The SOCial Hour – Preparing for Your First SOC 2 Examination

ASA Webinar

August 13, 2024

forvis mazars

Introductions

Preparing for Your First SOC 2 Examination
Meet the Presenters

Karen Cardillo
Director, SOC & HITRUST

336.259.6611
karen.cardillo@us.forvismazars.com

Ryan Boggs
Principal, SOC & HITRUST

828.989.3176
ryan.boggs@us.forvismazars.com

Agenda

1. Introductions
2. SOC Basics
3. Road Map for a Successful First Time SOC 2 Examination
4. Closing

SOC Basics

SOC Basics

SOC Reporting Overview

- **System and Organization Controls (SOC) for Service Organizations**
  - SOC for Service Organizations Reports are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address risks associated with an outsourced service.
- **Why SOC Reporting?**
  - As more and more companies use third-party service providers, there is more demand for a detailed understanding of the processes and controls of these third-party service providers (referred to as service organizations).
  - Service organizations need to show their customers (referred to as user organizations) or prospective customers what processes and controls they have in place around internal controls over financial reporting and/or information security controls around the systems or services they provide.

For CPAs

Provides information to user auditors and service auditors on understanding and performing SOC for Service Organizations Reports

For Users & User Entities

Provides information to user entities on how to mitigate the risks associated with outsourcing services

For Service Organizations

Provides information to service organizations that they can use to build trust and confidence in their systems

SOC Basics

SOC Report Purpose

	SOC 1	SOC 2
What Is Covered by the Report?	Controls related to financial reporting for user organizations	Controls relevant to security, availability, confidentiality, processing integrity, and/or privacy
Intended Audience	Auditors and management of user organizations ("auditor-to-auditor communication")	Auditors, regulators, stakeholders, *e.g.*, management, business partners, customers
Report Format	Long form which includes a detailed description of the system and controls	Long form which includes a detailed description of the system and controls

- SOC 1 & SOC 2 reports are the most common and most useful for vendor risk management purposes.
- Selecting the correct report for the intended purpose is critical for obtaining the desired result
- This presentation will focus on preparing for a SOC 2 examination

forvis mazars

SOC Basics

SOC 2 Framework Overview

- **Five trust services categories:**
  - Security
  - Availability
  - Confidentiality
  - Processing Integrity
  - Privacy
- Criteria for each category is predefined and set forth by the AICPA
- Criteria for Security is required at a minimum, but criteria for additional categories of Availability, Confidentiality, Processing Integrity, and Privacy can be added at management's discretion

Preparing for Your First SOC 2 Examination
SOC Basics

SOC 2 Trust Services Categories

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. (Required for all SOC 2 examinations)

Availability

Information and systems are available for operation and use to meet the entity's objectives.

Processing Integrity

System processing is complete, valid, accurate, timely, and authorized 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 of to meet the entity's objectives.

SOC Basics

SOC 2 Criteria Based on Trust Services Category

- **Security:** Baseline line common criteria for required for all SOC examinations, 33 criteria organizations into nine criteria groups
- **Availability:** Three additional criteria
- **Processing Integrity:** Five additional criteria
- **Confidentiality:** Two additional criteria; however, IT system scope may expand significantly as controls must extend to wherever the in-scope confidential data goes
- **Privacy:** 17 additional criteria organized into eight criteria groups.

SOC Basics

Confidentiality & Privacy Distinction

- The Privacy Trust Services Category is designed to apply only to **Protected Health Information** (PHI) or **Personally Identifiable Information** (PII)
- The Confidentiality Trust Services Category is designed to apply more broadly to various types of sensitive information
- Sensitive information varies from organization to organization but often includes nonpublic information such as the following:
  - regulatory compliance information;
  - financial information used for both internal and external reporting purposes;
  - proprietary information provided by business partners
- Organizations who have access to PHI or PII (usually within the healthcare or financial services industries) include criteria relevant to privacy in the scope of their SOC 2 Examinations

SOC Basics

SOC 2 Examination Scope Terminology

SOC 2 Examinations can either be as of a specified date or cover a period of time.

- **SOC 2, Type 1 Examination**
  - Not to be confused with a SOC 1, a SOC 2, Type 1 report signifies that the report is only as of a specific point in time
  - This type of report includes design and implementation but does not include operating effectiveness of controls
  - Practical Use: Most useful for providing assurance to clients and business partners that controls are designed and implemented
- **SOC 2, Type 2 Examination**
  - A Type 2 report signifies that the report covers the operations of controls over a specified period of time
  - This type of report includes design, implementation, and operating effectiveness of controls
  - Period of time should not be less than three months
  - Practical Use: Most useful for providing assurance to clients and business partners that controls are designed and operating effectively over a period of time

Road Map for a Successful First Time SOC 2 Examination

Road Map for a Successful First Time SOC 2 Examination

Setting Expectations

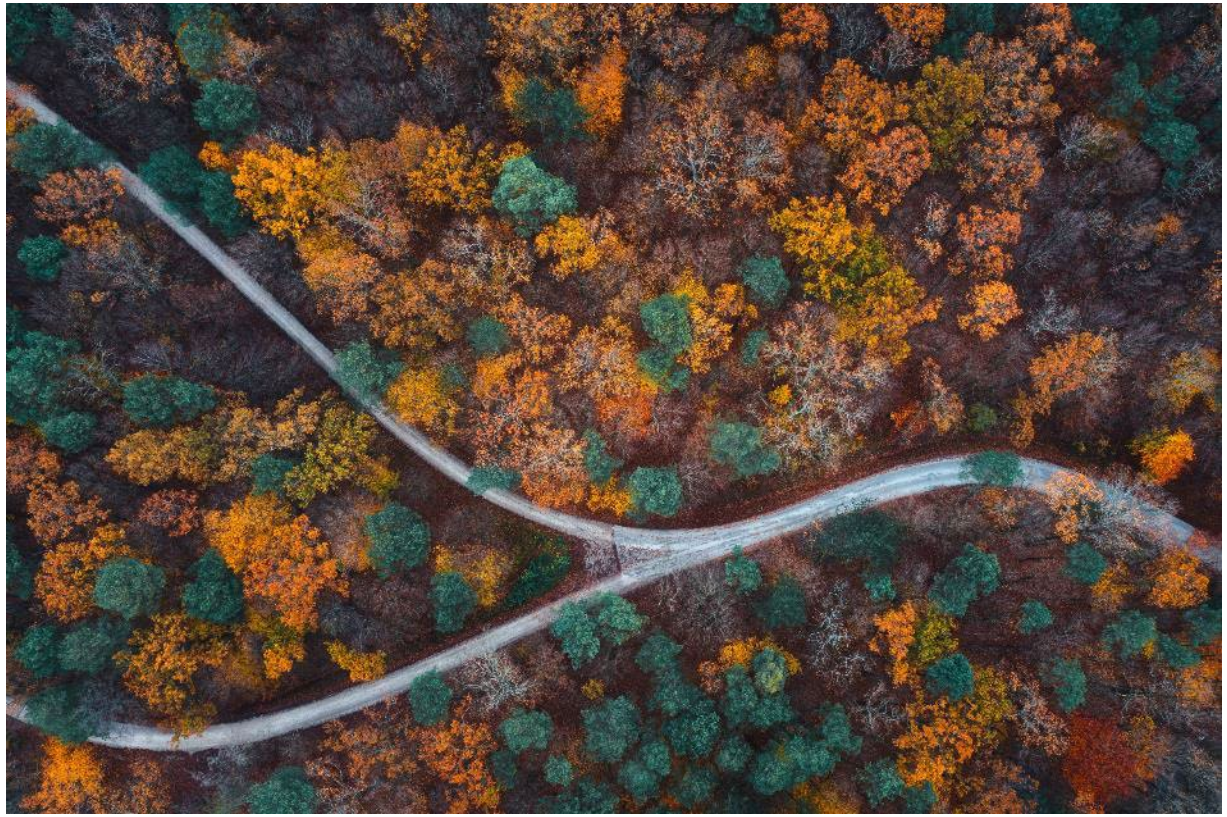
- SOC 2 examinations demonstrate a business' commitment to data security
- A SOC 2 examination engagement is **not a self-assessment**, an **independent certified public accountant is required** to perform the assessment and issue an opinion
- A SOC 2 examination that **results in control deviations or a qualified opinion** could be **viewed negatively in the market**, so it is important to prepare for your first SOC 2 examination to help ensure a successful audit
- When starting from scratch, a **typical timeline** from scoping the future examination to delivery of your first SOC 2 Type 2 Examination Reports ranges from **12 to 18 months**

Preparing for Your First SOC 2 Examination

Road Map for a Successful First Time SOC 2 Examination

Milestones

1. Understand the SOC 2 Requirements
2. Set the Project Scope
3. Perform an Internal Gap Analysis
4. Develop Policies and Procedures
5. Implement New Policies and Security Controls
6. Provide Training and Awareness
7. Pre-Examination Readiness Assessment
8. Gap Remediation
9. Begin SOC 2 Examination



Road Map for a Successful First Time SOC 2 Examination

Understanding the SOC 2 Requirements

- Familiarize yourself with the SOC 2 framework and its five trust service criteria: security, availability, processing integrity, confidentiality, and privacy
- Review the AICPA SOC 2 Trust Services Criteria to understand the specific controls and requirements for each criterion
- Identify the relevance of each criterion to your organization’s operations

Road Map for a Successful First Time SOC 2 Examination

Setting the Project Scope

- Identify your principal service commitments and system requirements made to users
- Identify the trust service categories most relevant to the services you provide/most requested by your users or business partners
- Define the scope of your future SOC 2 examination, including the systems, processes, and/or services that will be evaluated
- Identify and involve relevant subject matter experts during planning and scoping, including members from IT, HR, and Legal
- Identify managed services (subservice organizations) provided by others required for you to achieve your own service commitments to customers (for example, cloud service providers, data centers, managed IT service providers)

Road Map for a Successful First Time SOC 2 Examination

Performing the Internal Gap Analysis

- Identify the relevant trust service criteria that apply to your organization's operations
- Document existing controls and processes, and assess their effectiveness in meeting your organization’s principal service commitments and system requirements based on the SOC 2 criteria
- Consider the applicability and relevance of the Points of Focus defined for each applicable SOC 2 criterion (not all Points of Focus are required to be addressed, but are useful in identifying risks)
- Conduct a high-level gap analysis and risk assessment to identify areas where your current practices and controls fall short of SOC 2 criteria requirements

forvis mazars

Preparing for Your First SOC 2 Examination

Road Map for a Successful First Time SOC 2 Examination

Developing Policies & Procedures

- Identify and assign controls to subject matter experts/control owners
- Develop and implement policies and procedures to address any control gaps identified during the high-level gap analysis
- Ensure that policies cover critical areas such as access control, data protection, change management, risk management, vendor management, incident response, and monitoring
- Document procedures and responsibilities for implementing and enforcing policies and procedures

Road Map for a Successful First Time SOC 2 Examination

Implementing New Policies & Security Controls

- Prioritize assess gaps based on potential impact and feasibility of remediation
- Roll out new policies and procedures and ensure availability to teams for implementation
- Implement missing technical and administrative controls to safeguard data
- Establish regular security monitoring, key performance indicators, and logging practices
- Establish control documentation practices, continuous monitoring, and a process regular reviews of policies and procedures
- Establish a process for periodic (no less than annual) risk assessments to identify emerging threats and vulnerabilities

Road Map for a Successful First Time SOC 2 Examination

Providing Training & Awareness

- Develop and provide training and awareness programs for employees and contractors to help ensure that they understand their roles and responsibilities
- Training and awareness programs should cover security best practices, data handling procedures, and incident response protocols at a minimum
- New hires should be required to undergo training within a finite period of time of hire
- Existing employees should be required to undergo training on at least an annual basis

Preparing for Your First SOC 2 Examination

Road Map for a Successful First Time SOC 2 Examination

Pre-Examination Readiness Assessment

- Conduct a readiness assessment to help ensure that all controls and documentation to support implementation and operation of the controls are in place
- Confirm populations for transaction-based controls, *e.g.*, access provisioning, access deprovisioning, and change management, are available over a period of time and are verifiably accurate and complete
- Verify that policies and procedures are accurate and up-to-date
- Develop description of the system (“system narrative”) based on policies and procedures

Road Map for a Successful First Time SOC 2 Examination

Gap Remediation

- Confirm identified gaps with control owners
- Develop recommendations for remediating gaps
- Prioritize gaps and establish timeline
- Track gaps to remediation
- Confirm remediation of all identified gaps

Road Map for a Successful First Time SOC 2 Examination

Beginning a SOC 2 Examination

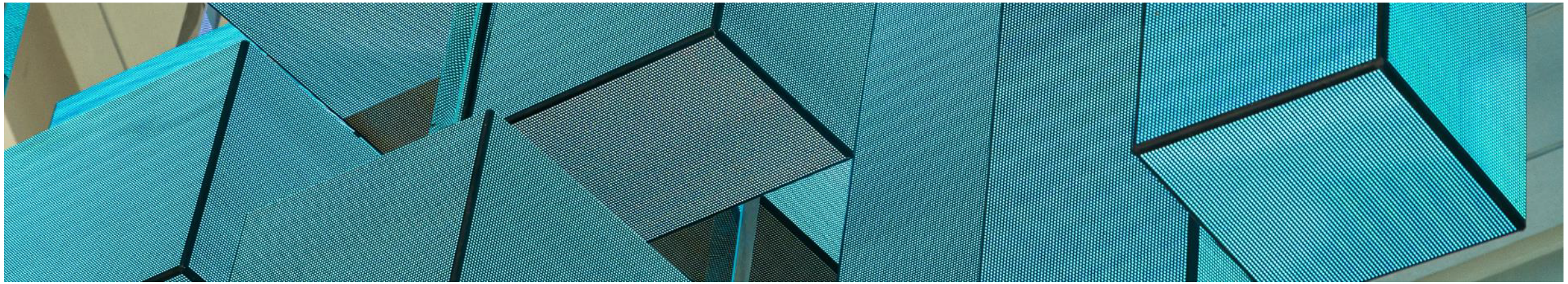
- All gaps should be cleared before you undergo a SOC 2 Type 1 examination or before you begin your specified period for a SOC 2 Type 2 examination
- Specified period in a SOC 2 Type 2 examination is the period of time for which the controls are going to be assessed
- Select a qualified CPA firm with experience in conducting SOC 2 examinations
- Work with the CPA firm to schedule the examination and provide necessary documentation and access to systems

Road Map for a Successful First Time SOC 2 Examination

Common Pitfalls

Beware of **common pitfalls** and showstoppers

- Segregation of duties *not* enforced
- User access *not* being deprovisioned timely based on termination date
- Retention period of logs and historical evidence set to a period that is *less than* your SOC 2 Type 2 examination period
- Inadequate monitoring of services provided by critical vendors



Road Map for a Successful First Time SOC 2 Examination

Documentation Expectations

- Oftentimes, process owners are completing or performing the controls but are not documenting what they have done and there is no audit trail to "test" during the audit
- If it is not documented, it did not happen
- When in doubt, over document

Road Map for a Successful First Time SOC 2 Examination

Additional Tips

- Educate the control owners that during the readiness assessment, we are wearing our consulting hats
- Do not try to hide issues during the Readiness Assessment, be as open and honest as possible. This way, we can identify areas that need to be addressed prior to the actual examination
- Do not provide your “best” example during the Readiness Assessment
- You **don’t** have to undergo the journey to SOC 2 compliance alone – leveraging readiness assessment services from an experienced CPA firm like Forvis Mazars can help you prepare for a successful first SOC 2 examination

Questions?

Contact

Forvis Mazars

Karen Cardillo
Director
SOC & HITRUST Practice
karen.cardillo@us.forvismazars.com

Ryan Boggs
Principal
SOC & HITRUST Practice
ryan.boggs@us.forvismazars.com