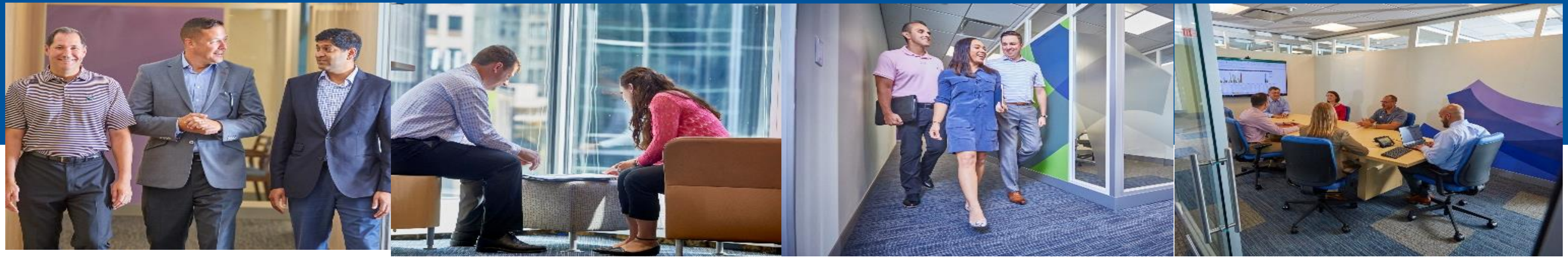
SCHNEIDER DOWNS

Big Thinking. Personal Focus.

How to Prepare for a SOC 1 and SOC 2 Examination



September 24, 2019

Introduction

- Eric Davis, CPA
  - Senior, Risk Advisory Services
  - 5+ years of SOC experience
  - Industries: healthcare, logistics, mortgage and banking and technology

Agenda

- What is a SOC Report?
- Terminology
- Types of SOC Reports
- Contents of a SOC Report
- How to Prepare for a SOC Examination
- Timeline
- Keys to Success
- Common Mistakes

What is a SOC Examination?

- System and Organization Control (SOC) Examinations:
  - Suite of services developed by the American Institute of CPAs (AICPA)
  - Attestation engagements that must adhere to AICPA standards (SSAE 18)
  - Examinations must be performed by a CPA
  - The output is an internal control report that provide users (i.e., customers) of an outsourced service with information on how to address the risks associated with the service they are outsourcing

Terminology

- **Service Organization** – organization or segment of an organization that operates information systems and/or provides services to other entities
- **Service Auditor** – a practitioner who reports on controls at a service organization
- **User Entity** – an entity that uses a service organization
- **User Auditor** – an auditor who audits and reports on the financial statements of a user entity
- **Subservice organization** - service organization(s) used by another service organization to perform some of the services provided to user entities
- **Carve-out method** - the controls of the subservice organization are excluded from the SOC report
- **Inclusive Method** - the controls of the subservice organization(s) are presented (and tested in the case of a Type 2 report) within the SOC report. Both the service organization and subservice organization's management must provide written assertions that are included in the report
- **Complementary user entity controls** - controls for which management of the service organization assumes will be in place at user entities in regards to the actual services being performed by the service organization
- **Complementary subservice organization controls** - controls expected to be implemented at the carved-out subservice organizations that are necessary to meet the applicable control objectives or trust services criteria, either alone or in combination with controls at the service organization

SOC Report Options

Report	Scope/Focus	Summary	Applicability
SOC 1	Internal Control Over Financial Reporting	Detailed report for customers and their auditors	▪ Focused on financial reporting risks and controls specified by the service provider ▪ Applicable where the service provider performs financial transaction processing systems
SOC2	Security, Availability, Processing Integrity, Confidentiality and/or Privacy	Detailed report for customers and specified parties	▪ Focused on Security, Confidentiality, Availability, Processing Integrity and/or Privacy ▪ Applicable to a broad variety of systems
SOC 3	Same as SOC 2	Short report that can be generally distributed	▪ Same as above without disclosing detailed controls and testing

Other SOC Report Options

- SOC for Cybersecurity– reporting framework through which organizations can communicate the effectiveness of their cybersecurity risk management program

- SOC for Supply Chains– still under development by the AICPA but will report on an entity’s system and controls to enable users to better understand and manage the risks arising from business relationships with their supplier and distribution networks

Types of SOC Reports

- Type 1 - Report on the fairness of the presentation of management’s description of the system and the suitability of the design of the controls

- Type 2 - Report on the fairness of the presentation of management’s description of the system and the suitability of the design and operating effectiveness of the controls

SOC Report Summary

- SOC 1 Type 1
- SOC 1 Type 2
- SOC 2 Type 1
- SOC 2 Type 2
- SOC 3
- SOC for Cybersecurity
- SOC for Supply Chain

Contents of a SOC Report

- Independent Service Auditor’s Report that includes the following:
  - The scope of the report
  - Each party’s responsibilities
  - Inherent limitations
  - Service auditor’s opinion about whether:
    - The description is fairly stated
    - The controls were suitably designed
    - The controls operated effectively (Type 2 only)
- Management’s Assertion
  - Letter signed by organization management asserting to the above

Contents of a SOC Report (cont.)

SOC 1	SOC 2
The types of services provided, including the classes of transactions processed.	The types of services provided
• Procedures in both automated and manual systems used to provide such services • The information used in the performance of the procedures • How the service organization’s system captures and addresses significant events and conditions other than transactions • The process used by the service organization to prepare reports and other information for user entities.	The components of the service organization’s system, which are as follows: • Infrastructure • Software • People • Procedures • Data The boundaries or aspects of the system covered by the description
Relevant aspects of the service organization’s • control environment • risk assessment process • information and communications (including the related business processes), • control activities • monitoring activities that are relevant to the services provided	Relevant aspects of the service organization’s • control environment • risk assessment process • information and communications • security policies • monitoring controls

Contents of a SOC Report (cont.)

SOC 1	SOC 2
Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them. For information provided to, or received from, subservice organizations: • the role of the subservice organizations or other parties, and • the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls	Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them. For information provided to, or received from, subservice organizations: • the role of the subservice organizations or other parties, and • the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls
Control objectives and control activities designed to meet the control objectives	The applicable trust services criteria and the related controls designed to meet those criteria.
Complementary subservice organization controls Complementary user entity controls	Complementary subservice organization controls Complementary user entity controls
Changes to the system that occurred during the report period	Changes to the system that occurred during the report period

Contents of a SOC Report (cont.)

- Information Provided by the Independent Service Auditor
  - Control activities specified by the service organization to meet the applicable trust service criteria (SOC 2) or the specified control objectives (SOC 1)
  - Service auditors tests of effectiveness and results (Type II reports)
- Other information provided by the service organization
  - Not covered by the service auditor’s report
  - Additional information such as business continuity and disaster recovery plans, management’s responses to auditor’s exceptions, etc.

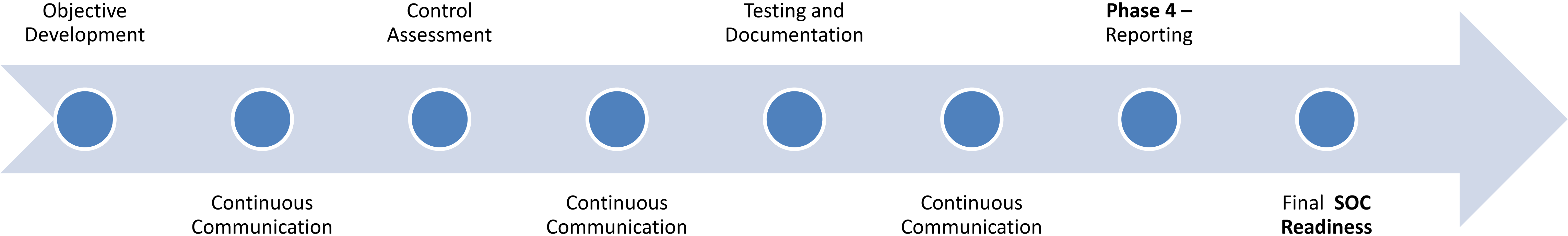
How to Prepare for a SOC Examination

- Determine who the users are and what the users' needs are and type of report needed (e.g., contractual requirements)
- Establish testing locations and information systems in scope
- Review scope and impact subservice organizations will have on report (carve out or inclusive)
- Identify risks (What could go wrong?)
- Identify internal control objectives and activities to mitigate risks
- Determine what controls are relevant to or required by users
- Determine the proper report period or as of date (match with users needs)
- Ensure there is proper evidence to support that controls to be tested is retained
- Relevant aspects of the control environment should be assessed
- Develop, review and update system description (control environment, services, scope, third parties, risks, control objectives, control activities, testing strategy, changes)
  - Changes in processes, systems and the control environment must be considered and incorporated into the description of the system in subsequent years

How to Prepare for a SOC Examination (cont.)

- Conduct a self assessment or a readiness assessment to determine whether controls are in place and properly designed. Readiness assessments can help identify opportunities for control optimization and for improvement opportunities to processes and controls. They can also facilitate evaluation of documentation maintained to support operation of controls.
- Appointing one or two personnel as project managers to facilitate coordination of the examination procedures and documentation requests.
- Create project plan and assign responsibilities
- Communicate the importance of the SOC examination to employees and control owners to set expectations, build awareness and support a control-minded culture.
- Proactive communication with process owners, auditors, users,

Example Timeline (SOC 1 Readiness)



Phase 1 -

Control Objective Development

Continuous Communication

Phase 2 – Preliminary Control Assessment

Continuous Communication

Phase 3 – Limited Control Testing and Documentation

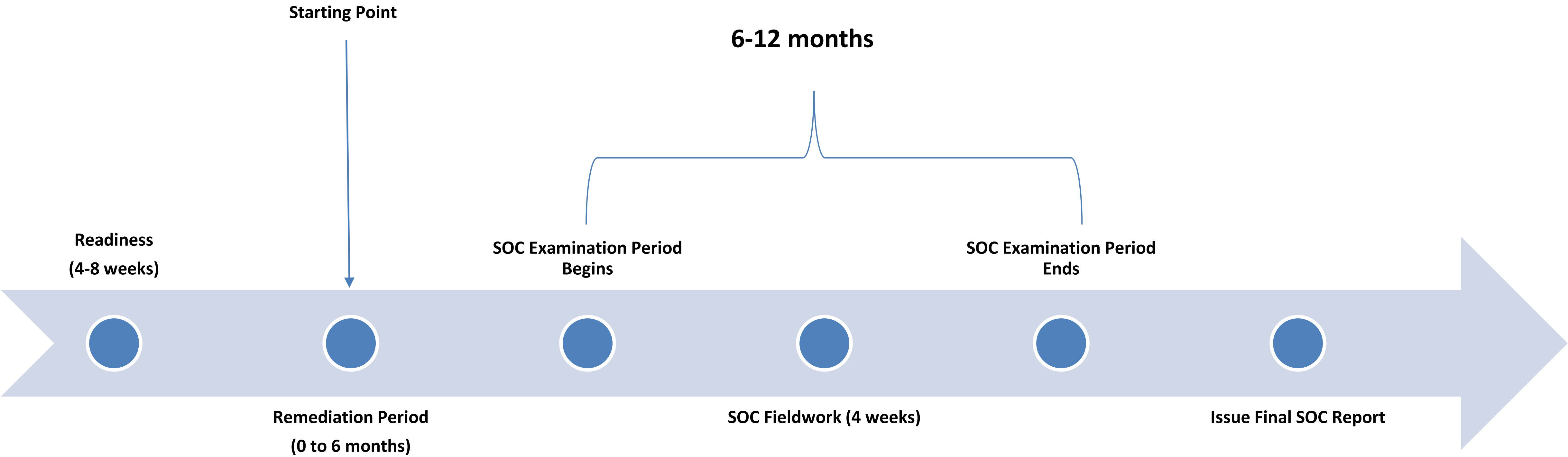
Continuous Communication

Phase 4 – Reporting

Final **SOC Readiness Assessment** Report

(4-8 weeks)

Example Timeline (SOC Report)



Starting Point

6-12 months

Readiness

(4-8 weeks)

Remediation Period

(0 to 6 months)

SOC Examination Period Begins

SOC Fieldwork (4 weeks)

SOC Examination Period Ends

Issue Final SOC Report

Common Mistakes

- Not defining proper controls or not defining controls accurately
- During process walkthroughs, process owners do not accurately describe the process
- No accountability at the service organization to manage the process
  - Can delay timing of testing and the report
- Insufficient documentation to evidence the control is designed appropriately and operating effectively (Type II only)
- Inability to provide complete/accurate populations for the defined report period
- Lack of ownership as to who will write or prepare the system description
  - Report delays/missed deadlines

Keys to Success

- Executive buy-in
- Understand that multiple departments will be involved
  - IT
  - Security
  - Development
  - Human Resources
  - Operations
  - C-suite
  - Third parties (depending on services provided)
- Assigning an appropriate internal project manager
- Managing customer/user expectations
- Managing internal stakeholder expectations

Keys to Success (cont.)

- Being honest and transparent during readiness
- Dedicating time and resources during remediation
- Standardizing and centralizing controls
- Look for opportunities for automation
  - Take advantage of system controls
  - Look to incorporate process automation
- Document review controls thoroughly
  - Ensure the auditor can verify what the review entailed (who, what, why, when and how)

Keys to Success (cont.)

- Maintaining audit documentation so it can be easily retrieved
- Providing requested documentation prior to fieldwork
  - Make sure your auditor provides a request list at least one week in advance
- Understanding that your system of internal controls is continuous and part of your daily processes and procedures

Questions?