NCONTRACTS

2026

GUIDE TO UNDERSTANDING SOC REPORTS

WHY A SOC REPORT?

SOC Reports are the preferred **OPERATIONAL RISK** documents to request from service providers that have been rated by the FI as having a critical/high/or significant inherent risk.

OPERATIONAL RISK includes non-financial risks that result from inadequate or failed policies and processes, non-compliance with regulatory mandates, technology failures that lead to breaches or business interruptions, as well as intentional or accidental personnel errors or fraud.

- **FFIEC** defines Operational Risk as the risk of loss resulting from inadequate or failed internal processes, people and systems, or external events.
- **FDIC** defines Operational Risk as the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk.
- **NCUA** defines Operational Risk as the risk of loss resulting from inadequate or failed internal processes, people and systems, or external events that result in an inability to deliver products, remain competitive, and manage information.
- **OCC** defines Operational Risk as the risk to current or projected financial condition and resilience arising from inadequate or failed internal processes or systems, human errors or misconduct, or adverse external events.

The Interagency Guidance on Third Party Relationships (June 6, 2023) states that "when relevant and available, review SOC reports, assessments, or certifications by independent third parties related to relevant standards and determine whether scope is appropriate, and whether findings justify additional scrutiny".

WHAT IS A SOC REPORT?

- SOC (System and Organizational Controls) Reports are the result of an audit performed by independent CPAs (Certified Public Accountants). The auditor is contracted and paid for by the entity being audited, most of the time. Clients may require an entity to be audited and pay for the audit as part of a pending contract. The independent audit covers the design and operational effectiveness of a service provider's "system" of policies and protocols related to the delivery of some or all services and/or products provided by the Company (in a SOC 2 Type 2). SOC auditors are required to be independent and objective and should be trained to perform a SOC audit.
- SOC reports provide information for users of the Company's products and services to help users better assess and mitigate the risks associated with the outsourced relationship.
- The **American Institute of Certified Public Accountants** (**AICPA) is a private standards organization.** On May 1, 2017, AICPA replaced the SSAE16 standard with the SSAE18 standard, which defines the guidelines and procedures for SOC audits performed after that (5/1/17) date. *(You can buy the 200+ page SOC book from AICPA's public website. It is very technically oriented and not for the casual reader. However, it is very comprehensive.)*

- The SSAE18 standard requires the audited company to identify additional subservice providers that are necessary to support the delivery of the entity's products or services. Outsourced service providers (your fourth party providers) are documented near the beginning of the SOC report in the SCOPE of the report and may also be further detailed within the body of the report.
- The company being audited is responsible for providing a description of their services, products, and/or applications and their related system of controls, protocols, and policies designed to support the delivery of products and/or services. Company management must provide an assertion/attestation that the description they provide is accurate. That attestation is at the beginning of the SOC report and should match the auditor's opinion.
- The body of a SOC report is written by the entity being audited.
- The auditor is responsible for writing the opinion on the appropriateness and adequacy of the design of controls and state whether controls operated effectively during the audit period The testing section of the SOC report is written by the auditor and is at or near the end of the report.

TYPES OF SOC REPORTS

- **SOC 1:** Designed to review a company's internal controls as they relate to or influence financial reporting. These audits are appropriate for companies that provide products that could have an impact on a user's financial reporting.
- **SOC 2:** Designed to review a vendor's non-financial internal controls over one or more of the Trust Services Criteria relevant to security, availability, processing integrity, confidentiality, and privacy. The Security criteria are the base criteria and is included in all SOC 2 assessments.
    - **SECURITY:** The system is protected against unauthorized access, use, or modifications.
    - **AVAILABILITY:** The system is available for operation and use as committed or agreed upon.
    - **PROCESSING INTEGRITY:** System processing is complete, valid, accurate, timely, and authorized.
    - **CONFIDENTIALITY:** Information designated as confidential is protected as committed or agreed upon.
    - **PRIVACY:** Collection, use, retention, disposal, and disclosure of personal information is in conformity with the organization's privacy policy and AICPA Privacy criteria.
- **SOC 3:** A high-level summary of a SOC 2 audit intended for public distribution. Because it is public-facing, a SOC 3 report omits many details included in a SOC 2 report, including testing details and results. A SOC 3 report does not provide enough information to serve as the primary Operational Risk due diligence source, so clients should request the SOC 2 report instead.
- **Type 1**: Reports on the appropriateness of the controls to achieve the desired control objectives as of a specified date. The operational effectiveness of those controls over a period of time is not tested in this report. This report may be appropriate for certain software to be installed on client/user systems. It may also be used as a company's first SOC report, since it is not as rigorous as a Type 2.
- **Type 2**: Reports on the suitability of the design and operating effectiveness of entity controls to achieve the related criteria and/or control objectives throughout a specified period. The time-period covered

by the audit is between 6 and 12 months. AICPA states that an audit of at least 6 months is necessary to validate that controls are operating effectively.

A SOC 2 Type 2 Audit/Attestation Report is preferred for reporting on computer technology and information security controls and has a higher likelihood of covering most or all GLBA related controls.

A SOC 2 audit may also be utilized to address compliance with other defined criteria, such as CSA (Cloud Security Alliance) controls over Cloud Security, NIST Standards, ISO Standards, or HITRUST controls that address privacy and security over protected health information.

TITLE OF REPORT

The title of the report includes the type of Audit Report (SOC 1, SOC 2, etc.) and the type of audit performed (Type 1 or Type 2). The period covered by the audit will be noted for Type 2 Audit Reports. For Type 1 reports, the date of the actual audit will be listed (for example: as of February 28, 2025). The audited company decides the type of audit to be performed. For SOC 2 audits, the service provider also decides which trust criteria the company will be audited against.

AUDITOR'S OPINION

Is located near the beginning of the audit report. A SOC auditor's opinion states that the auditor has reviewed the assertion provided by the service provider and has validated whether all claims made by the audited company are accurate; whether policies and controls are appropriately designed; and whether controls are operating effectively to achieve control objectives. The audit opinion should be dated and signed (electronic signature is OK). The date on the auditor's opinion may not always match the end of the audit period.

The auditor's opinion will be one of the following:

- **UNQUALIFIED**: This is the most desired outcome. (also known as UNMODIFIED or a "CLEAN" opinion) This affirms that the company's management description of its system is free from material misstatements, controls are appropriately designed, and those controls operated effectively throughout the audit period. This opinion may still result in some Issues or Exceptions that are identified by the auditor. However, all company control objectives were appropriately designed and/or met during the audit period. Identified Issues should have a "Management Response" that describes a plan to remediate identified in Issue(s). Remediation generally occurs prior to the end of the audit period. If there is no Management Response to an identified issue that could have an impact on the services you receive from the provider, reach out to your service provider and request one.
- **MODIFIED/QUALIFIED:** The auditor, having obtained sufficient and appropriate audit evidence, concludes that misstatements, individually or in aggregate, are material *but not pervasive* OR the auditor is unable to obtain sufficient appropriate audit evidence on which to base their opinion, but the auditor concludes that the possible effects of undetected misstatements could be material *but not pervasive.* This opinion tells the client that certain controls were not appropriately designed

and/or did not operate effectively. However, in this type of opinion most controls operating as the company designed and intended during the audit period. In this type of opinion, the auditor will typically give the client an opportunity to address issues, and the auditor will then retest related controls. The opinion is still qualified, but you will know that the issue has been addressed prior to the end of the audit period.

- **DISCLAIMER OF OPINION**: (Serious) This is NOT an opinion and means that the auditor is choosing not to render an opinion. The auditor may be unable to obtain sufficient appropriate evidence on which to base their opinion and concludes that misstatements could be both material and pervasive. An extremely limited scope may also result in a Disclaimer of Opinion. For example, a Disclaimer of Opinion may result when an auditor does not have access to data, or certain data is unavailable or missing for whatever reason. In that instance the auditor is unable to test or validate control effectiveness due to a lack of data provided by the service provider.
- **ADVERSE OPINION**: (Very Serious) The auditor has determined that misstatements, individually or when grouped with other misstatements, are both material and pervasive. This is a relatively rare opinion from an auditor. Misstatements may be intentional (as in fraud or management override of controls) or unintentional due to one of more material deficiencies in the system. An example of an Adverse Opinion may occur when the auditor discovers a security or privacy data breach during the audit, due to insuffient security and monitoring controls.
- **EMPHASIS OF A MATTER**: May apply to Unqualified or Qualified Opinions. The Emphasized Matter is not necessarily negative. This is simply bringing something to the attention of the report user, as an enhanced explanation and it may not affect the auditor's opinion. Examples of this might be a data center change in the middle of the audit period or operational changes that occurred during COVID.

The auditor is responsible for determining the materiality of a deviation and for determining whether the deviation, alone or in aggregate, rises to the level of a deficiency. The auditor determines materiality based upon the auditor's professional judgement and whether the deviation is pervasive in nature.

SCOPE OF REPORT

Not all reports include a scope section. When included, the scope may identify third-party service providers needed to meet the control objectives covered in the report. It typically states that those third-party providers' controls are excluded from the SOC report's scope. The scope may also specify which products, services, or physical locations are included or excluded from the audit. Confirm that the stated scope applies to the products or services you receive.

MANAGEMENT ASSERTION

Generally located after the Auditor's Opinion section, somewhere near the beginning of the report. A typical title would be, "Management of XX Company's Assertion Regarding its XX System." The assertion is written by the company being audited and states that company management has truthfully and accurately written a description of the services or products covered by the audit. This typically also

includes a description of services and the scope or boundaries of the audit. The Management Assertion will be written to closely mirror the language of the auditors' opinion. It should be signed and dated by a representative of company management. An unsigned assertion should be questioned and sent back to the entity for a signature.

BODY OF REPORT

This is written by the company being audited. Topics typically addressed within the body of the report include company organization; management oversight; policies and/or practices related to information security; network and computer policies; third party oversight; operational controls and policies; risk management; personnel hiring, training, and competency; logical and physical access controls; change management; network incident response; and business continuity/availability. SOC 2 reports are designed to address certain predefined criteria, standards, or best practices. SOC 1 reports are designed to address the internal controls of a service organization and the effect those controls may have on a user entity's financial statements. Some SOC reports include information related to various products or business continuity protocols at the very end of the report. That information is not validated by the auditor and would be "out of scope" of the audit.

COMPLEMENTARTY USER ENTITY CONTROLS AND USER ENTITY RESPONSIBILITIES

CUECs are additional controls that **should be implemented** by the user of the services or product to ensure that service provider controls operated as intended and designed during the audit. These controls are identified and documented within the SOC report by the company being audited, they are generally located right before the testing results (for SOC 2). Customers of the audited company (you) are responsible for ensuring CUECs have been reviewed to determine which are applicable based upon the services contracted from the vendor. Your auditors will expect you to document how you are meeting the applicable CUECs. CUECs may be met through entity wide or departmental policies, or certain employees may be assigned responsibility for implementing and monitoring certain controls. CUECs do not generally change much year to year unless the service provider has major changes within their operating environment. An example of a CUEC might be requiring all users of the software to have unique IDs and complex passwords. Your internal IT policy may satisfy that requirement.

CUERs are additional controls that the service provider **recommends** the end user implement. However, the controls of the service provider will still operate as intended and designed, even if the end user does not implement CUERs. Because of that, many end users do not do anything with the CUERs and auditors do not generally require that they be completed. Find out in advance whether your auditor has specific requirements for CUERs.

COMPLEMENTARY THIRD-PARTY ORGANIZATION CONTROLS

These are controls performed by a third-party organization (such as a data center) which are necessary to provide reasonable assurance that one or more of the service organization's commitments and system requirements are achieved. Management of the service organization is required to disclose the

types of third-party organization controls that the subservice organization is required to implement. The primary service provider is responsible for maintaining adequate third-party/supply chain/and partner oversight programs to evaluate and monitor outsourced services or partners that are necessary for the delivery of the vendor's products or services. If your auditor requires a SOC report from your vendor's third-party service providers (your fourth-party providers), you will need to go through your service provider to obtain that SOC report, since you do not have a contract with that service provider.

CONTROL TESTING

The controls and policies covered within the body of the report are tested by the auditor and documented in this section. Testing may take the form of looking at policies, speaking with management, and/or reviewing audits previously performed by the company. Auditors may also perform their own audits by looking at logs or through generally on-site observation to see whether policies are being enforced. Exceptions or deficiencies noted by the auditor during the examination are detailed within this section. Company management usually document a management response to exceptions that are identified during the audit. A management response is not required as part of the SOC audit. However, most service providers include a response that details how they have addressed or plan to address exceptions identified by the auditor. Management Responses may be located within the Testing Section or may be located at the end of the SOC report.

COMPANY ADDITIONAL INFORMATION

Information within the SOC report after the testing section is not part of the report that is audited. Management's response to Exceptions may be noted within this area. Some companies use this space to highlight additional products or to provide additional information about their business continuity or information security plans.