SOC Compliance
VendorInsight
White Paper

MITRATECH

SOC 1, 2 OR 3:

What's Best for You?

VendorInsight

INTRODUCTION
SOC Controls

Almost a decade after Service Organization Controls (SOC) reports were introduced, there is still confusion over the differing report types and their linkage to vendor risk analysis and internal control synergy.

The confusion stems from the variety and contexts of SOC audits. On the surface there are three categories of SOC reports, but within those three SOC categories, there are two types.

While a SOC 1 report is for service organizations that impact or may impact their clients' financial reporting, a SOC 2 report is for the security of client data that service organizations hold, store or process. Both SOC 1 and SOC 2 reports are available under restrictions, typically NDAs, and can be classified as Type 1 or Type 2. A SOC 3 report, however, also covers data but is a general use report that can be distributed to any party or parties.

The differences are daunting for any organization to manage, but especially those overseeing critical or high-risk vendors. If some vendors provide a SOC 1 and others give you SOC 2 or even a SOC 3, how do you know if you're receiving the most appropriate information for your vendor relationship? And do you know what to look for within each of them to properly manage your risk and align your organization's control environment?

"SOC controls are a series of standards designed to help measure how well a given service organization conducts and regulates its information."

INTRODUCTION
SOC Controls

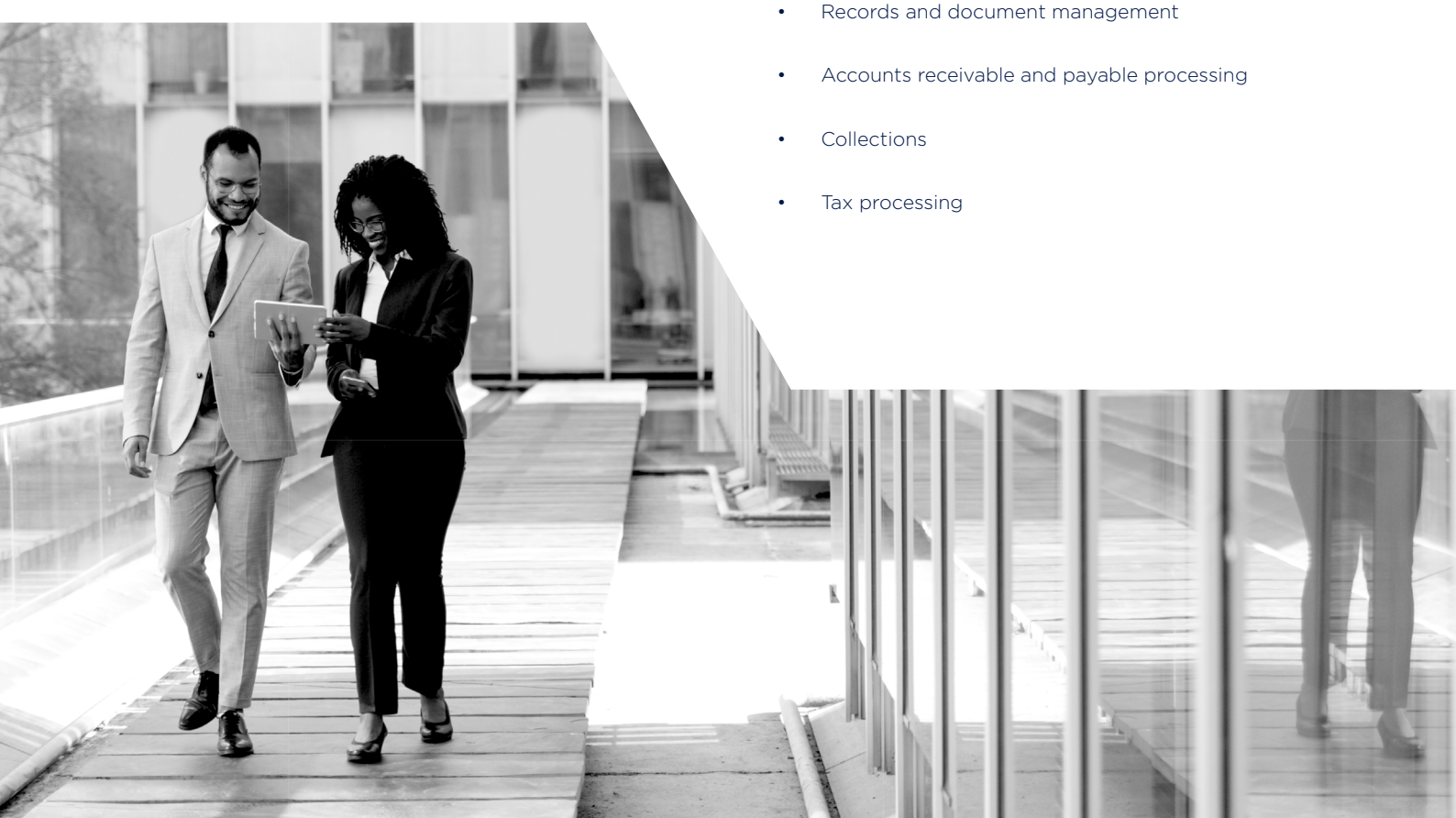
THE NECESSITY OF SOC AUDITS

More and more, financial institutions are outsourcing functions to third-party vendors, which introduces additional risk(s) and raises liability concerns. What's fueling the reliance on these vendors? The factors include:

- The need to offer a wide array of products and services
- Pressure on improving operational costs to remain competitive in the market
- Increasing reliance on technology to meet customer needs and expectations
- Limits on availability and specialized skills with internal resources

Common Functions Provided by Service Organizations

- Core account processing
- Transaction processing services
- Investor and stockholder services
- Telecommunications platforms
- Cloud computing providers
- Networking monitoring
- Collocation data processing centers
- Payroll and employee scheduling services
- Managed information security and network monitoring
- Human resources and benefits management
- Records and document management
- Accounts receivable and payable processing
- Collections
- Tax processing



SOC 1
Reports Describe Internal Controls

The American Institute of Certified Public Accountants (AICPA) designed SOC reports to be the auditing standard for services organizations. The report replaced the former SAS 70 in 2011, when SSAE 16 took effect. Today, SOC 1 reports may also be known as SSAE 18 reports.

SOC 1 engagements are based on the Statement on Standards for Attestation Engagements 18 standard. The previous standard was SSAE 16, but this was superseded by SSAE 18 in May 2017. The new auditing standard has a broader scope, including key insight into material subcontractors, or as they are typically referenced, fourth parties, used in the delivery of the contracted product or service.

A SOC 1 report is:

- Created by an audit firm in confidence to the vendor's management and Board of Directors
- Designed to verify a vendor's internal controls
- For any work managed by a vendor that could impact a company's financial accuracy and reporting

Determining which of your vendor's products and services should require a SOC 1 report is critical to a comprehensive and successful vendor management program. The most common vendors are those responsible for processing transactions — paying, receiving and the accumulation of interest that is paid or earned. Within your organization, your vendor compliance, internal audit/compliance, IT management and legal departments may be responsible for requesting and reviewing this documentation.

SOC 1 has two types of auditor-prepared reporting.

- **Type 1** reports detail the design of a service organization's financial controls, but not the operating effectiveness. The report validates that the controls are in place at a specific time and date.
- **Type 2** includes a description of the service organization's system. In addition, the auditors test the design and operating effectiveness of key internal controls over a period of six months at minimum.

The differences between the two types can cause confusion. While your risk management, compliance or vendor management professionals may understand the differences, other departments who work day-to-day with vendors may not.

This can result in your organization failing to collect, review and thoroughly understand which reports they need and what information in the report is relevant or requires additional action.

Both types of SOC 1 reports are confidential documents. The audit firm performing the audit delivers the report to management with the promise of confidentiality They are available to vendor clients typically upon request under a confidentiality arrangement. The request and review of available SOC reports prior to entering a contractual obligation with a vendor is an accepted best practice within the onboarding process of a vendor.

SOC 1
Reports Describe Internal Controls

SUBCONTRACTORS OR FOURTH-PARTY VENDORS

Requirements for SOC 1 reports from fourth-party vendors have grown, and organizations are now reviewing more data from multiple vendors than ever before.

Previously, financial institutions struggled to track their vendor's vendors (third parties). The SSAE 18 addresses this by adding transparency in the monitoring of material fourth-party vendors.

A financial institution might not even realize their vendor has a third party which it outsources services or functions to until it reviews a SOC 1. A fourth party could be conducting business in a manner that does not align with the company's internal practices or business objectives (i.e., storing customer data outside of the United States) which could lead to a negative impact to the business.

A card processor for a bank is one example of a vendor requiring a SOC 1 report. This vendor manages and reports transactional activity continuously. For a financial institution, there is a direct link between the data the vendor is handling and the bank's records for customer balances and generated income. The financial controls the card processing vendor has in place have a direct impact on the accuracy of the reported financial statements of its customer — the bank.

SOC 2
Reports Evaluate Data Management Practices

SOC 2 reports deal with data security. They clarify the service organization's control structure surrounding the protection of sensitive consumer data, data processing and office management solutions and company confidential information.

The reports address a service organization's controls relevant to operations and compliance to a defined code of conduct, They include a description of the service auditor's tests of controls and results.

SOC 2 reports are outlined by the AICPA's five Trust Services Criteria for the protection of data:

- Security
- Availability
- Processing integrity
- Confidentiality
- Privacy

While SOC 1 reporting utilizes the SSAE 18 professional standard, SOC 2 incorporates the AT-C Section 205 standard. This is a pivotal element for reporting on controls at service organizations. This is due to the increasing number of entities in today's cloud computing and technology business sectors.

SOC 2 reporting mirrors SOC 1 in its categorization:

- A **Type 1** affirms controls are in place and adequately defined.
- A **Type 2** reviews the controls in place and their effectiveness. Type 2 reports are validated over a period of three to six months.

Who needs a SOC 2 report? Anyone responsible for an organization's internal controls, regulatory and IT compliance should obtain and review a SOC 2 report. This includes vendor compliance, internal audit, IT management and legal departments.

A SOC 2 report is concerned with any vendor who has your customer or organization data including but not limited to account or social security numbers, the customer's name, confidential, and proprietary data.

One example of a vendor that should have required SOC 1 and SOC 2 reports for both third-party and fourth-party vendors would be those associated with mortgage loan subservicing.

When a bank provides a loan to a customer, often the loan is serviced by a third-party vendor. While the third party handles the financial information, and manages collections and delinquencies, they have a subcontractor, or fourth party, that provides the system used in the processing of payments, interest calculation, notices, etc.

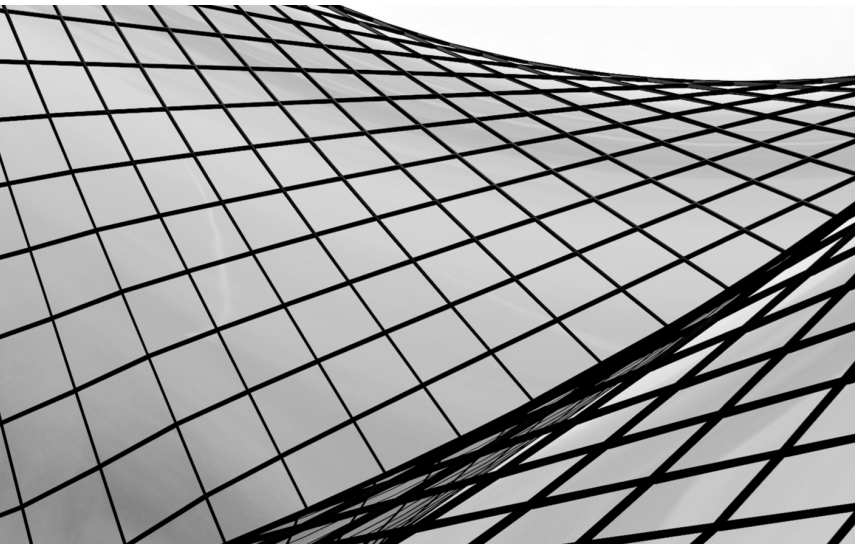
Somewhat more than 80% of mortgages are done this way. The service being purchases is supported by others down the line. In this instance, your organization should be asking for the SOC 1 and SOC 2, for data purposes, of not just your third party but also from the fourth-party vendors.

SOC 2
Your Organization's Responsibilities Outlined In CUECs Or CSOCs

Post-SSAE 18, risk managers and regulators are applying additional emphasis on a specific part of SOC 1 and SOC 2 reports. SOC 1 and SOC 2 reports from a vendor include details of the complementary user entity controls (CUECs) and complementary subservice organization controls (CSOCs):

- CUECs describe all controls within a vendor's systematic processes that rely on the user entity for implementation to ensure full functionality.
- CSOCs are controls that the service organization's management assumes will be implemented by the subservice organizations. They are necessary to achieve the control objectives stated in management's description of the service organization's system.

SOC 1 and SOC 2 reports contain this critical information to protect your organization. These sections describe what your organization is responsible for in the execution of the financial or data security controls. For example, CUECs and CSOCs may include tasks such as financial reconciliation, updates on user access and personnel changes or two-way reporting requirements.



SOC 2
The Confusion Over Qualified and Unqualified Opinions

In preparation of a SOC 1 or SOC 2 report, the auditor will state their opinion about the controls examined. An unqualified opinion means that the controls are described in a fair and accurate manner and operate effectively. Simply put, the controls meet all the required standards.

A qualified opinion, on the other hand, means that the auditor found items to be considered or addressed. The auditor may also detail exceptions.

While an unqualified opinion can sometimes have exceptions, any exceptions within a qualified opinion mean that there has been a significant failure in the control's functionality.

For example, a SOC 2 report describing the controls in place for personnel changes. When an employee leaves the company, if the systems and processes fail to remove their access to protected customer data, then that's a failure across the board. An auditor might describe this example of a failure in a qualified opinion, based upon the severity level of the exception identified.

SOC 3

Reports Are Intended For General Use

While SOC 1 and SOC 2 reports are proprietary, restricted use reports, SOC 3 reports are much less authoritative descriptions of a company's controls to meet the Trust Services Criteria.

Although these reports cover the same subject matter as SOC 2, SOC 3 reports are mostly marketing summations. They don't require NDAs, are not confidential and are often published on company websites.

SOC 3 reports give an overview for service organizations and do not include a description of the service auditor's tests of controls and results. Also, the description is naturally less detailed than the description in a SOC 2 report.

Who needs this? SOC 3 reports demonstrate to current and prospective customers that a service organization has the appropriate controls to mitigate risks. Ultimately, SOC 3 reporting often serves as part of the pre-contract vetting and vendor selection process.

Report Type	Standard	Topic	Prepared by	Availability	Types	Organization Responsibilities
SOC 1	SSAE 18 standard	Financial Controls	Auditors	Confidential	**1** – Controls in place at a moment in time **2** – Controls validated over a defined period	Contains CUECs and CSOCs
SOC 2	Trust Services Criteria	Data Security	Auditors	Confidential	**1** – Controls in place at a moment in time; **2** – Controls validated over a defined	Contains CUECs and CSOCs
SOC 3	Trust Services Criteria	Data Security	Marketing summary	Public	Can summarize either **Type 1** or **Type 2** SOC 2 report results	

AUTOMATING SOC REPORT REVIEW

SOC reports can often be voluminous, difficult to understand, and you may not have the expertise in your organization to review them. This is why more companies are turning to sophisticated Third-Party Risk Management (TPRM) software solutions and consultants to review reports, interpret the results, and make recommendations regarding the risks involved.

These tools can review SOC control audit reports for your vendors per your organization's submission to the TPRM provider, or by that provider requesting them directly from the vendor. As these are private and confidential documents, these are conducted under an open Letter of Authorization from your organization.

The TPRM provider reports its risk analysis and findings, and it's desirable they provide a separate segment that identifies the CUECs and CSOCs for integration into your internal organization controls. Ideally, they are also uploaded into a single central resource hub that provides a single source of truth for your organization.

CONCLUSION

When considering which SOC reports from your third and fourth-party vendors fit your organization's needs, you must first understand the reports. Consider the areas your vendor is managing and the impact it has on your financial reporting and data security to understand which SOC report(s) best suits your needs.

By reviewing the reports from an objective perspective with a meticulous eye, a Third-Party Vendor Risk Management provider may help your organization with internal and external responsibilities in developing a sound vendor risk management program. When it comes time to review SOC reports for your vendors, TPRM technology can do much of the work for you.

VENDORINSIGHT PROVIDES YOU WITH A SINGLE SOURCE OF TRUTH

SOC reports can often be voluminous, hard to understand, and your organization may lack the skills to review them.

VENDORINSIGHT CAN DO IT FOR YOU.

We have the expertise and experience to know what we're looking at, interpreting the results, and developing conclusions for your organization to assess any risks. You can submit SOC control audit reports for your vendors directly to VendorInsight, or we can obtain them directly from the vendor under an open Letter of Authorization.

We then provide a final report summarizing the risk analysis and findings, including a separate segment identifying the CUECs and CSOCs for integration into your internal organization controls.

The VendorInsight evaluation and final report, your documented review of our findings and attestation to complementary controls, and the vendor's documents are uploaded into electronic vendor folders. This provides a single source of reference, with everything you need in one place.

VendorInsight gives financial institutions the ability to review, approve, author comments and attest that controls are in place as defined as the complementary requirements for an effective control ecosystem. It's the only solution providing you with both the technology and expertise to successfully complete SOC review as part of your vendor management process.

ABOUT MITRATECH

Mitratech is a proven global technology partner for corporate legal, risk & compliance, and HR professionals seeking to maximize productivity, control expense, and mitigate risk by deepening operational alignment, increasing visibility and spurring collaboration across their organization.

With Mitratech's proven portfolio of end-to-end solutions, organizations worldwide are able to implement best practices and standardize processes across all lines of business to manage risk and ensure business continuity.

For more info, visit: www.mitratech.com

MITRATECH

info@mitratech.com
www.mitratech.com