The SOCial Hour – Preparing for Your First SOC 1 Examination

December 2024

forvis mazars

Introductions

Preparing for Your First SOC 1 Examination

Meet the Presenters

Karen Cardillo
Director, SOC and HITRUST

336.259.6611
karen.cardillo@us.forvismazars.com

Ryan Boggs
Principal, SOC and HITRUST

828.989.3176
ryan.boggs@us.forvismazars.com

Agenda

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

SOC Basics

Preparing for Your First SOC 1 Examination

SOC Basics

SOC Reporting Overview

- **System and Organization Controls (SOC)** for Service Organizations
  - SOC 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

forvis mazars

Preparing for Your First SOC 1 Examination

SOC Basics

Service Organization or Service Provider

Organization providing the outsourced service

Subservice Organization

Organization used by the service organization to provide third-party services to the service organization

User Organization or User Entity

Organization receiving the outsourced service

Service Auditor

Auditor performing SOC examination of the service organization's controls

User Auditors

External auditors of the user organization/entity

Control Activity

Activities, procedures, and processes performed by the service organization to help prevent risks
and achieve objectives

forvis mazars

Preparing for Your First SOC 1 Examination

SOC Basics

SOC 1

These attestation reports are specifically intended to meet the needs of entities that use service organizations (user entities) as their financial statement auditors (user auditors) use these reports to help evaluate the effect of the controls at the service organization on the user entities' financial statements.

SOC 2

These attestation reports are intended to meet the needs of a broad range of users that need assurance about a service organization's controls as they relate to the security, availability, and processing integrity of the systems the service organization uses to process its users' data and the confidentiality and privacy of the information processed by those systems.

SOC 3

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

SOC for Cybersecurity

The AICPA's cybersecurity risk management reporting framework helps organizations communicate about the effectiveness of their cybersecurity risk management programs.

- SOC 1 and 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 1 Examination

Preparing for Your First SOC 1 Examination

SOC 1 Basics

FAQ

Help! The contract I am negotiating says I am required to undergo a **SSAE 18** or **SSAE 21** examination. What does that even mean?

- SSAE 18 and SSAE 21 are examination standards set forth by the AICPA that govern all SOC examination engagements
- If contract requirements only specify undergoing an SSAE 18 or SSAE 21 examination, more information would be required to determine exactly which type of SOC examination is being requested

Preparing for Your First SOC 1 Examination

SOC 1 Basics

SOC 1 Report Purpose

	SOC 1
What Is Covered by the Report?	Controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting
Intended Audience	Management of the service organization, management of user organizations, and the auditors of the user organizations ("auditor-to-auditor communication")
Report Format	Long form which includes a detailed description of the service organization's system, control objectives, and controls

- A service organization's controls are relevant to a user entity's internal control over financial reporting when they are part of the user entity's information and communications component of internal control maintained by the service organization
- Service organizations frequently receive requests from user entities for these reports because the auditors of the user entities' financial statements need them to obtain information about controls at the service organization that may affect assertions in the user entities' financial statements

Preparing for Your First SOC 1 Examination

SOC 1 Basics

Why SOC 1 Reporting Matters

- Builds trust with clients and partners
- Enhances internal control systems
- Reduces the risk of financial misstatement of users of the company's service or system
- Demonstrates your commitment to regulatory compliance and corporate governance

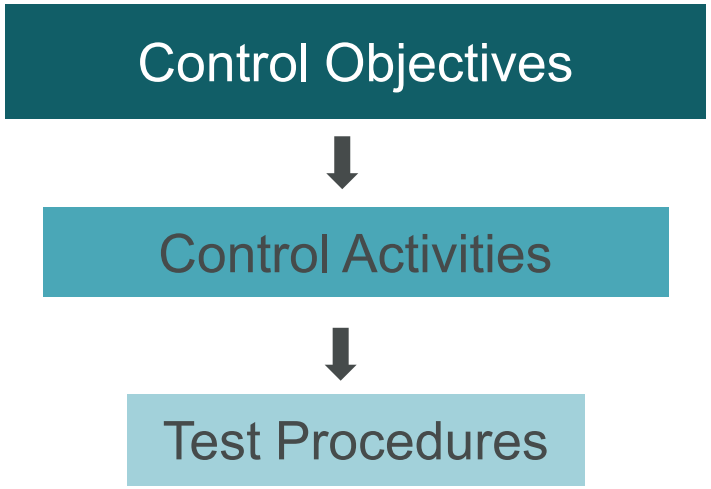
forvis mazars

Preparing for Your First SOC 1 Examination

SOC 1 Basics

How Is Compliance for a SOC 1 Report Organized?

- SOC 1 Reports are comprised of **control objectives**
- A **control objective** is the aim or purpose of specified controls at the service organization
- As businesses provide different services to user organizations and have different objectives for those services, **there is not a pre-defined set of control objectives all service organizations are required to meet**
- **Control objectives are normally defined by the service organization** but can also be defined by a third party, such as a user of the service organization's service or system
- **Control activities** are defined by the service organization to achieve the specified objectives
- **Test procedures** are procedures performed by an auditor to validate the design and, when applicable, operating effectiveness of controls to achieve the specified control objectives



Preparing for Your First SOC 1 Examination

SOC 1 Basics

Understanding SOC 1 Examination Scope Terminology

SOC 1 Examinations can either be as of a specified date or cover a period of time

- **SOC 1, Type 1 Examination**
  - Not to be confused with “SOC 1,” a 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 user auditors that controls are designed and implemented
- **SOC 1, 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 user auditors that controls are designed and operating effectively over a period of time

Roadmap for a Successful First Time SOC 1 Examination

Preparing for Your First SOC 1 Examination

Roadmap for a Successful First Time SOC 1 Examination

Setting Expectations

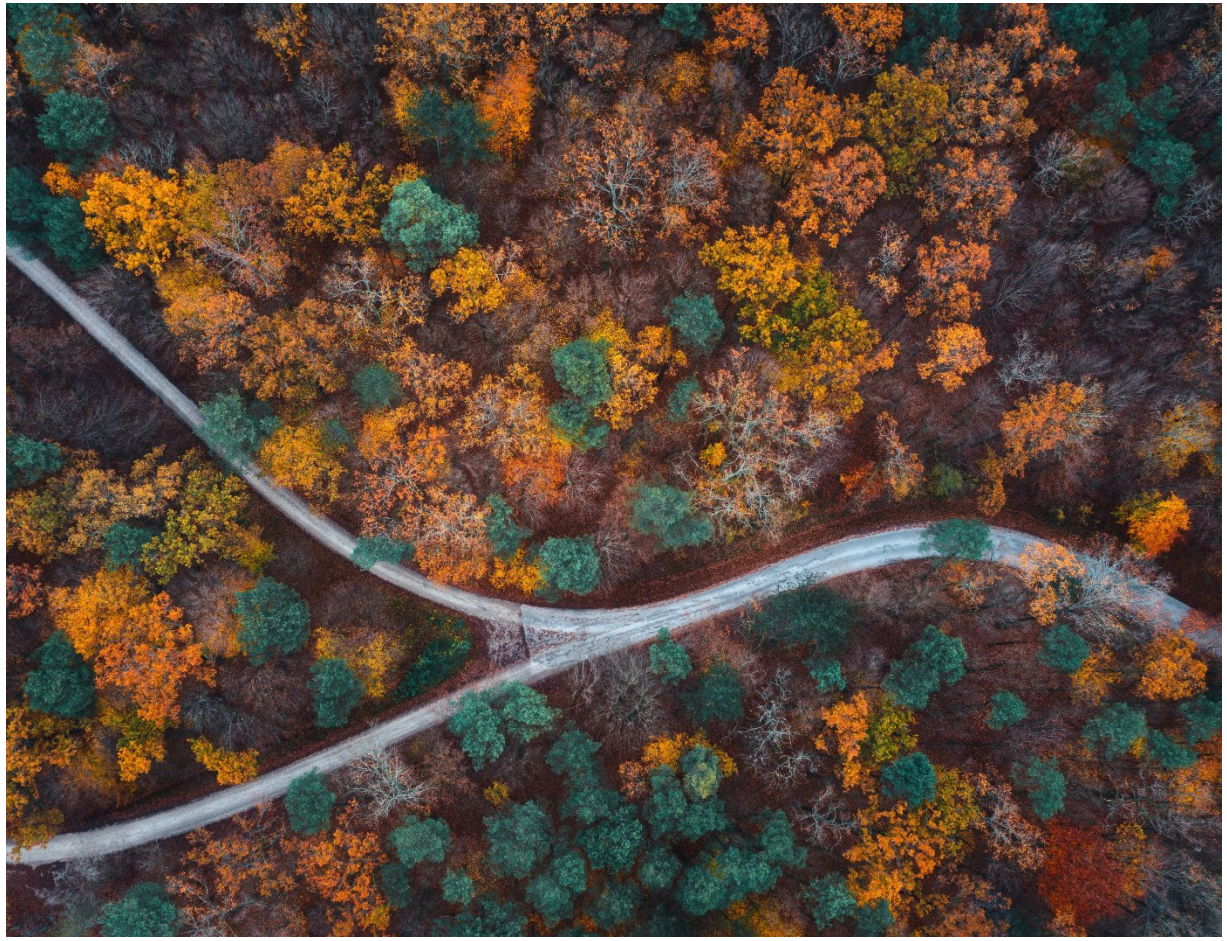
- SOC 1 Examinations demonstrate a business' commitment to maintaining strong internal controls
- A SOC 1 Examination engagement is **not a self-assessment**, an **independent certified public accountant is required** to perform the assessment and issue an opinion
- A SOC 1 Examination which **results in control deviations or a qualified opinion** could be **viewed negatively in the market**, so it is important to prepare for your first SOC 1 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 1 Type 2 Examination Reports ranges from **12 to 18 months**

Preparing for Your First SOC 1 Examination

Roadmap for a Successful First Time SOC 1 Examination

Milestones

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



Preparing for Your First SOC 1 Examination

Roadmap for a Successful First Time SOC 1 Examination

Understand the Project Scope

- Determine whether you need a Type 1 or a Type 2 Report
- Identify and involve relevant Subject Matter Experts during planning and scoping, including members from IT, HR, and Legal
- Define the scope of your future SOC 1 Examination
  - Identify the systems and processes impacting your user entities' internal control over financial reporting
    - Where does client data flow?
    - What key reports or outputs are provided to clients?
  - 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)
- Communicate expectations and timelines

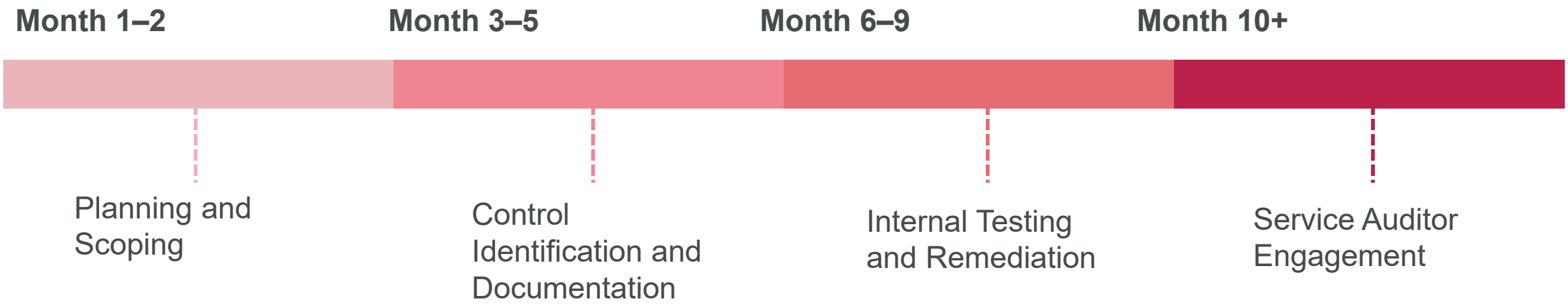
It can take 12–18 months from preparing for your SOC 1 Examination to having a SOC 1 Examination Report in hand, so it is imperative to start planning as soon as possible

forvis mazars

Preparing for Your First SOC 1 Examination

Roadmap for a Successful First Time SOC 1 Examination

Example SOC 1 Timeline



Timelines can vary depending on the strength of your initial internal control environment, complexity and scale of processes and people involved, and number of information systems involved.

Preparing for Your First SOC 1 Examination

Roadmap for a Successful First Time SOC 1 Examination

Month 1–2: Planning and Scoping

- **Engage With Key Stakeholders**
  - Identify the internal teams (e.g., Finance, IT, HR) that will be involved in the SOC 1 preparation
  - Appoint a project leader or team to oversee the process

- **Determine Audit Scope**
  - Define which systems, processes, and controls impact financial reporting
  - Determine the audit boundaries (e.g., which services or business units are in scope)
  - Clarify if any third-party vendors that impact financial reporting will be included
  - Develop a data flow or process flow of data inputs from clients and outputs back to clients

forvis mazars

Preparing for Your First SOC 1 Examination

Roadmap for a Successful First Time SOC 1 Examination

Month 3–5: Control Identification and Documentation

- Identify and define Control Objectives
  - Identify financial reporting-related Control Objectives (e.g., data integrity, transaction processing)
  - Identify Information Technology General Controls (e.g., access management, segregation of duties, change management)
- Assess and document risks to achieving the Control Objectives
  - What could go wrong?
  - Consider both preventive and detective controls
- Document Controls
  - Develop and formalize written policies and procedures for key control areas
  - Verify that the documentation clearly defines how each Control Objective will be met and the risk(s) intended to be mitigated

Preparing for Your First SOC 1 Examination

Roadmap for a Successful First Time SOC 1 Examination

Month 3–5 Continued: Tips for Identifying SOC 1 Control Objectives

- Control Objectives should address the key processes its user entities care about and should align with financial reporting requirements, regulatory requirements, and Service Level Agreements as applicable.
- Common areas that SOC 1 Control Objectives should cover:
  - Organization management and oversight
  - Completeness and accuracy of inputs received into the system or service
  - Processing integrity
  - Completeness and accuracy of outputs or reports provided by the service organization to the user entity
  - Logical security to information systems where user entity data resides
  - Change management of information systems where user entity data resides
  - Backup and data recovery
  - Incident management

Preparing for Your First SOC 1 Examination

Roadmap for a Successful First Time SOC 1 Examination

Month 3–5 Continued: Tips on Developing Policies and Procedures

- Identify and assign documented controls to Subject Matter Experts/control owners
- Document procedures and responsibilities for implementing and enforcing policies and procedures
- Develop and implement policies and procedures to address any control gaps identified during the risk assessment and control documentation phase
- Consider defining audit artifacts at this stage (what will be used to evidence successful operation of the control)

forvis mazars

Preparing for Your First SOC 1 Examination

Roadmap for a Successful First Time SOC 1 Examination

Month 6–9: Internal Testing and Remediation

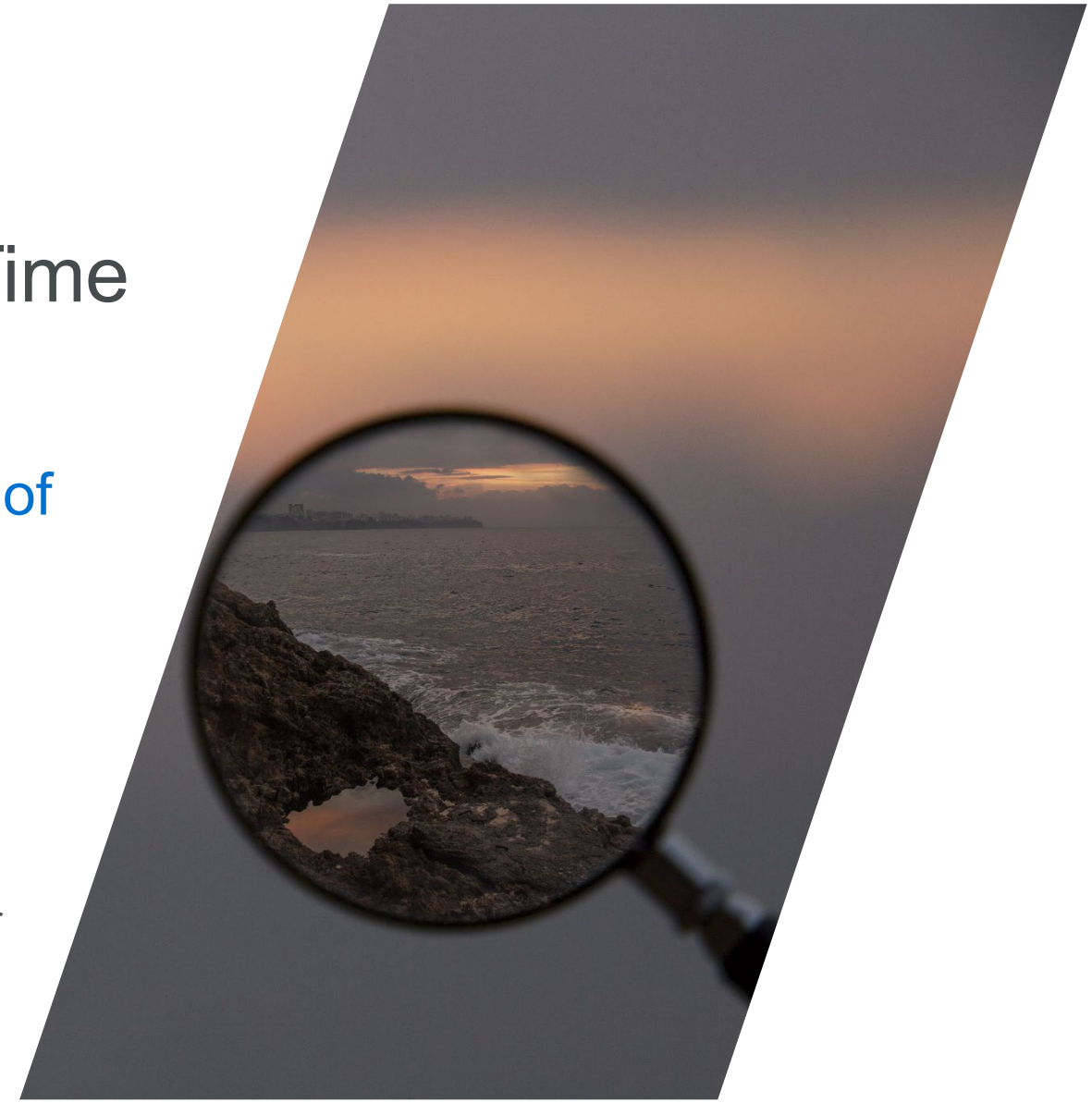
- **Conduct Initial Testing of Controls**
  - Perform Readiness Assessment testing to evaluate the design and operational effectiveness of key controls over a defined period
    - Is documentation available and maintained?
    - Are transactions logged and is a population of transactions able to be pulled over a period of time for on-occurrence/ad-hoc controls?
  - Verify that controls are functioning consistently across departments and systems
- **Remediate Gaps**
  - If issues are identified, implement corrective actions and perform follow-up testing
  - Update documentation to reflect any changes made during remediation
- **Prepare Staff for Examination**
  - Train employees on the SOC 1 Examination process and how they'll be involved (e.g., interviews, walkthroughs)
  - Ensure staff members understand how controls operate and can explain them to auditors

Preparing for Your First SOC 1 Examination

Roadmap for a Successful First Time SOC 1 Examination

Month 6–9 Continued: Tips on Initial Testing of Internal Controls

- Conduct a Readiness Assessment to help ensure that all controls and documentation support design and implementation of the controls in place
- Confirm populations for transaction-based controls (e.g., financial transactions, 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



Preparing for Your First SOC 1 Examination

Roadmap for a Successful First Time SOC 1 Examination

Month 6–9 Continued: Tips on Remediating Issues and Ensuring Continued Operation

- **Remediation**
  - Confirm identified gaps with control owners and develop recommendations for remediating gaps
  - Prioritize gaps and establish timeline
  - Track gaps to remediation and confirm remediation of all identified gaps
  - Implement new policies and procedures to help ensure availability to teams for implementation
- **Ensuring Continued Operation**
  - Establish regular Key Performance Indicators and logging practices
  - Establish control documentation practices, continuous monitoring, and a process for regular reviews of policies and procedures
  - Establish a process for periodic (no less than annual) risk assessments to identify emerging threats and changes in processes

forvis mazars

Preparing for Your First SOC 1 Examination

Roadmap for a Successful First Time SOC 1 Examination

Month 6–9 Continued: Providing Training and Awareness

- Develop and provide training and awareness programs for employees and contractors to help ensure that they understand their roles and responsibilities for the SOC 1 Examination
- Consider developing training and awareness programs that address key process areas, including Standard Operating Procedures, security awareness, and incident response
- Communicate what to expect during a future SOC 1 Examination
  - Walkthroughs and observations
  - Population and system-generated listing requests
  - Documentation requests

forvis mazars

Preparing for Your First SOC 1 Examination

Roadmap for a Successful First Time SOC 1 Examination

Month 10+: Service Auditor Engagement and Undergoing an Examination

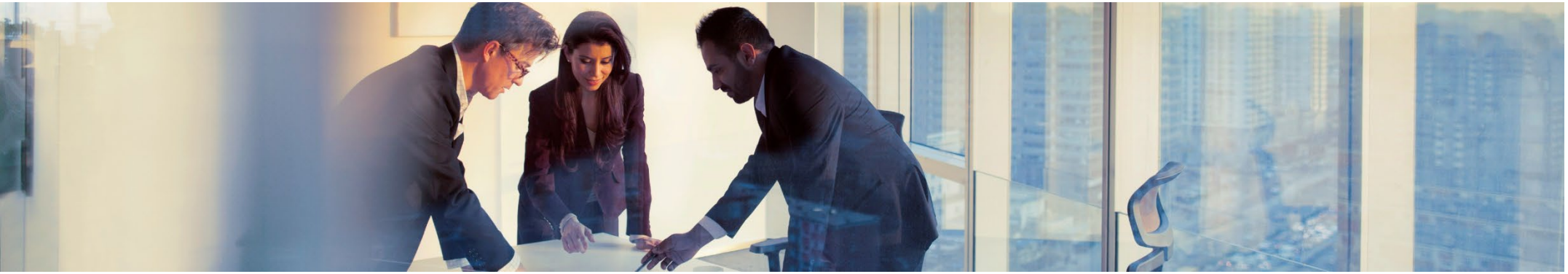
- **Service Auditor Engagement**
  - Hold a kickoff meeting with auditors to review the scope, timeline, and documentation
  - Provide access to relevant control evidence, records, and documentation
  - SOC 1 Examinations are typically 6–12 months long
- **Walkthroughs, Interviews, and Testing**
  - Auditors request walkthroughs and interview relevant staff members to verify that controls are properly implemented and understood
  - Auditors test the controls as of the agreed-upon specified date (Type 1) or across the agreed-upon specified time period (Type 2; typical time period for a SOC 1 Type 2 is 6–12 months).
  - Be prepared to address any questions or requests for additional documentation during the examination

Preparing for Your First SOC 1 Examination

Roadmap for a Successful First Time SOC 1 Examination

Month 10+: Tips on Undergoing Your First SOC 1 Examination

- All gaps should be cleared before you undergo a SOC 1 Type 1 Examination or before you begin your specified period for a SOC 1 Type 2 Examination
- Specified period in a SOC 1 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 1 Examinations
- Work with the CPA firm to schedule the examination and provide necessary documentation and access to systems



Preparing for Your First SOC 1 Examination

Roadmap for a Successful First Time SOC 1 Examination

Common Pitfalls

Beware of **common pitfalls** and showstoppers

Inadequate Documentation

Controls may exist but are not properly documented, making it difficult for auditors to assess their design and effectiveness.

Poor Scope Definition

Failing to properly define the scope of the audit can result in too many or too few controls being examined which can lead to scope creep (testing unnecessary controls) or missing critical control areas.

Lack of Readiness Assessment Testing

Companies may rely solely on the Service Auditor during the examination to identify gaps or issues, neglecting to perform testing prior to the examination.

Not Engaging Stakeholders Early Enough

Waiting too long to engage with key departments (e.g., IT, HR, Finance) can lead to delays in gathering required documentation or identifying control owners.

Overlooking Third-Party Vendors

Failing to account for third-party service providers who may have an impact on financial reporting can result in control gaps.

Over-Complicating Controls

Some companies over-engineer their controls, making them unnecessarily complex and difficult to maintain. Controls should be simple and practical. Focus on controls that are easy to implement, measure, and test. Controls are not a process narrative of what happens, but what actions are taken to help ensure objectives are achieved.

Unrealistic Timelines

Companies often underestimate the time needed to prepare for a SOC 1 Examination, especially for a Type II Examination that requires demonstrating control effectiveness over time.

Preparing for Your First SOC 1 Examination

Roadmap for a Successful First Time SOC 1 Examination

Emphasis on Standard Documentation Expectations

- If it is not documented, it did not happen
- Oftentimes, process owners complete/perform the controls but do not document what they have done and there is no audit trail to “test” during the audit
- When in doubt, over document

Roadmap for a Successful First Time SOC 1 Examination

Additional Tips

- Educate the control owners that during the Readiness Assessment, the service auditor is wearing its Consulting hat
- Do not try to hide issues during the Readiness Assessment, be as open and honest as possible. This way, the service auditor can identify areas which need to be addressed prior to the actual Examination
- 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 initial SOC 1 Examination and can help expedite preparation

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