s various needs – *currently a Top 5 initiative of the Institute*

- The Cybersecurity Working Group of AICPA’s Assurance Services Executive Committee is developing guidance for the profession to utilize when performing and reporting on attestation engagements relating to cybersecurity

  - Specifically, the Working Group is charged with:

    - Designing an attest engagement that meets the needs of a broad range of potential stakeholders
    - Developing the related practitioner guidance, including the identification of suitable criteria against which processes and controls can be measured

- The primary goals of the attest engagement will be to:

  - Improve management’s communication with interested parties (i.e. transparency) regarding the entity’s cyber risk management program
  - Enhance confidence in the integrity of the information provided via an auditor’s attestation
Why are existing SOC 1 and SOC2 (Trust Services) attest reports inadequate to provide this desired level of transparency?

SOC 1 reports

► While the IT general controls incorporated into a SOC 1 engagement include certain fundamental security-related controls, many key aspects of an effective security risk management program (including those specifically responsive to cybersecurity risks) are not typically in scope.

► These reports cover only a portion of an entity’s operations (that relating to an outsourced financial reporting-related service); they also do not provide adequate visibility into the broader cybersecurity risk management program over:
  ► The enterprise-wide operations of the entity
  ► The manufacturing and distribution operations of supply chain vendors
Recent Developments
Cyber Security

Why are existing SOC 1 and SOC2 (Trust Services) attest reports inadequate to provide this desired level of transparency?

SOC 2 reports

► While additional aspects of an entity’s security risk management program (beyond those included in a SOC1) are included in the scope of a SOC 2 engagement, various control and process areas specifically responsive to cybersecurity risks are not typically in scope.

► These reports only cover those aspects of an entity’s operations that support an outsourced services; they do not provide adequate visibility into the broader cybersecurity risk management program over:
  ► The enterprise-wide operations of the entity
  ► The manufacturing and distribution operations of supply chain vendors
Cyber Security Maturity Model
Effective mapping tool

► Cyber is such a broad topic and means different things to different people

► The Maturity Model is an effective way of rationalizing what the key areas of Cyber are and allows for any organization to plot themselves in each area of the model

► By answering a small number of questions, EY will be able to plot your maturity level for each cyber ‘domain’, which can then be compared against either peers/competitors and/or where you wish to be i.e. a gap analysis tool
The CMM covers around 20 different domains, each mapped from Level 1 (least mature) through to Level 5 (most mature), such as:

- Strategy
- Governance and organization
- Policy and standards framework
- Identity and Access Management
- Threat and vulnerability management
- Security monitoring
- Metrics and reporting
Questions?

Please contact:

Kerr Kennedy  
Senior Manager  
IT Risk & Assurance  
Ernst & Young Ltd.  
3 Bermudiana Road, Hamilton HM08, Bermuda  
Direct: +1 441 294 5460  
Cell: +1 441 531 1010  
Office: +1 441 295 7000  
kerr.kennedy@bm.ey.com
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young Ltd. (Bermuda), Ernst & Young, Ernst & Young Ltd. (Cayman), and Ernst & Young LLP are client-serving member firms of Ernst & Young Global Limited operating in Bermuda, the Bahamas, the Cayman Islands and the BVI (collectively the “BBC”) and the United States, respectively.

EY is a leader in serving the global financial services marketplace. Nearly 35,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Office today includes more than 6,500 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America. EY professionals in our financial services practices worldwide align with key global industry groups, including EY’s Global Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY’s financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

© 2016 Ernst & Young Ltd.
All Rights Reserved.