Understanding SOC Reports

Bryan Newlin, CPA, CISA

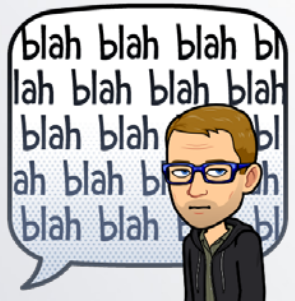
Principal | YHB CPAs & Consultants

Agenda

- What are SOC Audit Reports?
- Brief History of SOC Audits
- Brief History of the Trust Services Criteria
- Why are SOC Audits Different from other IT Reports?
- Understanding the Elements of the Report
- Key elements when performing your SOC Audit Report Review
- New types of SOC Audits

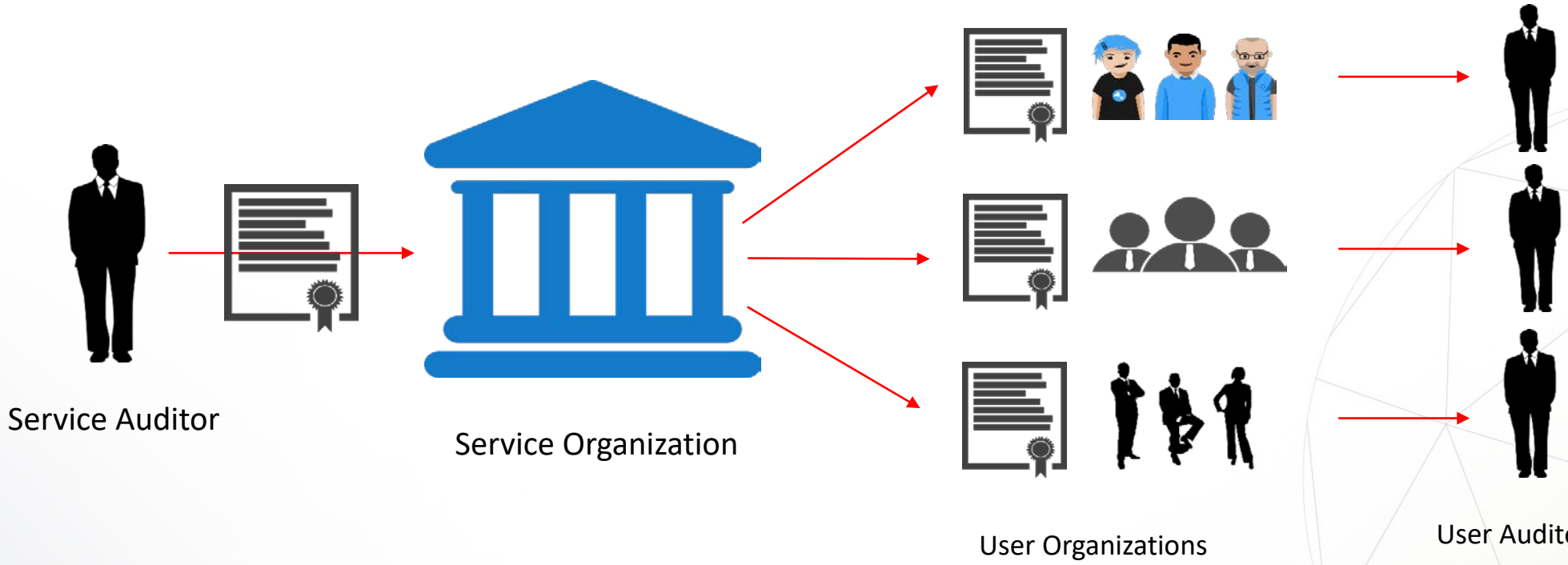
What are SOC Audit Reports?

- SOC = System & Organization Control Reports
- SOC ≠ SOX ≠ SOC (Security Operation Center)
- An **independent** accountant's **attestation** report which gives an opinion on the accuracy of a narrative description, the design of internal controls, and in the case of a type 2 report, the effectiveness of the controls over a period of time.
- An auditor-to-auditor communication; a restricted use report limited to the *service auditor*, *service organization*, the *user organization*, and *user auditor*.



What are SOC Audit Reports?

- Definition 2: It's how a service organization shows their customer's that they are giving them <u>good data</u> and keeping ***<u>their</u>*** <u>customer's information</u> safe.



A Brief History of SOC Reports

History of SOC Audit Reports

- SAS 70 issued in April 1992
- Sarbanes-Oxley Act of 2002 introduced ICFR Opinions and increased reliance on internal controls.
- GLBA and increased Vendor Management requirements resulted in companies misusing SAS 70 reports.

History of SOC Audit Reports

- Trust Services Categories (formerly Trust Services Principals)
  - TSC = Security, Availability, Processing Integrity, Confidentiality, Privacy
  - SysTrust & WebTrust Engagements
  - TSC were adopted as part of SOC 2 and SOC 3 reports
  - More recent developments include:
    - Alignment with COSO Internal Control Framework
    - Renaming “Principals” to “Categories and Criteria”

History of SOC Audit Reports

- Attest standards were updated in 2009, resulting in SSAE 16 and AT 101
- Two reports (SAS 70 & SysTrust) become SOC
- AICPA rebranded SAS 70 to SOC Suite of Services and introduced:
  - SOC 1
  - SOC 2
  - SOC 3
- AICPA Changed the meaning of SOC

Current SOC Suite of Services

- SOC 1 for Service Organizations: ICFR
- SOC 2 for Service Organizations: Trust Services Criteria
- SOC 3 for Service Organizations: General Use Report
- SOC for Cybersecurity
- SOC for Supply Chains

Why are SOC Audits Different?

How are SOC Audits Different?

- Other control frameworks and certifications options:
  - ISO 27001
  - NIST Cybersecurity Controls
  - PCI
  - COSO
  - ITIL
  - FedRamp
  - CMMC

- SOC – No prescriptive controls, industry agnostic

How are SOC Audits Different?

- Performed by CPA Firms
  - Minimum education standards
  - Professional exams & continuing education
  - Quality Control requirements
  - Recourse for failing to comply with professional requirements
- Several concepts make a SOC audit report unique:
  - Attestation
  - Independence
  - Opinion

Understanding SOC Reports

Understanding SOC Reports

- SOC 1 for Service Organizations: ICFR
  - Description criteria defined by Management
  - Control Objectives defined by Management
  - Controls are defined by Management

- SOC 2 for Service Organizations: Trust Services Criteria
  - Description Criteria defined by AICPA
  - Trust Services Criteria defined by AICPA
  - Controls are defined by Management

- Both have options for type 1 or type 2

Understanding SOC Reports

- Important Terms to Know
  - Type 1 vs. Type 2
  - Service Auditor – Service Organization – User Organization – User Auditor
  - Subservice Organizations| Inclusive vs. Carve Out
  - Complementary Subservice Organization Controls
  - Complementary User Entity Controls

Understanding SOC Reports

- Report Sections
  - Management's Assertion
  - Independent Auditor's Opinion
  - Narrative Description of the System
  - Controls and Auditor's Tests of Controls
  - Other Information Provided by the Service Organization

Reviewing a SOC Report

Reviewing a SOC Report

- Let's review a SOC 1 Report looking for the following elements:
  - Cover page
  - Opinion Letter
  - Assertion and Criteria
  - Narrative Description
  - CUECs
  - Controls and Tests of Controls
  - Exceptions

Reviewing a SOC Report

- Red Flags
  - Opinion
  - Quantity and quality of exceptions
  - Stale dated reports
  - Annual type 1 reports, never type 2
  - Scope does not align with the services provided
  - Material inaccuracies in details of the report (e.g. Report states a SOC 1 but uses the Trust Services Criteria)
  - Evaluate the Service Auditor

Other SOC Reports

Other SOC Reports

- SOC 3 for Service Organizations: General Use Report
- SOC for Cybersecurity: Examination of an Entity's Cybersecurity Risk Management Program
- SOC for Supply Chain: Helps companies understand the risks associated with supply chains

Questions?

Bryan Newlin, CPA, CISA
Principal – Risk Advisory Services
bryan.newlin@yhbcpa.com