



SOC Reports

PROTECT THE INTEGRITY OF YOUR
INTERNAL CONTROLS

IGNITING GROWTH

AN OVERVIEW

Many service organizations depend on the integrity of their control environment to protect their business as well as their customers. With new technologies being unveiled at record speeds and the increasing prevalence of third-party vendors, that integrity is more complicated to secure.

One way to help ensure internal controls are in place and operating effectively is to conduct a **system and organization control (SOC) examination, also known as a SOC audit**. While these reports aren't required, financial statement auditors use them to reduce audit procedures, and sophisticated service organizations push for them as confirmation that their data is protected.

02 THE EVOLUTION OF SOC

06 SOC 1, 2 & 3: THE DIFFERENCES

Comparison

SOC 1

SOC 2

SOC 3

The Trust Services Criteria

08 SOC EXAMINATION DRIVERS

10 HOW TO PREPARE FOR A SOC EXAMINATION

Process Overview

Tips to Combat Examination
Challenges



WHY ISSUE A SOC REPORT?

More and more companies are outsourcing services. Ideally, a third-party vendor would exert the same level of internal controls you would. To make sure everyone is on the same page, it's important to know what your vendors are doing when it comes to:

- Financial and performance history
- Security and availability safeguards
- Reliable processing integrity
- Confidential and private records
- Regulatory and operational compliance
- Compliance with service-level agreements
- Regular due diligence and monitoring

New services within outsourcing arrangements that drive SOC adoption include the following:

- Software as a service (SaaS)
- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Cloud providers

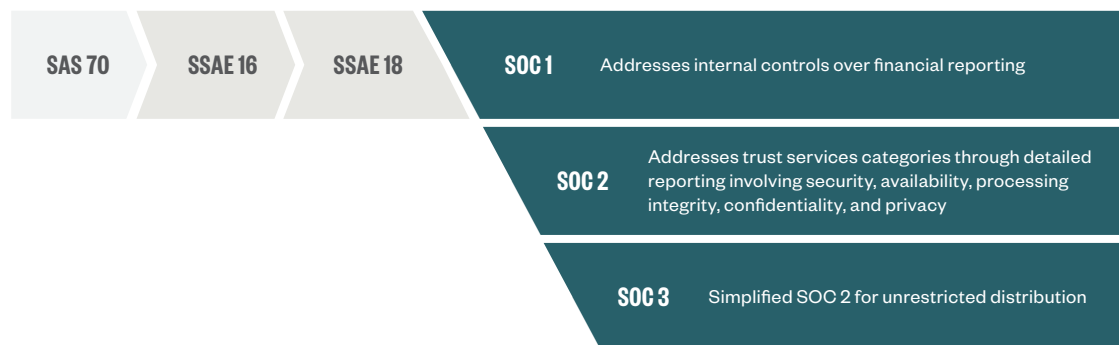
The Evolution of SOC

Prior to 2011, service organization reports were completed under Statement on Auditing Standards (SAS) No. 70. The American Institute of CPAs (AICPA) then moved to Statement on Standards for Attestation Engagements (SSAE) No. 16 to account for limitations within SAS 70, keep pace with changes in regulatory compliance, and more closely mirror international auditing standards.

After the SAS 70 report was retired, SOC 1, under SSAE No. 16, was implemented to help technology service providers address their growing assurance needs.

In April 2016, SSAE No. 16 was replaced by SSAE No. 18, which affects naming conventions, vendor management, complementary subservice organization controls, service auditor risk assessment, and written assertion requirements. The SSAEs have subsequently been codified, and SSAE No. 18 as it relates to SOC examinations is now AT-C 320.

In addition to SOC 1, which focuses on internal controls over financial reporting, there's also SOC 2 for a broader range of service providers with internal controls that can cover any combination of security, availability, processing integrity, confidentiality, and privacy. SOC 3 is a simplified SOC 2 that can be used for general distribution. SOC 2 and SOC 3 follow AT-C 205.



SOC 1, 2 & 3: The Differences

SOC examinations aren't formally required, but they're increasingly being requested as part of doing business. The purpose of a SOC engagement is to report on the effectiveness of a company's internal controls and safeguards they have in place while providing feedback that's both independent and actionable.

There are three kinds of SOC reports and two types within each kind. Each has a specific use. Which is right for you?

REPORTS	CONTROL DOMAINS	EXAMINATION FOCUS	DISTRIBUTION
SOC 1 Assesses internal controls for financial reporting	<ul style="list-style-type: none"> • Transaction processing • Supporting IT general controls 	Service provider-defined: Control Objectives <i>Vary depending on the type of service provided</i>	Restricted <i>to users and auditors</i>
SOC 2 Assesses internal controls for compliance or operations	<ul style="list-style-type: none"> • Infrastructure • Software • People • Procedures • Data 	Standardized: Trust Services Categories <ul style="list-style-type: none"> • Security • Availability • Processing integrity • Confidentiality • Privacy <i>Categories covered are selected by the service provider</i>	Restricted <i>to users, auditors, and specified parties</i>
SOC 3 A smaller scale SOC 2 report for marketing purposes			Unrestricted

Each kind of SOC engagement has two types of report.

REPORT TYPES	SOC REPORTS			TESTING COVERAGE		
	SOC 1	SOC 2	SOC 3	DESIGN	OPERATING	RESULTS OF TESTS
TYPE 1 Examines controls at a point of time	•	•		•		
TYPE 2 Examines controls over a period of time	•	•		•	•	•

SOC 1

SOC 1 looks at internal controls for financial reporting. For example, a financial services provider that provides transaction processing may request a report to look at its transaction processing and operations.

Once an organization defines the controls it would like examined, there's a lot of work that goes into an independent examination to assess if those controls are in place and operating effectively.

SOC 1 is considered an auditor-to-auditor communication, which means an auditor provides it and then hands it to the auditor requesting it.

Types

There are two types of reports for these engagements:

TYPE 1

This looks at the design and implementation of internal controls at a certain point in time, which gives this examination a so-called as-of date.

TYPE 2

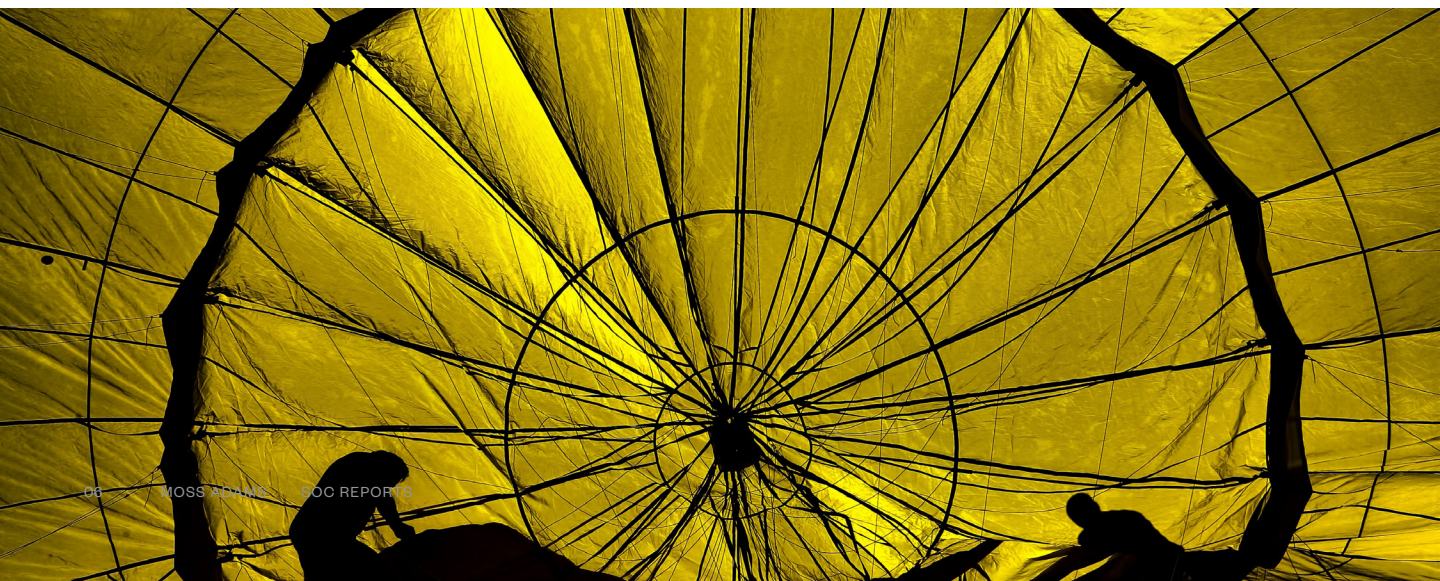
This is the report you want. It looks at design and operating effectiveness of internal controls over a period of time, usually a 12-month period, which gives a much more meaningful perspective compared with Type 1.

Distribution

Distribution of SOC 1 examination details is restricted to management, customers, and financial statement auditors to keep sensitive information confidential. However, you can look for the AICPA seal to see if a company completed its examination.

SOC COMPLIANT SEAL

Even when you may not have access to a SOC 1 or 2 report because of distribution restrictions, you can look for a SOC compliant seal on a company's website or other materials.



SOC 2

Most technology companies have a need for SOC 2 examinations, regardless of their line of service, because they use or are themselves third-party vendors that store, process, or maintain data.

There's been huge growth in the number of SOC 2 examinations performed—and it's anticipated to continue. This is largely due to increased security concerns that rise proportionally as the IT industry promotes new products and services in the cloud.

Trust Services Categories

SOC 2 examinations emphasize system reliability by measuring the effectiveness of internal controls related to five trust services categories:

- Security
- Availability
- Confidentiality
- Processing integrity
- Privacy

Each of these trust categories has predefined criteria (see page eight).

Companies Using SOC 2 Reports

SOC 2 reports are now considered a base requirement for technology service providers. They're embraced by:

- Software as a service (SaaS)
- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Cloud-based providers
- Data centers and colocation facilities
- IT-managed services companies
- IT-hosted services
- Business intelligence software

Types

Similar to a SOC 1 report, there are two types within SOC 2:

TYPE 1

This looks at management's description of a service provider's system and the suitability of the design of controls.

TYPE 2

This looks at management's description of a service provider's system and the suitability of the design and operating effectiveness of controls.

Distribution

Also like SOC 1, SOC 2 examination details can be distributed only to management, current and prospective customers, and financial statement auditors.

SOC 3

SOC 3 reports are essentially a smaller-scale SOC 2 report and used primarily for public distribution. Companies generally must complete a SOC 2 examination before requesting a SOC 3 report. While demand is extremely low for these reports, the distribution element can often be compelling for companies.

CARVE-OUT VERSUS INCLUSIVE METHOD

Many service providers prefer the carve-out method, which includes the services performed by a vendor organization in the service provider's system description but excludes the control objectives and related controls of the subservice organization.

The inclusive method looks at the services performed by a vendor in the service provider's system description as well as the control objectives and related controls of the vendor's organization. Start-ups that have most of their functions in house, or bigger companies that have a large number of in-house processes, may opt for the inclusive method.

THE TRUST SERVICES CATEGORIES

Security

Availability

Confidentiality

Processing Integrity

Privacy

Every report includes security as part of the common criteria.






Management can choose which of the other trust services categories they'd like to include in the examination.

For instance, if you believe a service provider is dealing with confidential information, then you should push for that trust services category to be included.

Those trust services categories apply to these **system components** during an examination:





INFRASTRUCTURE	Physical structures, IT, and other hardware, including facilities, computers, equipment, mobile devices, and telecommunications networks	
SOFTWARE	Application programs and IT system software that support application programs, such as operating systems, middleware, and utilities	
PEOPLE	The personnel involved in the governance, operation, and use of a system—namely developers, operators, entity users, vendor personnel, and managers	
PROCEDURES	Automated and manual procedures	
DATA	Transaction streams, files, databases, tables, and output used or processed by a system	

ADVANCEMENTS IN THE PIPELINE

Trust services criteria were updated to align with the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) 2013 framework. The adoption date was examinations ending after December 15, 2018, with early adoption permitted.

Implementation of SOC 2+ will include the Health Information Trust Alliance (HITRUST) or other criteria.

Data integrity may be added as a sixth trust services category.



INCREASE IN DEMAND

SOC 2 REQUESTS

are increasing in tandem with the IT industry's growth.

If this continues, demand for SOC 2 examinations will eventually overtake SOC 1.



MOST REQUESTED TRUST SERVICES CATEGORIES:

SECURITY

AVAILABILITY

CONFIDENTIALITY

Demand for privacy may change with AICPA revisions. See page seven.



MAJORITY OF REPORTS USE THE CARVE-OUT METHOD

Learn more on page seven.

Criteria Topics by Category

SECURITY

- IT security policy
- Security awareness and communication
- Risk assessment
- Logical access
- Physical access
- Environmental controls
- Security monitoring
- User authentication
- Incident management
- Asset classification and management
- Systems development and maintenance
- Personnel security
- Configuration management
- Change management
- Monitoring and compliance

AVAILABILITY

- Availability policy
- Backup and restoration
- Incident management
- Disaster recovery
- Business continuity management
- Security
- Change management
- Monitoring and compliance

CONFIDENTIALITY

- Confidentiality policy
- Confidentiality of inputs
- Confidentiality of data processing
- Confidentiality of outputs
- Information disclosures (including third parties)
- Confidentiality of information in systems development
- Incident management
- Security
- Change management
- Monitoring and compliance

PROCESSING INTEGRITY

- System processing integrity policies
- Completeness, accuracy, timeliness, and authorization of inputs, system processing, and outputs
- Information tracing from source to disposition
- Incident management
- Security
- Change management
- Availability
- Monitoring

PRIVACY

- Privacy policies
- Personally identifiable information (PII) classification
- Risk assessment
- Incident and breach management
- Provision of notice
- Choice and consent
- Collection
- Use and retention
- Disposal
- Access
- Disclosure to third parties
- Security for privacy
- Quality
- Monitoring and enforcement

SOC Examination Drivers

SOC 1 and SOC 2 are now being used by service providers in a host of industries, but technology, financial institutions, and health care IT are particular growth sectors.

For technology companies, the main issues driving adoption of SOC reporting include the rapid rate of cloud adoption, cybersecurity threats, and compliance involving the Cloud Security Alliance (CSA), International Organization for Standardization, and the National Institute of Standards and Technology.

Compliance issues for technology in health care related to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and HITRUST are powerful drivers when it comes to trust criteria within security, confidentiality, and privacy of information.

WHO NEEDS SOC?

SOC examinations aren't just for technology corporations. They benefit a range of different entities, from financial institutions to benefit plan administrators and health care organizations. Traditional outsourcing arrangements apply to:

- Financial institutions
- Bank trust departments
- Credit unions
- Collection agencies
- Hedge fund accounting services
- Data analysts
- Payroll bureaus
- Third-party administrators
- Benefit plan administrators
- Document management
- Specialized services





Here are some other drivers, in no particular order of prevalence:

Clients and Due Diligence

Service providers don't conduct a SOC examination just because they want one; they request a report because user entities and user entities' auditors demand them—this is the primary driver. When you use a third-party service organization, you're hiring it to do work completely and accurately for the right fee. Part of due diligence and evaluating the completeness and accuracy of the work your service provider performs is to look at its SOC report.

Competitive Measure

In some cases, having a SOC examination is the minimum requirement for companies looking to enter a given market or to gain or retain customers.

Compliance

Organizations also conduct SOC examinations to comply with the requirements of Section 404 of the Sarbanes-Oxley Act (SOX 404) or other financial or business audit requirements. Organizations funded by external financiers may also require the issuance of a SOC report. Similarly, regulatory authorities often request that companies undertake SOC examinations.

Develop Internal Controls

A number of organizations requesting SOC examinations are start-ups—emerging entities with five to 50 employees. While raising funds or going public, they're looking to develop internal controls, set up a risk assessment infrastructure, or create sophisticated documentation controls. In these cases, issuing a SOC report can increase credibility and boost confidence in its management by validating an organization's control environment.

Monitoring Control

Like formal vendor due diligence, SOC reports can help highlight specific controls in place at a service organization. This helps customers understand the core controls they're able to leverage to better monitor performance. By understanding these automated and manual controls, an informed customer is empowered to maintain much tighter oversight of third-party vendors.

Reduce Auditor Procedures

A company can significantly reduce the effort required by auditors and customers when evaluating a service organization with an effectively structured SOC examination and well-designed controls supported by meaningful test procedures. As such, the better the SOC report, the greater the reliance on testing with fewer auditor procedures needed by the report users.

Regulatory Changes

The implementation of the Affordable Care Act (ACA) in 2010 added a host of regulatory and compliance requirements, including measures to ensure the privacy of patient data. Health care organizations are required to maintain more stringent controls on privacy and confidentiality, considering the type of information they maintain. This, in turn, has increased the demand for SOC 2 examinations on the part of health care organizations. Similarly, HIPAA and HITRUST are driving a rapid increase in demand for SOC reports.





SERVICE PROVIDERS
DON'T CONDUCT A SOC
EXAMINATION JUST
BECAUSE THEY WANT
ONE. THEY REQUEST A
REPORT BECAUSE USER
ENTITIES AND THEIR
RESPECTIVE AUDITORS
DEMAND THEM.

How to Prepare for a SOC Examination

The process for getting a technology service provider started with SOC 1 and SOC 2 is relatively straightforward. Once this preliminary readiness assessment is complete, a timeline can be put in place for the engagement that will be driven based upon the results of the assessment.

- 1 Determine if there's sufficient demand for the SOC examination.
- 2 Assign a SOC lead and solicit commitment from control owners.
- 3 Understand the process, time, and effort involved.
- 4 Select a service auditor.
- 5 Choose which report to issue—SOC 1, 2, or 3 and a Type 1 or 2 report.
- 6 Plan and prepare for the SOC examination:
 - Determine impact related to subservice organizations.
 - Self-assess readiness of controls and remediate gaps.
 - Document the system descriptions and controls for the examination.
- 7 Participate in the examination.

REMEMBER:

The SOC process takes time and effort.

Select the right service auditor to help you define the scope of controls, the type of examination, and the timing.

Put in place an effective internal team to help support the examination effort.



A Note On Controls

There's no ideal ratio in terms of IT controls versus business controls assessed during a SOC examination. In SOC 2 examinations, IT controls make up the majority of controls. For SOC 1, the number of controls varies from 15 to 20, or, in some cases, over 200, with IT controls representing up to one-third of the total controls.

Technology service providers should avoid using a universal benchmark for the number of controls; instead, they should focus on a clear understanding of the nature and specificity of the controls required for their unique operating environments and the expectations of their customers given the solutions being brought to market.

In designing these controls, service providers need to have:

- A clear understanding of the controls they **currently have** and what additional controls they **need to have**
- The time frame necessary to implement the additional controls

Neglecting this analysis can lead to an unclear definition of controls, which can then result in unneeded delays in the examination process itself.

TIPS FOR DEFINING CONTROLS

Leverage existing sources:

- Customer contracts
 - Request for proposal responses
 - Due diligence questionnaires
 - Compliance forms
 - Quality control and internal examinations
 - Competitor reports
-

Start with a solid outline from which you can expand and formalize.

Review wording and presentation of controls with your service auditor.

Isolate control activities from the control descriptions.

Ensure management has a reasonable basis to assert controls and monitor that they're operating effectively.

TIPS TO COMBAT SOC EXAMINATION CHALLENGES

The challenges faced by organizations conducting SOC examinations vary depending on their operational maturity.

Generally, service providers that are more operationally mature have ample experience in the SOC examination process and look for ways to improve efficiency and reduce cost. Less operationally mature organizations commonly struggle with up-front issues such as failing to properly prepare for a SOC examination and underestimating the formality needed to generate consistent examination evidence.

In contrast, even larger organizations can be susceptible to risks such as underengineering controls to avoid dealing with complex networks of internal stakeholders. Or they may have highly distributed operations that make it difficult to implement and enforce standardized controls practices.

Here are some tips to help you avoid common challenges and pitfalls that risk delaying an examination's completion.



Commit to the Examination Process

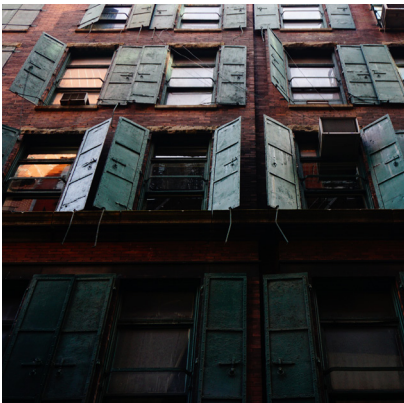
Companies often fail to appreciate the sustained organizational effort required to complete the examination and struggle with varying levels of commitment between senior management and staff.

The challenges faced by organizations conducting SOC examinations vary depending on their operational maturity.



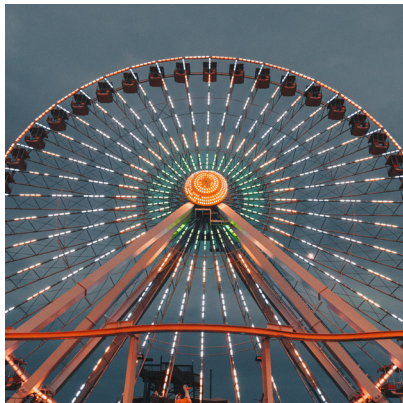
Think Long Term

Short-term convenience within the service provider culture can often undermine implementation of long-term controls, seriously hinder the SOC examination process, and introduce controls that won't be effective over time.



Educate On Controls

Control owners and other relevant stakeholders at the service provider often don't understand the nature of the controls and what they're being audited against. This doesn't apply just to an IT director; everyone needs to have a higher level of awareness.



Assign One Point of Contact

Auditors need to maintain a number of different communication channels. A single point of contact to oversee the entire process on behalf of the service provider will help streamline this process. It might also make sense for your organization to pull in two contacts—one within IT and the other in finance—to help facilitate communication between the two arenas.



Coordinate Between All Parties

Navigating a complex network of stakeholders with sometimes competing interests can be a challenging undertaking. While it might be tempting, don't shortchange the examination process by minimizing the areas involved and underengineering the controls.

Our approach to staffing SOC examinations is to combine industry-focused and seasoned auditors with operational and IT auditors who can address requirements unique to your control environment.

For more information on how to monitor outsourced vendor relationships and ways to manage the risks associated with outsourcing, including SOC reports, contact your Moss Adams professional.

Contact

CHRIS KRADJAN

Partner and SOC Lead

(206) 302-6511

chris.kradjan@mossadams.com

KIMBERLY KOCH

Partner and SOC Lead

(509) 777-0107

kim.koch@mossadams.com

TAFT KORTUS

Industry Group Leader
Technology, Communications & Media

(206) 302-6377

taft.kortus@mossadams.com

mossadams.com/technology

About Our Technology Practice

In addition to our financial statement audit and tax services, our professionals can meet many more operational needs specific to technology companies:

IT CONSULTING

We provide SOC 1 and SOC 2 assessments and a full spectrum of consulting services in the areas of IT operations, systems, management, security, and organization.

ROYALTY COMPLIANCE

We've performed hundreds of royalty compliance audits for software developers, intellectual property licensors, and patent holders.

TRANSACTION SERVICES

Information is your most important asset in any transaction. We work with more than 200 private equity firms and their portfolio companies, ranging in size from emerging funds to those with more than \$1 billion under management.

Our valuation consulting services in particular support mergers and acquisitions, financial reporting, ad valorem tax reporting, estate and gift tax reporting, financial feasibility studies, insurance claims, underwriting, employee stock ownership plans, and litigation.

SOC SERVICES

- SOC pre-audit gap analysis and readiness assessments
- Coordination among management, user entities, and auditors
- Coaching and review of client-prepared control objectives and narratives
- Independent assistance to document client-defined control objectives and narratives
- SOC 1, SOC 2, and SOC 3 examinations (Type 1 and Type 2 audits)
- Dual reporting under Attestation Standards and International Standard on Assurance Engagements (ISAE) 3000 for clients involved in international markets
- Aligning SOC 2 and SOC 3 audits to leverage the CSA's Cloud Control Matrix
- Conversion from 2016 to 2017 Trust Services Criteria for SOC 2 and SOC 3

About Moss Adams

With more than 3,200 professionals across 25-plus locations in the West and beyond, Moss Adams provides the world's most innovative companies with specialized accounting, consulting, and wealth management services to help them embrace emerging opportunity. Discover how Moss Adams is bringing more West to business.

Assurance, tax, and consulting offered through Moss Adams LLP. Investment advisory services offered through Moss Adams Wealth Advisors LLC.