Crowe Horwath.

Smart decisions. Lasting value.℠

Emerging/Alternative Third Party Assurance Reporting

August 9, 2016

Eve Rogers, Partner, Crowe Horwath LLP
Regina Davis, Manager, Crowe Horwath LLP

This presentation was developed exclusively for the attendees of Geek Week 2016.

Agenda

- Introduction of Presenters
- Service Organization Controls (SOC) Reports Overview
- Components of a SOC Report
- Emerging / Alternative Trends in Third Party Assurance Reporting
- Questions

Introduction of your Presenters

- Eve Rogers, CPA
  - Partner – Atlanta Office

- Regina Davis, CISA, CRISC, PMP
  - Technology Risk Manager – Atlanta Office

Service Organizations Controls (SOC) Reports Overview

A Little Background…..

- **SAS 70 is a US Standard -** Although used internationally, SAS 70 reports were issued only by U.S. registered firms.
- **An International Standard 3402 was developed –** Standards on Assurance Engagements (ISAE) 3402, “Assurance Reports on a Service Organization's Controls,” was finalized by the International Auditing and Assurance Standards Board (IAASB) in December 2009.
- **AICPA Issues SSAE 16 –** Statement on Standards for Attestation Engagements (SSAE) 16, “Reporting on Controls at a Service Organization,” is the result of efforts by the American Institute of CPAs (AICPA) to clarify its standards and to converge them with IAASB standards.
- **It’s not a Certification –** Compliance with SSAE 16 does not result in an organization’s becoming “SSAE 16 certified” or gaining a certificate or designation.

Where we are today…

- CPA's are being asked to provide auditing assurance on topics other than financial statements, which could not be done under SAS 70 or SSAE 16.

- **SOC 2 and SOC 3 standard was developed –** AICPA issued auditing standards that report on a range of "trust 'services" that go beyond financial reporting,

- The reporting options include
  - SOC 1 – Report on controls over financial reporting (SSAE 16/SAS 70)
  - SOC 2 – Report over compliance with Trust Services Principles (TSP)
  - **SOC 2 + – Report can be expanded to cover additional regulations**
  - SOC 3 – Report over compliance with TSP, publically available

Types of SOC Reports

Report	Report's focus	Audience
SOC 1	Report on internal controls over financial reporting	Restricted Use
SOC 2	Report on controls related to Security, Availability, Processing Integrity, Confidentiality and/or Privacy (Trust Services Principals)	Restricted Use
SOC 3	Report on controls related to Security, Availability, Processing Integrity, Confidentiality and/or Privacy (Trust Services Principals)	General Purpose

Contents of a SOC Report

SOC 1

- Service auditor's opinion
- Management's assertion
- Management's detailed description of systems
- Details on the auditor's tests of controls related to each **control objective** and results

SOC 2

- Service auditor's opinion
- Management's assertion
- Management's detailed description of systems
- Details on the auditor's tests of controls related to each selected **trust services principle** and results

SOC 3

- Service auditor's opinion
- Management's assertion
- Management's **summary description** of its systems and the boundaries of the systems

SOC Report – Key Points

- Reports may be Type 1 or Type 2
  - Type 1: Attests on design and implementation of controls as of a certain date
  - Type 2: Attests on design and operating effectiveness of controls over a timeframe, typically between six months and one year
- Intended Parties
  - Customers, Regulators, Business Partners, Suppliers, Directors
- Example Industries
  - SOC 1: outsourced payroll processors, outsourced card processors, software development firms, banks offering trust and investment services
  - SOC 2: data centers, SIEM, cloud computing, health care service providers (claims management and processing)

SOC 1 Key Points

- 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
- Service auditor is attesting to management's description of systems and controls
- Is consistent with International guidance ISAE 3402

SOC 2 – Key Points

- Engagement performed under AT section 101
- Reports on the internal controls of a Service Organization
- Uses criteria in *Trust Services Principles Criteria and Illustrations*
- Five Trust Services Principles
  - *Security*: The system is protected against unauthorized access, both physically and logically.
  - *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 held by an organization is securely protected.
  - *Privacy*: Personal information is collected, used, retained, disclosed and destroyed in conformity with the commitments in the entity's privacy notice and with criteria established in Generally Accepted Privacy Principles (GAPP).
- Scope may include one or more of the 5 Trust Services Principles

SOC 2 – Key Points

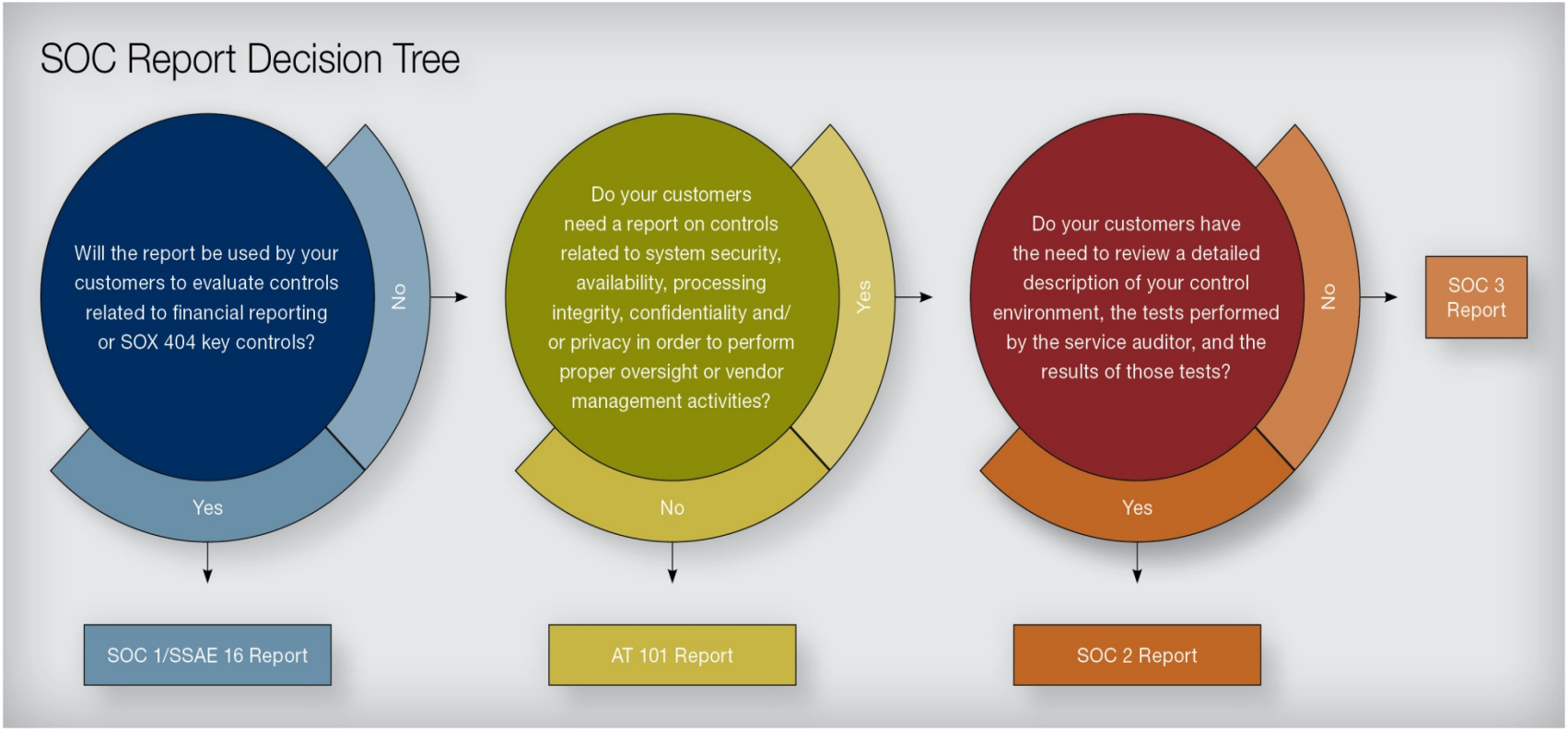
- Security
  - For SOC 2, the word “Security” carries a broad meaning.
  - Example: In the context of the availability principle, the term security may relate to the protection of the system from interruptions in processing availability.
- Risks Addressed by Controls
  - Due to the differences in subject matter and needs of intended users, the risks and the controls that address those risks are likely to differ between SOC 1 and SOC 2.
  - Example: In a SOC 1, controls over changes to application programs would typically focus on those that may affect the financial reporting process, while in a SOC 2 that addresses the processing integrity principle, controls over program changes may cover a much broader range of application programs (for example, customer service applications and manufacturing process control applications).

SOC 3 – Key Points

- Similar in structure to a SOC 2 to include common Criteria and applicable Trust Services Principles
- Not restricted in its use and may be publically available
- Does not include tests over the design and operating effectiveness

Which Report Should Be Chosen?

When deciding which type of report is most appropriate, consider these questions.



Components of a SOC report

SOC Report Contents

SOC 1 and 2 Report Contents

- Service Auditor Opinion
- Management's Assertion
- Description of Systems
- Test Results
- Complementary User Entity Controls
- Other Information

SOC 3 Report Contents

- Service Auditor Opinion
- Management's Assertion
- Summarized Description of Systems

Service Auditor’s Opinion

- Opinion references service organization responsibilities
  - Providing the assertion
  - Preparing an accurate and complete description
  - Designing and effectively operating controls to achieve the control objectives
  - Selecting criteria and identifying the risks that threaten the achievement of the control objectives
- Opinion continues to cover subject matter
  - Fair presentation of the description of the system; design and implementation of controls; and operating effectiveness
  - Includes the entire period, rather than as of a point in time (Type 2 report)
  - Does not include a statement on whether management had a reasonable basis for providing their assertion
  - Consider explanatory paragraph if assertion is incorrect
  - For SOC 2 reports covering Privacy, the opinion includes a statement about whether management complied with its statement of privacy practices throughout the period.

Management's Assertion

- Management must provide a signed assertion which is included in the report.

- Key Components of Management's Assertion
  - The description fairly presents the system that was designed and implemented throughout the specified period
  - The controls were suitably designed throughout the specified period
  - The controls were operating effectively throughout the specified period
  - Management complied with the commitments in its statement of privacy practices throughout the specified period (if the privacy principle is in scope)

- Typically those that sign the representation letter are the same as who will provide the assertion

Basis for Management's Assertion

- Management's activities such as monitoring or separate evaluations may provide support for assertion:
  - Ongoing monitoring activities
  - *Regular management and supervisory activities*
  - *Sub-certifications*
  - *Review of compliant files*
  - Separate evaluations
- *Support for Assertion*
  - *Internal auditors or other personnel (risk/compliance) performing specific audits /examinations*
  - *Information from external parties (e.g. Regulatory reviews*)
  - Combination of both
- Support for Assertion
  - Management determines the support they will need
  - No requirement to retain documentation – however a prudent and sound governance practice

Description of the Service Organization's System

- The Description of Systems include:
  - The components of the system used to provide the services (i.e., Infrastructure, Software, People, Procedures and Data)
  - The boundaries of the system
  - The process used to prepare and deliver reports and other information to user entities and other parties
  - CUECs contemplated in the design of the Service Organization's system
  - Any criteria that is not addressed by a control and the reasons.
  - Other aspects of the organization's control environment, risk assessment process, information and communication systems and monitoring of controls.
  - If the report is a type 2 report, details of changes that have occurred during the audit period covered by the audit.
  - The AICPA has identified additional requirements for the description if the privacy principle is being covered. (Reference next slide)
  - See the AICPA SOC 2 Guide a complete list of requirements.

Additional Considerations for the Privacy Principle (SOC 2)

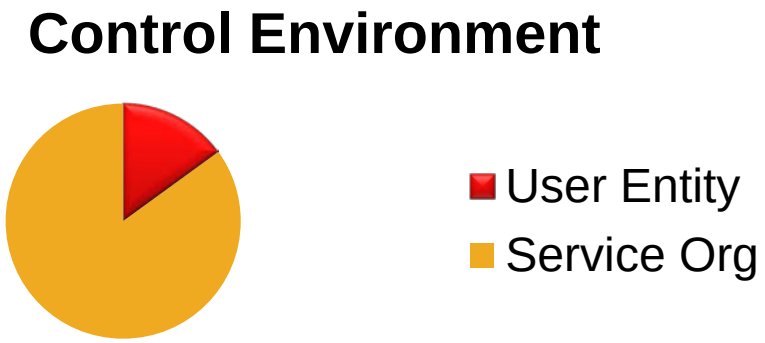
- Opinion & Management's Assertion Considerations
  - Includes whether management complied with its commitments in its statement of privacy practices throughout the period.
- Modifications to the Description
  - Types of personal information is obtained and how it is collected
  - Process for identifying specific requirements in agreement with user entities and applicable laws and regulations and how controls are implemented to meet those requirements.
- Should include the organization's privacy notice if the organization is responsible providing a privacy notice to the individuals from whom information is collected.
- If the user entities are responsible for providing a privacy notice:
  - Should include a statement regarding how the notice is communicated to individuals, that the user entities are responsible for communicating the notice to individuals and that the service organization is responsible for communicating its privacy practices to the user entities in its statement of privacy practices.
  - Should include the statement of privacy practices
- See AICPA SOC 2 guide for complete list of modifications to the description.

Test of Design and Operating Effectiveness

- SOC 1
  - Controls objectives over financial reporting
- SOC 2
  - Seven Criteria Common to all Principles
    - Organization and management
    - Communications
    - Risk management and design and implementation of controls
    - Monitoring of controls
    - Logical and physical access controls
    - Systems operations
    - Change management
  - Five Trust Service Principles
    - Security
    - Availability
    - Processing Integrity
    - Confidentiality
    - Privacy
- SOC 3
  - There are no tests of design and operating effectiveness.

Complementary User Entity Controls (CUECs)

- Controls listed that are the responsibility of the User of the service provided.



Example:

- User Entity is responsible for the provisioning and appropriateness of end user access.

Other Information

- This section is not part of the description of systems.

- Examples of ‘Other Information’
  - “Forward looking” information
  - Business Continuity & Disaster Recovery Plans
  - Organizational Charts
  - Discussion of future service enhancements
  - Planned infrastructure upgrades

➔ **Key Point**: This section is unaudited by service auditor

Emerging / Alternative Trends

Emerging / Alternative Trends in Third Part Assurance Reporting

- SOC 2+
- Cybersecurity Attestation

What is a SOC 2 +?

- A SOC 2 report on '**Steroids**'.
- Expanded coverage to include Additional Subject Matter and/or Criteria:
  - HIPPA
  - Cloud Security Alliance Cloud Control Matrix (CSA CCM)
  - HITRUST Common Security Framework
  - ISO 27001
  - NIST 800-53 R4
  - COBIT5
  - COSO 2013 Framework
  - Historical data related to the availability of computing resources
  - Compliance with a statement of privacy practices

➔ **Key Point**: It can be tailored to organization's need as long as the additional matter/criteria are referenced in the opinion, description, etc.

Cybersecurity Attestation - Background

- Cybersecurity is the most significant emerging technology risk area today for most entities (businesses, government and individuals).

- Recent breaches have had major economic and reputational consequences.

- Stakeholders and regulatory bodies are demanding increased visibility and assurance regarding organizations cyber risk management programs.

➔ ***Senior Management and Boards of Directors are expected to demonstrate increased oversight of their organization's Cybersecurity Risk Management Program responsibility and controls.***

Cybersecurity Attestation - Challenges

- Most organizations have immature Cybersecurity Risk Management Programs and oversight.
- There are many Cybersecurity risk and control frameworks, but no generally recognized industry leading framework or standards.
- There are many firms that provide Cybersecurity assessments, but the assessment methods used vary greatly, report distribution is often restricted, and many reviews are focused exclusively on identifying vulnerabilities rather than assessment of a firm's Cyber Risk Management Program.

➔ ***There is a need for third party assurance over an entity's Cybersecurity Risk Management Program and Controls available to interested parties. The standards used should be robust and comparable form one entity to another.***

Cybersecurity Attestation - Objectives

- The AICPA believes that an ***independent examination*** of the companies' cybersecurity risk management program can be consistently performed across all industries and companies.

- The proposed service would be ***voluntary, flexible, and separate*** from the existing financial statement audit.

- A holistic approach is required focusing on:
  - (a) assessing the program to reduce the ***likelihood of breach***,
  - (b) the design, implementation and ***operating effectiveness*** of controls,
  - (c) as well as the ***ability to mitigate and recover*** from breaches sustained.

- Bring to bear benefits that are unique to, or exemplified by, the public accounting profession – i.e. positive assurance ***opinion*** (using 'reasonable assurance' standard), adherence to stringent ***professional standards***, as well as ***consistency and comparability*** across industries, entities and reports.

➔ ***McKinsey Global Survey indicated that over half of executives interviewed believe that cybersecurity is a strategic risk for their companies. Yet only 5% of companies' report "mature" or "robust" cybersecurity risk management maturity capabilities.***

Cybersecurity Attestation – Key Components

The Proposed Assurance / Attestation Engagement would have Three Key Components:

1. **Management's Description**: The first element is a management-prepared, narrative description of the entity's cybersecurity risk management program and controls which
   - Identifies sensitive information and training
   - How program manages Cyber risks and threats
   - Summary of controls implemented and operated to address cyber risks.

2. **Management's Assertion**: Management also provides an assertion that the controls implemented as part of the program are suitably designed and operate effectively.

3. **The Practitioner's Opinion:** The final element is a CPA's opinion on the description (i.e., its completeness and accuracy) and the suitability of design and operating effectiveness of the controls implemented as part of the program.

Proposed Approach to Cybersecurity Attestation Engagement - Highlights

- **Consistency –** Assurance provided would benefit from the practitioner's consistency, rigor, independence, and objectivity.
- **Credibility –** The involvement of an independent, objective, and credentialed professional can effectively increase the credibility of entity-prepared information.
- **Voluntary --** The proposed engagement would be entirely voluntary on the part of companies and audit firms. If chosen, this new service would constitute an examination under the attestation standards of the audit profession (i.e., they would not be a consulting type service).
- **Flexible --** Companies could choose one of several available sound cybersecurity internal control frameworks for their cybersecurity risk management program, they do not need to alter their frame work for the assurance engagement.
- **Broader Distribution –** Unlike the SOC 1 and SOC 2, (which are 'limited use reports) the Cybersecurity assurance engagement is proposed to be 'general use' reports which can be provided to investors, third party business partners and other 'interested' parties (with sufficient knowledge of Cybersecurity.)

Cybersecurity Attestation – Current Status and Timeline

Current Status

- The AICPA Cyber Working Group ("WG") has drafted an approach document that has been reviewed and circulated to the organizations represented on the WG and to professional organizations for review and comment.
- The WG has drafted an opinion, assertion and a preliminary set of 'description criteria for review and comment. Now the WG is focusing on developing a 'practitioner's guide' for the engagement.

Timeline

- Planning to issue a 'practitioner's guide' for comment by Q4 2016
- Guidance to become effective by year-end 2016

➔ ***Note:*** *The timeline for issuing is frequently delayed. The timeframes outlined above are now relatively aggressive, given the level of comment provided during the review phase of the deliverables developed to date, but are still the target deadlines.*

Questions?

Thank you!

Eve Rogers, CPA

Partner

Phone +1 404 442 1634

Eve.Rogers@crowehorwath.com

Regina Davis, CISA, CRISC, PMP

Technology Risk Manager

Phone +1 404 442 1632

Regina.Davis@crowehorwath.com