Crowe

Smart decisions. Lasting value.™

SOC Reports: Demystifying Service Organization Responsibilities

October 23, 2019

Introductions

Meet your Speakers

Lisa Stinson, CPA
Crowe Consulting Senior Manager
217.862.2710
Lisa.Stinson@crowe.com

Kelly Bucci, CPA, CFE, CGMA
Crowe Consulting Manager
217.862.2712
Kelly.Bucci@crowe.com

Agenda

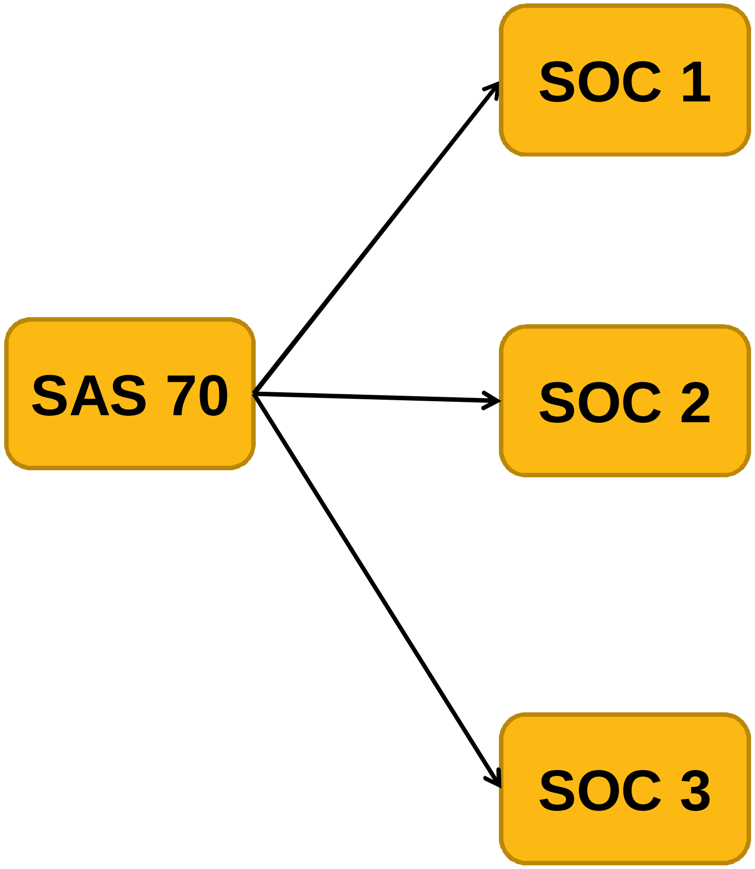
- Service Organization Controls (SOC) Overview
  - Types of Reports
  - Report Contents/Structure
  - Examples
- Entity User Responsibilities
- Common Findings/Issues
- Questions

Course Objectives

- Gain an understanding of the purpose and content of a Service Organization Controls (SOC) report.
- Understand an entity's responsibility related to SOC reports.
- Determine controls necessary when using a service organization, whether or not a SOC report is provided.
- Identify user control considerations and how to take appropriate action related to user responsibilities.
- Learn how to identify significant subservice organizations and the responsibilities an entity is required to take over subservice organization controls.

Service Organization Controls(SOC) Overview

History and Evolution of SOC Reporting



SOC Reporting Options

- **SOC 1**
  - SOC for Service Organizations: ICFR – Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting

- **SOC 2**
  - SOC for Service Organizations: Trust Services Criteria – Report on Controls at a Service Organization Relevant to **Security (Common Criteria) , Availability, Processing Integrity, Confidentiality or Privacy**

- **SOC 3**
  - SOC for Service Organizations: Trust Services Criteria for General Use Report

- **SOC for Cybersecurity**
  - Reporting on an Entity's Cybersecurity Risk Management Program and Controls

SOC 1 Overview

What is a SOC 1?

- Prepared under SSAE 18 (after May 1, 2017)
- Designed to address controls likely to be relevant to user entities' internal control over financial reporting
- Provides audit evidence more relevant to a financial audit engagement
- Two types:
  - Type 1 – Design of controls to achieve control objectives as of specified date
  - Type 2 – Design and operating effectiveness of controls to achieve control objectives throughout a specified period

SOC 2 Overview

What is a SOC 2?

A report on controls at a service organization relevant to:

- **Security**: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives
- **Availability**: Information and systems are available for operation and use to meet the entity's objectives
- **Confidentiality**: Information designated as confidential is protected to meet the entity's objectives
- **Privacy**: Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives
- **Processing integrity**: System processing is complete, valid, accurate, timely and authorized to meet the entity's objectives

Care should be taken when utilizing a SOC 2 or SOC 3

SOC 3 Overview

What is a SOC 3?

A report designed to meet the needs of users who need assurance about the controls at a service organization relevant to security, availability, processing integrity confidentiality, or privacy (similar to SOC 2), but do not have the need for or the knowledge necessary to make effective use of a SOC 2 Report. Because they are general use reports, SOC 3 reports can be freely distributed.

Key Parties in a SOC Report

Objective of a SOC 1 Report and Definition of Key Players

The Service Auditor’s Report is intended to provide customers and independent accountants of customers with an audit opinion over the service organization’s internal controls over financial reporting

Service Provider
(Company Issuing SOC Report)

User
(Customer of the Service Provider)

Service Auditor
(Auditor Opining On SOC Report)

User Auditor
(External Auditor of the User)

Report Content/Structure

- Section I: Independent Service Auditor’s Report (Scope, Responsibilities and Opinion)

  Prepared By Service Auditor
- Section II: Management Assertion & Description of Systems (Controls)

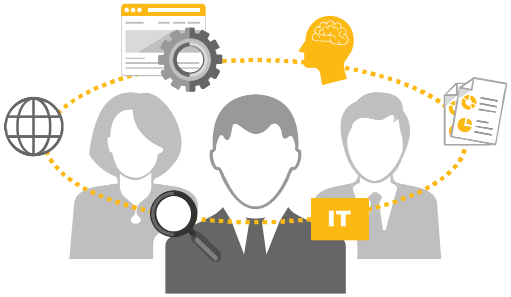
  Prepared By Service Provider
- Section III: Complementary User Entity Controls

  Prepared By Service Provider
- Section IV: Subservice Organizations

  Prepared By Service Provider
- Section V: Types/Description of Tests of Operating Effectiveness & Control Objective Matrices (Testing/Findings)

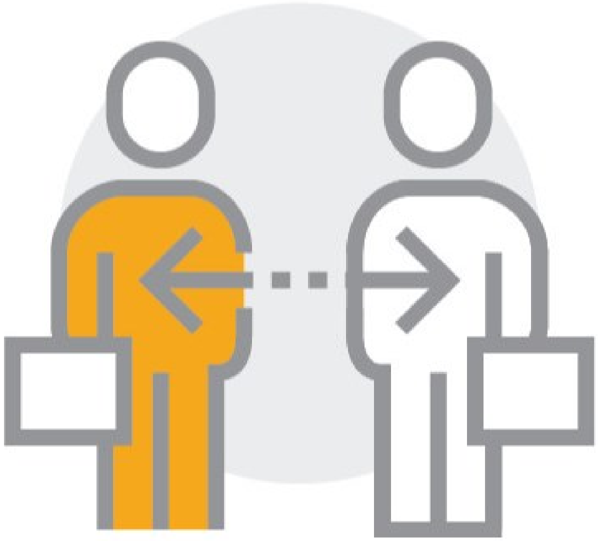
  Prepared By Service Auditor
- Section VI: Additional Information

  Prepared By Service Provider



Service Provider Examples

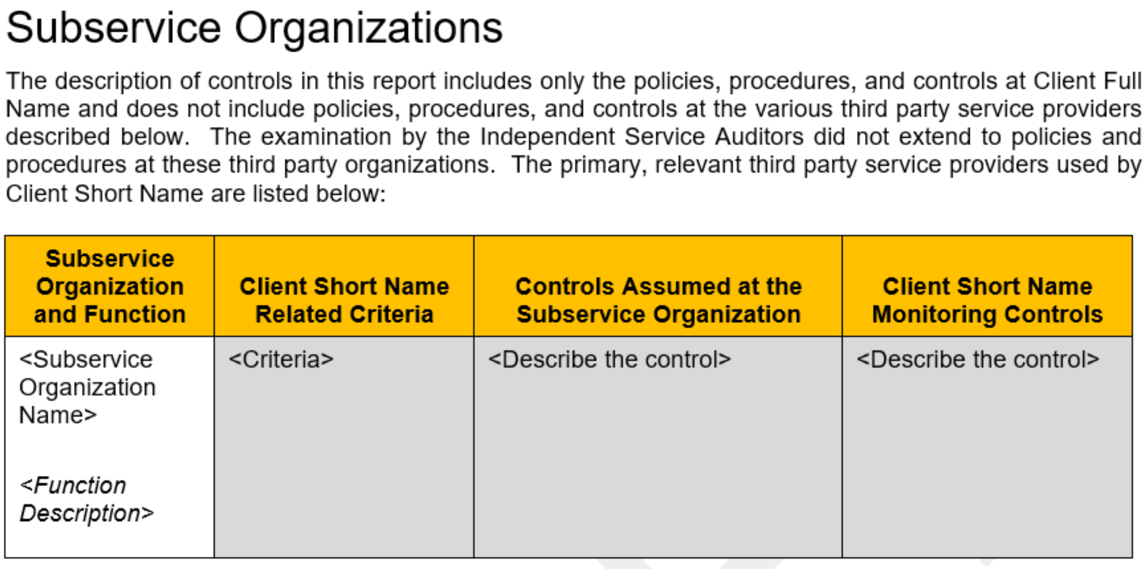
- Outsourced payroll
- Program administration
  - Investment programs
  - Retirement programs
  - College Savings programs
  - Healthcare Programs
- Payment processor
- Loan servicing
- Investment services



Entity User Responsibilities

Entity User Responsibilities – Inventory of Key Providers

- A user entity must evaluate all service organizations utilized and whether the services provided by the organization are significant to its operations
- Subservice organizations should also be analyzed
- List of organizations and rationale for significance should be documented.



Subservice Organizations

The description of controls in this report includes only the policies, procedures, and controls at Client Full Name and does not include policies, procedures, and controls at the various third party service providers described below. The examination by the Independent Service Auditors did not extend to policies and procedures at these third party organizations. The primary, relevant third party service providers used by Client Short Name are listed below:

Subservice Organization and Function	Client Short Name Related Criteria	Controls Assumed at the Subservice Organization	Client Short Name Monitoring Controls
<Subservice Organization Name> *<Function Description>*	<Criteria>	<Describe the control>	<Describe the control>

Entity User Responsibilities – Review

- Determine when the SOC Reports are being issued to timely obtain the reports

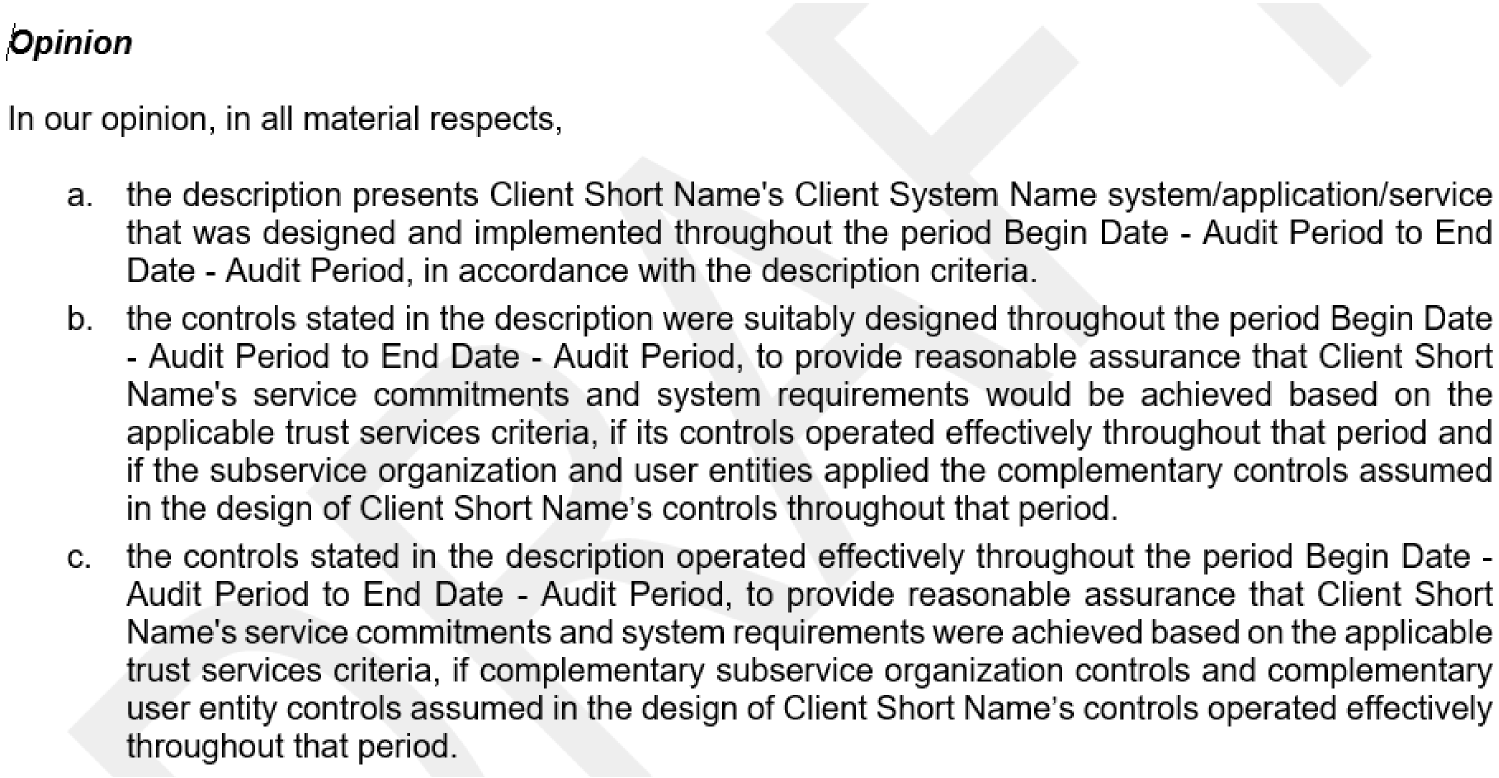
- Perform a thorough review of the SOC Reports

- Document the review

- Determine the scope of the report covers your entity’s key system/service

Entity User Responsibilities - Opinion

Section I: Independent Service Auditor’s Report



Opinion

In our opinion, in all material respects,

a. the description presents Client Short Name's Client System Name system/application/service that was designed and implemented throughout the period Begin Date - Audit Period to End Date - Audit Period, in accordance with the description criteria.

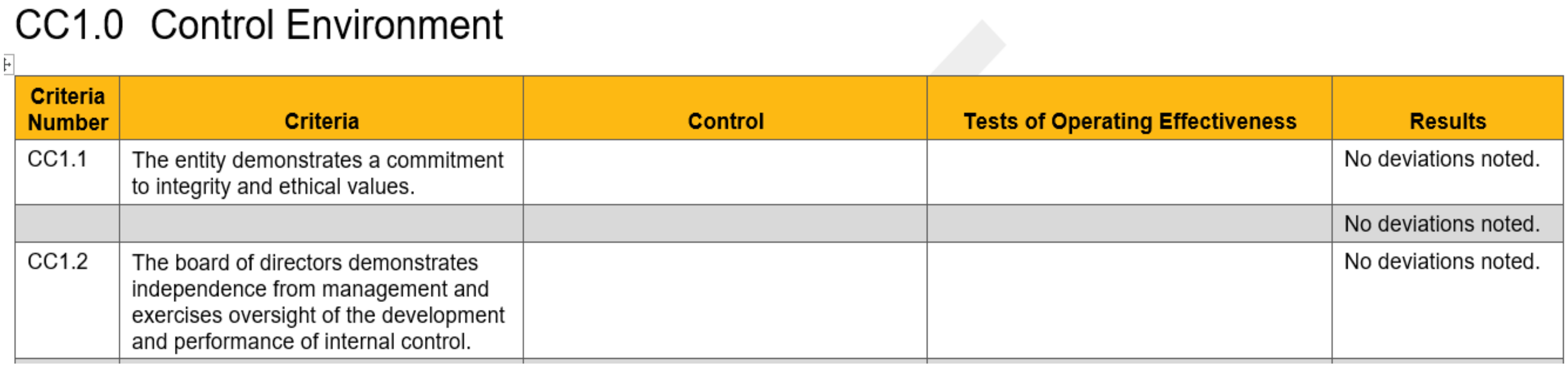
b. the controls stated in the description were suitably designed throughout the period Begin Date - Audit Period to End Date - Audit Period, to provide reasonable assurance that Client Short Name's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Client Short Name’s controls throughout that period.

c. the controls stated in the description operated effectively throughout the period Begin Date - Audit Period to End Date - Audit Period, to provide reasonable assurance that Client Short Name's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Client Short Name’s controls operated effectively throughout that period.

Entity User Responsibilities – Controls/Test Results

Independent Service Auditor’s Description of Tests of Controls and Results (Testing)

- Do controls cover services provided by organization to our entity?
- Were the controls adequate for services being provided?
- Were findings/deviations identified related to the controls?

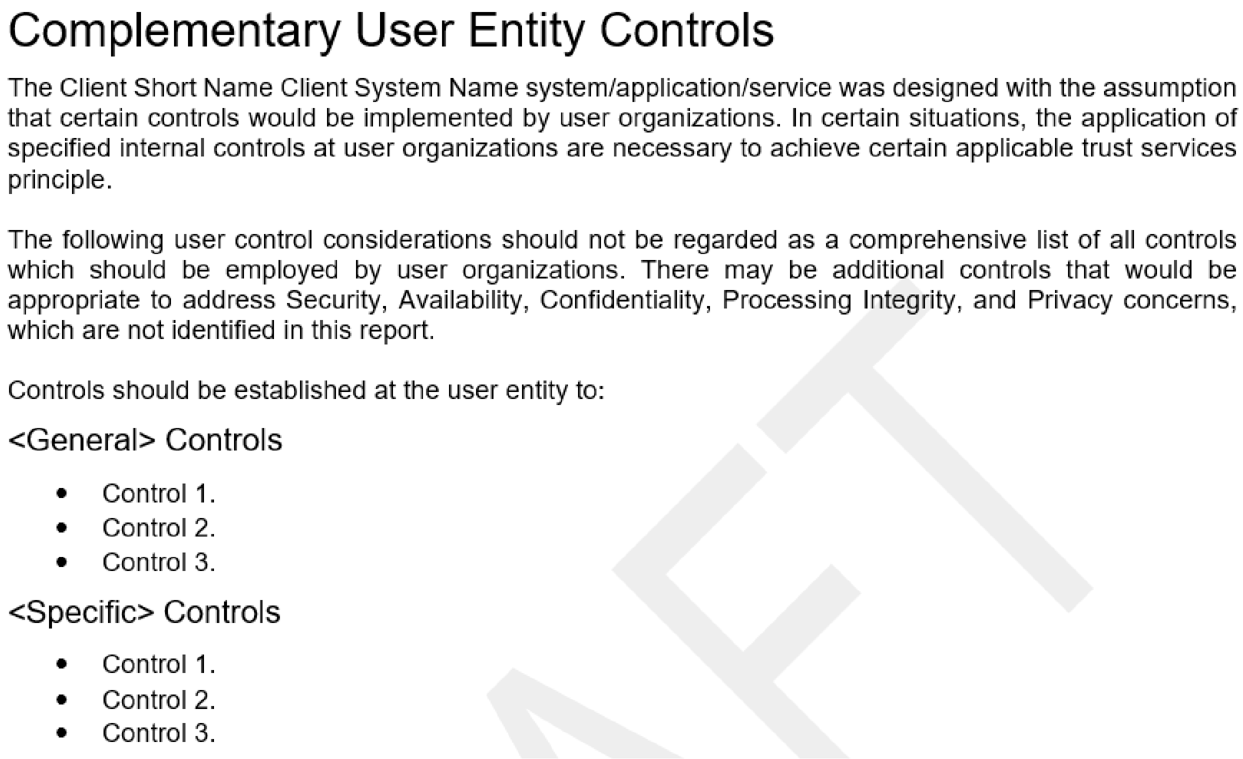


CC1.0 Control Environment

Criteria Number	Criteria	Control	Tests of Operating Effectiveness	Results
CC1.1	The entity demonstrates a commitment to integrity and ethical values.			No deviations noted.
				No deviations noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			No deviations noted.

Entity User Responsibilities – Complementary User Controls

Section V: Complementary User Entity Controls



Complementary User Entity Controls

The Client Short Name Client System Name system/application/service was designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specified internal controls at user organizations are necessary to achieve certain applicable trust services principle.

The following user control considerations should not be regarded as a comprehensive list of all controls which should be employed by user organizations. There may be additional controls that would be appropriate to address Security, Availability, Confidentiality, Processing Integrity, and Privacy concerns, which are not identified in this report.

Controls should be established at the user entity to:

<General> Controls

- Control 1.
- Control 2.
- Control 3.

<Specific> Controls

- Control 1.
- Control 2.
- Control 3.

Common Findings/Issues

Common Findings/Issues

- Lack of service organization and subservice organization analysis
- Lack of timely review of SOC Report
- Lack of adequate review/understand of SOC Report
- Failure to document review of SOC Report
- Failure to review and/or implement user control considerations
- Failure to review subservice organizations
- Failure to gain an understanding of service organization controls when no SOC report exists
- Failure to determine the SOC report obtained actually covers the services provided to your entity

BEST PRACTICES?

Questions?

Lisa Stinson, CPA
Crowe Consulting Senior Manager
217.862.2710
Lisa.Stinson@crowe.com

Kelly Bucci, CPA, CFE, CGMA
Crowe Consulting Manager
217.862.2712
Kelly.Bucci@crowe.com