WOLF
& COMPANY, P.C.

# Understanding SOC Reports for Effective Vendor Management

Jason T. Clinton
January 26, 2016

# Before we get started…

- Today's presentation slides can be downloaded at https://www.wolfandco.com/webinars/2016
- The session will last about an hour.
- Our audience will be muted during the session so if you have questions throughout the presentation, please send them by using the "question box" located on the webinar's control panel.

# About Wolf & Company, P.C.

- Established in 1911
- Offers Audit, Tax, and Risk Management services to nearly 250 financial institutions
- Offices located in:
  - Boston, Massachusetts
  - Springfield, Massachusetts
  - Albany, New York
  - Livingston, New Jersey
- Nearly 200 professionals


*As a leading regional firm, we provide our clients with specialized industry expertise and responsive service.*

# Financial Institution Expertise

- Provide services to nearly 250 financial institutions:
  - Approximately 50 FIs with assets > $1B
  - Approximately 30 publicly traded FIs
  - Constant regulatory review of our deliverables
- Over 60 Risk Management Professionals:
  - IT Assurance Services Group Professionals
  - Internal Audit Services Group Professionals
  - Regulatory Compliance Services Group Professionals
  - WolfPAC® Solutions Group Professionals
- Provide RMS in 27 states and 2 U.S. territories

# Meet Today's Presenter

**Jason T. Clinton**

IT Assurance Senior Consultant

Phone:  617-261-8132

Email: jclinton@wolfandco.com

# Objectives

- Learn the differences between the three SOC reports
- Understand which SOC reports you should be requesting from your service providers
- Learn the sections of the SOC reports and how to effectively review the information

# SOC Terminology

- Service Organization
- Service Auditor
- User Entity
- User Auditor

# Service Organization Control Reports (SOC)

- **AICPA SOC 1 Report**
  Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting. (SSAE No. 16)

- **AICPA SOC 2 Report**
  Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, and/or Privacy

- **AICPA SOC 3 Report**
  Trust Services Report for Service Organizations

# Type 1 vs. Type 2

- **Type 1**
  - Report on management's description of a service organization's system and the suitability of the design of controls
  - **As of a specified date**
- **Type 2**
  - Report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls
  - **Throughout the specified period**

# SOC 1 (SSAE No. 16) Report

- Performed using AICPA Guide: “Service Organizations – Applying SSAE No. 16, Reporting on Controls at a Service Organization (SOC 1)”
- Type 1 and Type 2 format
- The service organization defines the control objectives that relate to the types of assertions commonly embodied in the broad range of user entities’ financial statements
- Restricted use report

# SOC 2 Report

- Performed using AICPA Guide: “Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)”
- Type 1 and Type 2 format (structured similarly to SSAE No. 16 (SOC 1))
- The report is based on predefined criteria:  Trust Services Principles and Criteria
- The service organization selects the principles that best align with the scope of services delivered to the user entities for whom the reports are intended
- Can be used by those that have sufficient knowledge and understanding of the services, systems, and internal controls

# SOC 3 Report

- More general purpose and less detailed than a SOC 2
- The report is based on predefined criteria:  Trust Services Principles and Criteria
- The service organization selects the principles that best align with the scope of services delivered to the user entities
- Report can be made public
- Must be a Type 2 and cannot have control exceptions or complementary user entity controls

# SOC 2 & 3 – Trust Services Principles and Criteria

- Set of profession attestation and advisory services based on a core set of principles and criteria that address risks and opportunities of IT-enabled systems and privacy programs
- Developed by AICPA and the CPA Canada (Formerly Canadian Institute of Charted Accountants)

# Trust Services Principles

- **Security** – System is protected against unauthorized access, use, or modification (both physical and logical).
- **Availability** – System is available for operation and use as committed or agreed.
- **Processing Integrity** – System process is complete, accurate, timely, and authorized.
- **Confidentiality** – Information designed as confidential is protected as committed or agreed.
- **Privacy** – The system's collection use, retention, disclosure, and disposal of personal information is in accordance with the entity's commitments and system requirements.

# Trust Services Criteria

The Principles are organized into seven categories (except Privacy) as follows:

- **Organization and Management –** The entity has a defined structure to manage and support personnel in the system.
- **Communications –** The entity has communicated its policies, processes, and system requirements to authorized users and responsible parties of the system.
- **Risk Management and Design and Implementation of Controls –** The entity has a process to identify risks and design and implement controls.

# Trust Services Criteria

The Principles are organized into seven categories (except Privacy) as follows:

- **Monitoring of Controls –** The entity monitors the system and takes action to address deficiencies.
- **Logical and Physical Access Controls –** The entity restricts logical and physical access to the system.
- **System Operations –** The entity manages the execution of system procedures and detects and mitigates processing deviations.
- **Change Management –** The entity has a controlled change management process and controls to prevent unauthorized changes.

# SOC Report Products/Services

- SOC 1
  - Payroll Providers
  - Data Processors
  - Loan Servicing
  - Trust Companies
- SOC 2 / SOC 3
  - Managed Security Providers
  - Cloud Computing
  - Non-Transactional Website Hosting
  - Data Centers

# Elements of a SOC 1 & SOC 2 Report

- **Section 1:** Service Auditor
  - Independent Service Auditor's Report (Opinion Letter)
- **Section 2:** Service Organization
  - Service Organization's Assertion
- **Section 3:** Service Organization
  - Description of Service Organization's System
  - Control Objectives and Control Activities (SOC 1) / Trust Services Principles and Criteria and Controls (SOC 2)
  - Complementary User Entity Controls
- **Section 4:** Service Auditor (Type 2 only)
  - Independent Service Auditor's Description of Tests of Controls and Results
- **Section 5:** Service Organization
  - Additional Information Provided by the Service Organization

# **Section 1:** Service Auditor's Report

- Identifies products / services in scope
- Defines period of coverage (Type 2) or as of date (Type 1)
- Inclusive or Carve-Out Method
- Opine on whether documented controls satisfy the control objectives (SOC 1) or trust services criteria (SOC 2)
- Identifies exceptions to testing of the documented controls (Type 2)

# **Section 2:** Service Organization Assertion

- Identifies products / services in scope
- Defines period of coverage (Type 2) or as of date (Type 1)
- Assert on whether documented controls satisfy the control objectives (SOC 1) or trust services criteria (SOC 2)
- The criteria used in making the assertion

# **Section 3:** Description of Systems

- The type of services provided
  - Classes of transactions processed (SOC 1)
  - Components of the system including Infrastructure, Software, People, Procedures, and Data (SOC 2)
  - How the system captures and addresses significant events and conditions
  - Reporting
- Relevant aspects of:
  - Control Environment
  - Risk Assessment Process
  - Monitoring Controls
  - Information and Communication
- Complementary user entity controls

# **Section 4:** Independent Service Auditor's Description of Tests of Controls and Results

- Control objectives and related controls (SOC 1) or Trust Service criteria and related controls (SOC 2)
- Types of tests:
  - Inquiry
  - Observation
  - Inspection
  - Re-performance
- Testing of operating effectiveness

# Example of Testing in a SOC 1

| Physical Security: Controls provide reasonable assurance that physical access restrictions are implemented to ensure only authorized individuals have access to sensitive areas. | | | |
|---|---|---|---|
| Control Activity | Test Type | Test | Results |
| A key fob is required for entry to the server room. Server room access is only provided to authorized employees. | I | Inspect documented policies to ensure that physical access to the server room is required to be restricted to authorized employees. | No exceptions noted. |
| | O | Observe that a key fob is required for entry to the server room. | No exceptions noted. |
| | I | Inspect the key fob access report and authorization forms to ensure that only authorized individuals have access to the server room. | No exceptions noted. |

# Testing in a SOC 2

| CC1.0 – Common Criteria Related to Organization and Management | | | |
|---|---|---|---|
| **Criteria** | **Control** | **Test** | **Test Results** |
| 1. The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and requirements as they relate to security and availability. | 1. The Written Information Security Program (WISP) assigns the Information Security Officer as responsible and accountable for system security and availability. | Inspected the Written Information Security Program (WISP) to determine it assigns the Information Security Officer responsible and accountable for system security and availability. | No exceptions noted. |
| | 2. Employees roles and responsibilities are defined in written job descriptions that are available on the intranet and updated annually. | Inspected a sample of written job descriptions to ensure employees' roles and responsibilities are defined. | No exceptions noted. |
| | | Observed written job descriptions are available to employees through the Company's intranet. | No exceptions noted. |
| | | Inspected a sample of written job descriptions to ensure the job descriptions are updated on an annual basis. | No exceptions noted. |

# **Section 5:** Additional Information Provided by the Service Organization

- Information the Service Organization may detail in this section includes:
  - Management's response and remediation plans for exceptions noted
  - New products and services
  - Business continuity / disaster recovery planning

# Elements of a SOC 3 Report

- **Section 1:** Service Auditor
  - Independent Service Auditor's Report (Opinion Letter)
- **Section 2:** Service Organization
  - Service Organization's Assertion
- **Section 3:** Service Organization
  - Description of Service Organization's System

# Vendor Management

- SOC reports should be requested for vendor due diligence and vendor oversight

- User entities' SOC report review documentation should include the following:
  - Products and services covered in the report
  - Type (1 or 2) of the report and period covered
  - Opinion of the service auditor
  - User entities responses to the complimentary user entity controls stated in the report
  - Exceptions noted by the service auditor

# Vendor Management

- User entities' SOC report review documentation should specify if the report covered the following elements:
  - Information Security Program
  - Business Continuity/ Disaster Recovery Program
  - Change Management Process
  - Logical and Physical Controls
  - Data Backup and Restoration
  - Incident Response Plan
  - Use of sub-service organizations

# Questions?

**Jason T. Clinton**

IT Assurance Senior Consultant

Phone:  617-261-8132

Email: jclinton@wolfandco.com