AICPA & CIMA

Together as the Association of International Certified Professional Accountants

SOC for service organizations toolkit

Contents

Welcome to the SOC for service organizations toolkit!

This toolkit provides resources for CPA firms that do not currently provide SOC[1] for service organizations examinations (SOC 1®, SOC 2®, and SOC 3® examinations) but are interested in entering this space. These resources include information about the services themselves as well as various factors the firm should consider before starting a SOC practice.

Note: This toolkit does not include resources regarding other SOC engagements such as SOC for Cybersecurity and SOC for Supply Chain examinations. Find additional information about SOC for Cybersecurity and SOC for Supply Chain examinations on the AICPA website.

The information contained in this toolkit is provided to assist the user in developing a general understanding of the topics discussed, but no attempt has been made to cover the subjects or issues exhaustively. SOC services continue to evolve, and toolkit users should look to relevant professional standards and related guidance when using the following resources.

Overview of SOC for service organizations engagements. Develop a basic knowledge by using this overview, which discusses the three SOC for service organizations engagements (SOC 1, SOC 2, and SOC 3) and variations of each. This primer is ideal for those who are unfamiliar with these engagements or as a refresher for those who have a general understanding. It also includes valuable information about quality control and peer review for firms offering these services.

Considerations for adding SOC services to your firm. This document poses several factors to consider, such as staffing and profitability, when determining whether a SOC practice makes sense for the firm.

SOC for service organizations implementation checklist. This convenient tool provides steps for firms to take when implementing new SOC 1, SOC 2, or SOC 3 services. The checklist includes considerations that can contribute to the success of the firm's SOC efforts, recommended certifications, and references to other SOC for service organizations toolkit components.

Client assessment template: SOC 1 and SOC 2 services opportunities. Access a list of questions firms can ask a client (or prospective client) to help determine the types of SOC services the client may benefit from.

Scoping and pricing considerations in SOC for service organizations engagements. Explore considerations related to the firm, the service organization, the engagement, and the service organization's system that are relevant to scoping and pricing SOC services.

SOC for service organizations learning resources. Take advantage of this collection of resources for professionals interested in learning more about

- controls over financial reporting;
- controls relevant to security, availability, and processing integrity of the system a service organization uses to process users' data; and
- controls relevant to the confidentiality and privacy of the information the system processes.

This document includes links to authoritative and interpretive guidance as well as supplemental resources to promote general understanding of IT security and internal controls.

[1] In 2017, the AICPA introduced the term system and organization controls (SOC) to refer to the suite of services practitioners may provide relating to system-level controls of a service organization or system- or entity-level controls of other organizations. Formerly, SOC referred to service organization controls. By redefining that acronym, the AICPA enables the introduction of new internal control examinations that may be performed (a) for other types of organizations, in addition to service organizations, and (b) on either system-level or entity-level controls of such organizations."

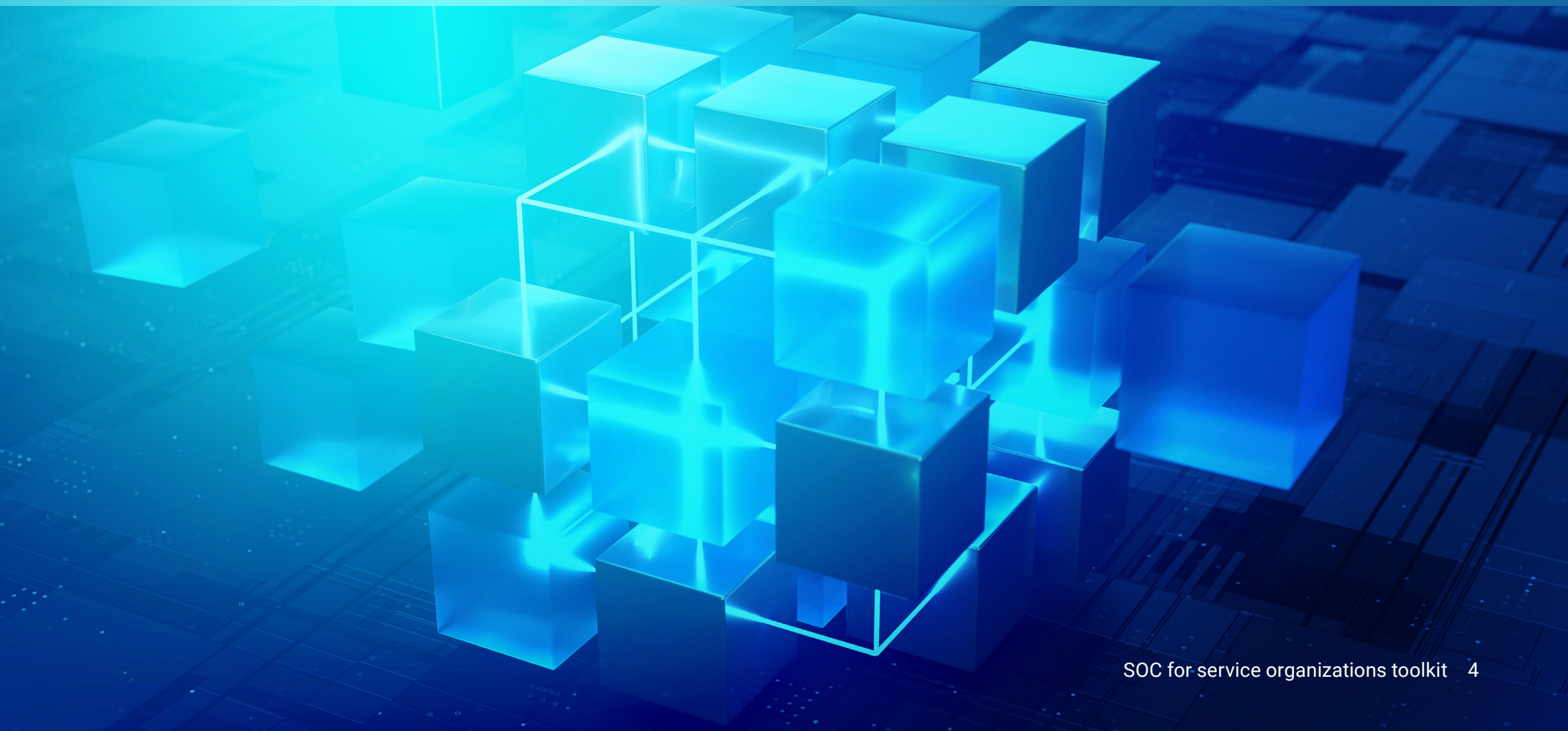
Additional resources

SOC survey results — an infographic that can be shared with clients, demonstrating the value of SOC 1 and SOC 2 examinations as part of a service organization's third-party risk management efforts.

SOC logo for CPAs (registration required) — can be used by CPA firms in marketing their SOC for service organizations services.

SOC logo for service organizations (registration required) — can be used by service organizations that undergo a SOC 1, 2, or 3 examination to promote that fact to potential clients and other interested users.

Overview of SOC for service organizations engagements



Overview of SOC for service organizations engagements

Today, more and more organizations are outsourcing certain functions or activities to third-party service providers. This allows organizations to provide services or products more efficiently and cost-effectively. Along with the benefits of doing business with third parties, however, come risks that need to be identified, assessed, and managed. Users of these outsourced services, and their auditors, are increasingly requesting more information about the effectiveness of controls at the service organizations they use or are considering using. CPAs can use the AICPA's various SOC for service organizations offerings to provide assurance reports that provide users with valuable information that is needed to assess and address the risks associated with outsourcing services, helping to build trust and transparency.

This document provides a primer for those who are unfamiliar with SOC for service organizations engagements or a refresher for those who have a general understanding. It does not provide detailed guidance on performing a SOC for service organizations examination.

The variety of SOC for service organizations offerings available include the following:

- **SOC 1® — SOC for Service Organizations: ICFR** (reporting on controls at a service organization relevant to user entities' internal control over financial reporting). These reports are specifically designed to address controls at the service organization that are relevant to the user entities' financial statements. They enable user auditors[2] to perform risk assessment procedures and obtain audit evidence about whether controls at the service organization are operating effectively. Use of these reports is restricted to management of the service organization, user entities, and user auditors. There are two types of SOC 1 examinations – a type 1 examination addresses the system description and design of controls as of a point in time and a type 2 examination addresses the system description, design of controls, and operating effectiveness of controls throughout a period.

- **SOC 2® — SOC for Service Organizations: Trust Services Criteria** (reporting on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy). These reports address controls relevant to security, availability, and processing integrity of the system the service organization uses to process users' data and the confidentiality and privacy of the information the system processes. They provide a level of detail sufficient to address the user's vendor risk management needs and are restricted to specified parties with sufficient knowledge and understanding of the service organization's system and the nature of services it provides. There are two types of SOC 2 examinations – a type 1 examination addresses the system description and design of controls as of a point in time and a type 2 examination addresses the system description, design of controls, and operating effectiveness of controls throughout a period.

- **SOC3® — SOC for Service Organizations: Trust Services Criteria for General Use Report**. Like SOC 2, these reports address controls relevant to security, availability, processing integrity, confidentiality, and privacy. However, they do not provide the same level of detail. Therefore, they are considered general use reports and can be freely distributed. Although SOC 3 reports are generally not required to be restricted, some report users may not have a sufficient understanding of the service organization's system to understand how controls within the system operate. Before agreeing to a SOC 3 examination, management of the service organization and the service auditor[3] need to consider whether a SOC 3 report, which includes only management's assertion and the service auditor's opinion about the effectiveness of controls at the service organization, is likely to meet the information needs of intended report users or whether it is likely that a SOC 3 report will be misunderstood by potential report users. In some instances, management and the service auditor may agree to restrict the use of a SOC 3 report to the subset of potential report users whose informational needs are likely to be met by the SOC 3 report.

[2] A *user auditor* is an independent CPA who audits and reports on the financial statements of a user entity.
[3] A *service auditor* is an independent CPA who reports on controls at a service organization.

The table below highlights the differences between SOC 1, SOC 2, and SOC 3 reports. Within the columns, certain text is set in bold to highlight key distinctions between the three types of examinations and related reports. Many elements in this table are discussed in further detail following the table.

Table 1: SOC reports — Key differences

Item	SOC 1 report	SOC 2 report	SOC 3 report[4]
What is the purpose of the report?	To provide management of the service organization, user entities, and the independent auditors of user entities' financial statements with information and a service auditor's[5] opinion about **controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting**. The report enables the user auditor to perform risk assessment procedures and, if the report is a type 2 report, to use the report as audit evidence about whether controls at the service organization are operating effectively.	To provide service organization management, user entities, business partners, and other specified parties with information and a service auditor's opinion about **controls at the service organization relevant to security, availability, processing integrity, confidentiality, or privacy**.	To provide interested parties with a service auditor's opinion about the effectiveness of **controls at the service organization relevant to security, availability, processing integrity, confidentiality, or privacy**.
Who are the intended users of the report?	**Auditors of the user entities' financial statements, service organization management, user entities**	**Service organization management and user entities, business partners, other parties specified within the report who have sufficient knowledge and understanding of the service organization, the services it provides, and the system used to provide those services, among other matters.**	**Interested parties**

[4] The same procedures are performed in a SOC 3 examination as in a type 2 SOC 2 examination. Typically, SOC 3 reports are issued in addition to the SOC 2 report when the service organization wants a general use report in addition to the restricted use report.

Item	SOC 1 report	SOC 2 report	SOC 3 report[4]
What professional standards and implementation guidance are applicable to the examination?	AT-C section 105, *Concepts Common to All Attestation Engagements*[6]	AT-C section 105, *Concepts Common to All Attestation Engagements*[5]	AT-C section 105, *Concepts Common to All Attestation Engagements*[5]
	AT-C section 205, *Assertion-Based Examination Engagements*[5]	AT-C section 205, *Assertion-Based Examination Engagements*[5]	AT-C section 205, *Assertion-Based Examination Engagements*[5]
	AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*[5]		
	AICPA Guide *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1®)* **(AICPA SOC 1 guide)**	AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* **(AICPA SOC 2 guide)**	AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* **(AICPA SOC 2 guide)**
What are the subject matters of management's assertion and the SOC examination?	**The description of the service organization's system**	**The description of the service organization's system**	**N/A**
	Type 1 examination: The design and implementation of **controls to achieve the service organization's control objectives**	Type 1 examination: The design and implementation of **controls to achieve the service organization's service commitments and system requirements**	**N/A**
	Type 2 examination: The design, implementation, and operating effectiveness of **controls to achieve the service organization's control objectives**	Type 2 examination: The design, implementation, and operating effectiveness of **controls to achieve the service organization's service commitments and system requirements**	The design, implementation, and operating effectiveness of **controls to achieve the service organization's service commitments and system requirements**

[5] In the attestation standards, a CPA performing an attestation engagement ordinarily is referred to as a *practitioner*. However, for SOC for service organizations engagements, the term *service auditor* is typically used.
[6] The full text of all AT-C sections is available via the AICPA website: "AICPA SSAEs – currently effective."

Item	SOC 1 report	SOC 2 report	SOC 3 report[4]
What are the criteria for the examination and where can they be found?	**Paragraph .15 of AT-C section 320[5] contains the minimum criteria** for evaluating the description of the service organization's system.	DC section 200, ***2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022)***, contains the criteria for evaluating the description of the service organization's system.	**N/A**
	Paragraph .16 of AT-C section 320[5] contains the criteria for evaluating the suitability of the design of the controls, **and paragraph .17** contains the criteria for evaluating the operating effectiveness of the controls.	TSP section 100, ***2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)***, contains the criteria for evaluating the design and operating effectiveness of the controls.	TSP section 100, ***2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)***, contains the criteria for evaluating the effectiveness of controls.
What are the components of a type 1 report?	Management's description of the service organization's system	Management's description of the service organization's system	**N/A**
	A written assertion by management of the service organization about the measurement of the subject matters against the criteria *as of a specified date*	A written assertion by management of the service organization about the measurement of the subject matters against the criteria *as of a specified date*	**N/A**
	A service auditor's report that expresses an opinion on whether the subject matters are in accordance with the criteria *as of a specified date*	A service auditor's report that expresses an opinion on whether the subject matters are in accordance with the criteria *as of a specified date*	**N/A**

Item	SOC 1 report	SOC 2 report	SOC 3 report[4]
What are the components of a type 2 report?	Management's description of the service organization's system	Management's description of the service organization's system	**N/A**
	A written assertion by management of the service organization about the evaluation of the subject matters against the criteria *throughout the specified period*	A written assertion by management of the service organization about the evaluation of the subject matters against the criteria *throughout the specified period*	A written assertion by management of the service organization about the evaluation of the subject matters against the criteria *throughout the specified period*. **As part of that assertion, management describes the boundaries of the system and the service organization's principal service commitments and system requirements.**
	A service auditor's report that i. expresses an opinion on whether the subject matters are in accordance with the criteria *throughout the specified period*, and ii. includes a description of the service auditor's tests of the controls and the results of those tests	A service auditor's report that i. expresses an opinion on whether the subject matters are in accordance with the criteria *throughout the specified period* and ii. includes a description of the service auditor's tests of the controls and the results of those tests	A service auditor's report that **expresses an opinion on whether management's assertion is fairly stated based on the criteria**.
Is use of the service auditor's report restricted to the intended users?	Yes	Yes	**No**[7]

[7] Although a SOC 3 report is ordinarily not restricted, nothing precludes the service auditor from restricting the use of that report to a specific group of users when the service auditor believes one or more groups of potential users are likely to misunderstand the report. Restrictions are discussed further in the section titled "Report Restrictions."

Types of SOC 1 and SOC 2 examinations

As reflected in the preceding table, the opinions and timeframes covered by a SOC 1 or SOC 2 examination vary based on report type. A type 1 examination on the suitability of design and implementation of controls is usually requested in situations in which it is not practicable to perform the type 2 examination. Examples of situations in which it may not be practicable or possible to perform a type 2 examination include the following:

- The service organization is in the start-up phase. Although controls have been designed and implemented, they have not been in operation for a period of time adequate to provide sufficient appropriate evidence about the operating effectiveness of controls to support the service auditor's opinion.
- The service organization is providing new services to clients and business partners and the system providing such services and the related controls have not been in operation for a period of time adequate to provide sufficient appropriate evidence about the operating effectiveness of controls to support the service auditor's opinion.

In situations such as these, intended users of the SOC report often request a type 1 SOC report until such time as a type 2 examination can be performed. By agreeing to a type 1 examination, the service organization is demonstrating that it has designed and implemented controls and is on its way toward type 2 assurance.

There is no type 1 equivalent for a SOC 3 report.

Components of the reporting package

As noted in the preceding table, contents of the reporting package vary by engagement. Neither professional standards nor SOC guides specify how the components should be organized within a type 1 or type 2 report, but they do discuss the information that should be included in each component. The following provides further information about key components of a SOC for service organizations report:

- The **description of the service organization's system (description)** is a narrative description of the system that was examined.

  In a SOC 1 examination, the service organization's system is defined as the policies and procedures designed, implemented, and documented by management of the service organization to provide user entities with the services covered by the service auditor's report (this may not be all of the services offered by the service organization). Management's description of the service organization's system identifies the services covered, the period to which the description relates (or, in the case of a type 1 report, the date to which the description relates), the control objectives specified by management, and the controls relevant to user entities' internal control over financial reporting that support the control objectives.

  In a SOC 2 examination, the service organization's system includes the infrastructure, software, procedures, and data that are designed, implemented, and operated by people to achieve one or more of the organization's specific business objectives (for example, delivery of services or production of goods) in accordance with management-specified requirements. The description describes the procedures and controls the service organization has implemented to manage the risks that threaten the achievement of the service organization's service commitments and system requirements. Depending on the trust services category or categories to be addressed by the examination, these controls are relevant to the security, availability, or processing integrity of the system the service organization uses to process users' data or the confidentiality or privacy of the information the system processes.

  The description is prepared by service organization management from documentation supporting the system of internal control and system operations, as well as consideration of the policies, processes, and procedures within the system used to provide the services. The service auditor evaluates the presentation of the system description in accordance with the description criteria as part of the examination.

  A SOC 3 examination does not include a description, per se. However, it does include a description of the boundaries of the system examined and the principal service commitments and system requirements made in connection with management's assertion.

- **Management's assertion** is a written declaration by management about whether the subject matters addressed in the service auditor's report are in accordance with the criteria.

In a SOC 1 examination, the assertion addresses whether, based on the criteria,

- management's description of the service organization's system fairly presents the system that was designed and implemented as of a specified date or throughout the specified period;
- the controls related to the control objectives stated in management's description of the service organization's system were suitability designed to achieve those control objectives as of the specified date or throughout the specified period; and
- in a type 2 examination, the controls related to the control objectives stated in management's description of the service organization's system operated effectively throughout the specified period to achieve those control objectives.

In a SOC 2 examination, the assertion addresses whether

- the description of the service organization's system presents the system that was designed and implemented as of a specified date or through the specified period in accordance with the description criteria;
- the controls stated in the description were suitably designed as of a specified date or through the specified period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, if those controls operated effectively; and
- in a type 2 examination, the controls stated in the description operated effectively throughout the specified period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

In a SOC 3 examination, the assertion addresses

- whether the controls within the system were effective throughout the specified period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria (in a SOC 3 report, the term effective encompasses both the suitability of design of controls and the operating effectiveness of controls); and
- the boundaries of the system and the service organization's principal service commitments and system requirements.

- The **service auditor's report** contains an opinion that addresses all of the subject matters in the examination using the same criteria as in management's assertion.
  - In a SOC 1 or SOC 2 examination, the opinion addresses (a) management's description of the service organization's system; (b) the suitability of design of controls; and (c) in a type 2 examination, the operating effectiveness of controls.
  - In a SOC 3 examination, as described in the AICPA SOC 2 guide, the opinion addresses whether management's assertion is fairly stated based on the applicable trust services criteria. (However, AT-C section 205 also permits a service auditor to express an opinion directly on the effectiveness of the controls within the system.)

- The **description of the service auditor's tests of controls and the results of the tests** is only presented in a type 2 report. The description of tests and results is intended to provide report users with sufficient detail about the nature and extent of the service auditor's procedures and results to enable report users to understand the service organization's controls and obtain information about the operating effectiveness of such controls. As mentioned previously, a SOC 3 report does not include a description of the service organization's controls, the tests performed by the service auditor, or the results of those tests.

Report restrictions

As noted in preceding sections, use of both SOC 1 and SOC 2 reports are restricted to the specified parties listed in the report.

- Because the criteria used for an engagement to report on controls at a service organization are relevant only for the purpose of providing information about the service organization's system, including controls, to those who have an understanding of how the system is used for financial reporting by user entities, SOC 1 reports are restricted to the following users:
  - Service organization management

- User entities (including indirect or downstream users if controls at the service organization are relevant to the internal controls over financial reporting [ICFR] of the indirect or downstream user entity)
- Auditors of the user entities' financial statements.

- SOC 2 reports are ordinarily restricted to the following:
  - Service organization management
  - Customers (or user entities) that use the system throughout some or all of the period
  - Business partners subject to risks arising from interactions with the system
  - Practitioners providing services to such customers and business partners
  - Prospective user entities and business partners
  - Regulators who have sufficient knowledge and understanding of the service organization, the services it provides, and the system used to provide those services, among other matters. The expected knowledge of specified parties in a SOC 2 report ordinarily includes the following:
    - The nature of the service provided by the service organization
    - How the service organization's system interacts with user entities, business partners, certain organizations to which it has outsourced functions (subservice organizations), and other parties
    - Internal control and its limitations
    - Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
    - User entity responsibilities and how they may affect the user entities' ability to effectively use the service organization's services
    - The applicable trust services criteria
    - The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks

Although a SOC 3 report is ordinarily appropriate for general use, the service auditor may decide to restrict its use to specified users when the service auditor believes one or more groups of potential users are likely to misunderstand the report. For example, when a service organization uses a subservice organization, the service auditor may believe that intended users of the report may need to also understand the effectiveness of controls at the subservice organization. If the examination carved out the services of that subservice organization, the service auditor may decide to restrict the SOC 3 report to those users who understand how controls at the subservice organization interact with controls at the service organization. The AICPA SOC 2 guide provides additional examples of situations when a SOC 3 report may be restricted.

Subservice organizations

Most entities, including service organizations, outsource various functions to other organizations (vendors). The functions provided by these vendors may affect the delivery of services to user entities. Although management can delegate responsibility for these functions, management retains responsibility for the achievement of the service organization's objectives. In some cases, these vendors are considered to be subservice organizations. The definition of a subservice organization varies by engagement type:

- A vendor used by a service organization to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting (SOC 1 examination)
- A vendor used by a service organization that performs controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved (SOC 2 and SOC 3 examinations)

The use of subservice organizations presents unique considerations in a SOC for service organizations engagement. Because management retains responsibility for the achievement of the service organization's objectives, the controls at the subservice organization need to be addressed in some way. There are two methods to address subservice organizations, as follows:

- **Carve-out method.** Management's description of the service organization's system identifies the nature of the services performed by the subservice organization but excludes controls at the subservice organization. (When using the carve-out method, controls at the subservice organization are not included in the scope of the engagement and are not subject to the service auditor's examination procedures.)
- **Inclusive method.** Management's description of the service organization's system includes a description of the nature of the services provided by the subservice organization, as well as relevant controls at the subservice organization. (When using the inclusive method, controls at the subservice organization are included in the scope of the engagement and are subject to the service auditor's examination procedures.)

Although the carve-out method is most frequently used, there are circumstances in which the inclusive method is more appropriate. For example, if the services provided by the subservice organization are extensive or an appropriate SOC report is not available from the subservice organization, there may be little value in a SOC report that does not address controls at the subservice organization. Additional considerations related to the use of the carve-out method or inclusive method can be found in the AICPA SOC 1 guide or AICPA SOC 2 guide.

Recently, a number of software solutions (tools) have been introduced that are designed to improve the efficiency with which service organizations can prepare for and undergo SOC 2 examinations. Use of these tools requires special considerations by the service auditor. Depending on how the tool is being used by the service organization, the tool may be part of the service organization's internal control environment. This means that the tool provider may be a subservice organization and also may raise concerns about the independence of a service auditor who also has a business relationship with the developer of the software tools. For more detail on the use of software tools, see the AICPA *FAQ, Effect of the use of software tools on SOC 2® examinations*.

Reporting on additional criteria

Service organizations frequently design their systems of internal control to support compliance with one or more processes or control frameworks established by a third party. Depending on the commitments they have made to customers or business partners, service organization management may engage a service auditor to examine and report on whether the service organization's controls met the requirements of those third-party frameworks, in addition to whether the controls provided reasonable assurance of achieving the service organization's service commitments and system requirements based on the trust services criteria. These engagements are commonly referred to as SOC 2+ examinations. In a SOC 2+ examination, management's assertion and the service auditor's report both include an evaluation of controls against the additional frameworks or criteria.

Related services

Readiness assessments

A CPA firm can be engaged to perform a readiness assessment (also referred to as a gap analysis or gap assessment) under AICPA consulting standards. A readiness assessment is ordinarily performed in advance of a service organization's first SOC examination or when there have been significant changes to a service organization's controls or revisions to criteria against which controls are evaluated (e.g., the AICPA trust services criteria). In other situations, management may request a readiness assessment when it doesn't have the capacity or expertise to prepare a description of the system in accordance with the description criteria, wants an objective evaluation of its documentation and overall preparedness for a SOC examination, or some combination thereof.

Activities performed by the CPA firm as part of a readiness assessment service may include, but are not limited to, the following:

- Collecting and reviewing system-related policies and procedures
- Aligning system-related policies, procedures, or controls to the
  - specified control objectives (SOC 1 examination)
  - specified service commitments and system requirements based on the trust services criteria related to those service commitments and system requirements (SOC 2 examination)

- Assisting management with the development of the description of the system, including the description of controls within the system
- Conducting interviews with control owners to identify existing control activities
- Inspecting documentation of control implementation and/or operating effectiveness
- Identifying gaps (from the current state to readiness for a SOC examination) in the system of internal control, policies, procedures, or controls that require remediation

If the CPA firm is asked to perform a readiness assessment as a precursor to performing a SOC examination, the firm should consider whether providing this nonattest service would impair its independence. For example, the service auditor may make recommendations about controls needed. The service auditor may not, however, assume management responsibilities by making decisions about the design and implementation of such controls within the system. Designing, developing, or customizing the service organization's system, including the related internal controls, would impair the service auditor's independence, as would performing certain implementation, installation, and configuration services. In some cases, it may become necessary for a different CPA firm to perform the SOC examination. Other independence considerations are addressed in the following section.

Other SOC engagements

The AICPA developed a suite of SOC service offerings that CPAs may provide in connection with the system-level controls of a service organization or entity-level controls of other organizations. In addition to the SOC for service organizations examinations discussed in this document, other SOC services include the following:

- **SOC for Cybersecurity.** As part of an entity's cybersecurity risk management program, an entity designs, implements, and operates cybersecurity controls. In a SOC for Cybersecurity examination, the practitioner examines and reports on a description of the entity's cybersecurity risk management program and the effectiveness of controls within that program.

  Find more information about SOC for Cybersecurity examinations on the AICPA website.

- **SOC for Supply Chain.** Internal and external forces such as globalization, global interconnectivity, automation, and other technological advancements are making today's supply chains highly sophisticated and complex. For entities that produce, manufacture, or distribute products, there's often a high level of interdependence and connectivity between them and their suppliers and their customers and business partners. A SOC for Supply Chain examination helps these organizations, and their customers and business partners, identify, assess, and address supply chain risks.

Additional information about SOC for Supply Chain examinations can be found on AICPA's SOC for Supply Chain page.

Independence

Independence, as defined by the AICPA Code of Professional Conduct, is required for all examination-level engagements, including SOC for service organization examinations. The independence assessment process may address matters such as scope of services (including nonattest services), fee arrangements, firm and individual financial relationships, firm business relationships, and employment and familial relationships with the client and client personnel.

When performing engagements in which independence is required in accordance with the attestation standards, the service auditor needs to be independent with respect to the responsible party (or parties), as defined in those standards. If a subservice organization is included within the scope of the SOC for service organization examination under the inclusive method, the subservice organization is also a responsible party. Consequently, the service auditor must also be independent of the inclusive subservice organization in these instances. The service auditor need not be independent of each user entity of the service organization or a carved-out subservice organization.

Quality control

QM section 10A, A Firm's System of Quality Control (formerly QC section 10),[8] applies to firms that perform SOC for service organizations examinations. Under this standard, a firm is required to establish and maintain a system of quality control to provide reasonable assurance that the firm and its personnel comply with professional standards and applicable legal and regulatory requirements and that reports issued by the firm are appropriate in the circumstances. If a firm performs SOC for service organizations examinations, the firm's policies and procedures regarding its system of quality control should address those examinations. Firms that are considering adding SOC for service organizations examinations to their practices should place emphasis on the engagement acceptance aspects of their quality control policies and procedures to properly evaluate whether they have sufficient experience and expertise to perform SOC for service organizations examinations. This toolkit's *Considerations for adding SOC for service organizations services to your firm* discusses skills and qualifications necessary to provide SOC services.

QM section 10A also requires the firm to assign responsibility for each SOC for service organizations examination to an engagement partner and to establish policies and procedures surrounding that role. Sometimes, not all members of the engagement team are CPAs. However, the service auditor's report must be signed by a CPA who is appropriately licensed based on the requirements of the state in which the examination is performed. In these situations, the firm must determine that the CPA has adequate involvement in the examination, as well as the appropriate competencies, to fulfill their responsibilities under the relevant professional standards and that the CPA's involvement is adequately documented in the workpapers.

Firms need to establish criteria to determine when an engagement quality control review should be performed. An engagement quality control review is a process designed to provide an objective evaluation before a report is released. As discussed in the following section, SOC 1 and SOC 2 engagements are "must select" engagements as defined in the AICPA's peer review standards. As such, the firm will usually include all SOC for service organizations examinations in their engagement quality control review process.

Peer review

AICPA bylaws and the AICPA Code of Professional Conduct require that members engaged in the practice of public accounting be employed by a firm enrolled in an AICPA-approved practice-monitoring program. Even if a service auditor or firm is not an AICPA member, state boards of accountancy may have additional practice monitoring requirements. Because of these requirements, most firms issuing SOC examination reports are required to enroll in a practice monitoring program such as the AICPA Peer Review Program. Firms enrolled in the AICPA Peer Review Program are required to have a peer review once every three years. Firms should enroll in the program no later than the date on which the firm issues a report on the first engagement that falls within the scope of the peer review standards.

There are two types of peer reviews: system reviews and engagement reviews. System reviews are required for firms that perform engagements under the Statements on Auditing Standards (SASs) or *Government Auditing Standards*, examinations under the Statements on Standards for Attestation Engagements (SSAEs), or engagements under PCAOB standards as their highest level of service and focus on a firm's system of quality control. System reviews include the review of a cross-section of engagements to obtain reasonable assurance that the firm is complying with its quality control policies and procedures and applicable professional standards.

Engagement reviews focus on work performed on a sample of engagements and are available to firms that do not perform audits or other similar work, such as examinations under the SSAEs. Because SOC for service organizations examinations are performed under the SSAEs, firms issuing SOC examination reports undergo a system review. Under the requirements for a system review, SOC 1 and SOC 2 examinations are currently "must select" engagements, meaning that at least one SOC 1 or SOC 2 examination will be selected by the firm's peer reviewer for review. Additionally, if a firm's most recent peer review was an engagement review and then the firm subsequently performs a SOC examination, the firm would be required to have a system review due 18 months from the year-end of the engagement or by the firm's next scheduled due date (whichever is earlier).

Additional information about the AICPA Peer Review Program can be found on the AICPA website.

[8] Firms should be aware of Statement on Quality Management Standards (SQMS) No. 1, *A Firm's System of Quality Management* (QM section 10), which was issued by the Auditing Standards Board of the AICPA in June 2022 and is effective for a firm's accounting and auditing practice as of December 15, 2025. This standard supersedes Statement on Quality Control Standards No. 8, *A Firm's System of Quality Control* (QM section 10A). The full text of all QC sections (now codified as QM sec. 10A) is available via **AICPA SQCS – currently effective** on the AICPA website.

Considerations for adding **SOC services to your firm**

Considerations for adding SOC for service organizations services to your firm

For decades, CPAs have been known for providing "traditional" tax and accounting activities and audits of historical financial statements. Today, however, CPAs are expanding their auditing services beyond audits of historical financial statements to include audits of new and emerging subject matters. That's because, more than ever before, customers, business partners, boards of directors, and others are looking for organizations to provide consistent, transparent information about matters beyond those addressed in historical financial statements. Such users are interested in understanding how organizations are managing their internal control environments, particularly with respect to security and data privacy controls. Like a CPA's opinion on historical financial statements, a CPA's opinion on internal controls can enhance the trust and confidence that interested parties have in that information. For that reason, CPA firms with an appropriate level of expertise — or dedication to obtaining that expertise — see new opportunities in system and organization controls (SOC) assurance.

The AICPA's suite of SOC services provides assurance related to system-level controls of a service organization or system- or entity-level controls of other organizations. SOC for service organizations examinations, which include SOC 1®, SOC 2®, and SOC 3® examinations, are examinations of system-level controls of a service organization relevant to the services they provide. These engagements are the focus of this document, which addresses the following considerations that may be helpful when determining whether the firm should offer SOC services:

- How will the firm benefit from providing SOC services?
- Does the firm have staff with the requisite skills and qualifications to provide SOC services?
- Will offering SOC services be profitable for the firm?

How will the firm benefit from providing SOC for service organizations services?

Consideration of the following may be helpful when determining whether the firm should offer SOC for service organizations services:

- Firm partners/owners may be interested in building the legacy of a successful and profitable firm that adjusts to the changing times.
- Clients consider the firm as a trusted adviser in evaluating internal controls over financial reporting in a financial statement audit. This expertise can extend to new and future-ready services (for example, evaluating controls to address the security of a system).
- Expanding service offerings to include SOC 1 and SOC 2 services may allow the firm to do the following:
  - Meet the needs of existing service organization clients who want to provide their customers and business partners with assurance about the effectiveness of their controls relevant to financial reporting (SOC 1 examinations) or their controls relevant to security, availability, and processing integrity of the system used to process users' data and the confidentiality and privacy of the information the system processes (SOC 2 examinations)
  - Defend client base against competitors who are providing SOC services to existing service organization clients
  - Prepare to deliver attestation services on subject matters and emerging technologies that rely on the effectiveness of systems of internal control (for example, greenhouse gas reporting)
  - Open up access to additional prospective service organization clients
  - Provide a recurring revenue stream, making it easier to justify adding full-time equivalents (FTEs) with the requisite skills and competencies

Does the firm have staff with the requisite skills and qualifications to provide SOC for service organizations services?

The performance of quality SOC for service organizations services requires personnel who possess a particular set of skills and competencies. Although some of those skills and competencies, such as analytical skills, expertise in evaluating processes and control effectiveness, providing advisory and assurance services related to control effectiveness, and the ability to apply judgment and professional skepticism, are similar to those needed to perform a financial statement audit or compliance audit, other skills and competencies differ. Additionally, the requisite skills and competencies necessary to perform a SOC 1 examination differ from those required for a SOC 2 examination, since the types of controls evaluated in each examination are different. Consideration of whether firm personnel possess these skills and competencies is critical to determining whether to provide SOC services.

Applicable to all SOC for service organization examinations

- An understanding of professional standards and applicable legal and regulatory requirements.
- Ability to apply professional judgment.
- Understanding of the firm's quality control policies and procedures.
- Technical expertise, including expertise with IT general controls in areas such as access management, change management, backups, and job processing.
- Knowledge of relevant industries in which the entity operates.
- An understanding of preventive, detective, and corrective control activities as part of a multi-layer approach to risk management.
- Ability to design tests of controls based on the specific control activities of a service organization.

SOC 1 examinations

SOC 1 examinations focus on controls at a service organization that are relevant to user entities' internal control over financial reporting. Firms who provide audit services may be able to leverage their existing financial statement audit expertise to provide SOC 1 services. Appropriate competencies include the following:

- An understanding of, and practical experience with, SOC 1 examinations of a similar nature and complexity through appropriate training and participation
- The ability to understand service organization and industry-specific risks related to how the service organization processes relevant financial information on behalf of user entities
- Expertise with specialized areas of accounting or auditing relevant to the services provided by the service organization
- Experience with evaluating the suitability of design and operating effectiveness of controls over financial reporting using a framework such as COSO

SOC 2 and SOC 3 examinations

SOC 2 and SOC 3 examinations focus on controls at a service organization that relate to security, availability, confidentiality, processing integrity, or privacy. Accordingly, they require specialized information technology (IT) knowledge in addition to expertise on internal control. Appropriate competencies and capabilities for engagement team members performing SOC 2 and SOC 3 examinations include the following:

- An understanding, or the ability to obtain an understanding, of systems used to provide services, including operating and security of such systems, gained either through experience with engagements of a similar nature and complexity or through appropriate training and participation
- Knowledge of whether the industry in which the service organization operates is subject to specific types of or unusual security risks
- An understanding of business processes, risks, and controls
- Knowledge of relevant IT systems and technology, such as networks, firewalls or firewall techniques, security protocols, cloud-based systems, key applications, operating systems, and databases

- Knowledge of any uncommon technologies or industry-specific technologies used by the service organization
- An understanding of IT processes and controls, such as the management of operating systems, networking, and virtualization software and related security techniques; security principles and concepts; software development; and incident management and information risk management
- Experience with evaluating the suitability of design and operating effectiveness of controls relevant to security, availability, processing integrity, confidentiality, and privacy
- An understanding of the description criteria and trust services criteria used in the engagement

"SOC for service organizations learning resources," provided in this toolkit, details several resources for obtaining information about IT processes and controls to supplement expertise obtained through experience working on engagements of a similar nature and complexity or through appropriate training and participation.

Additional staffing considerations

SOC for service organization examinations tend to be very labor intensive. Depending on the scope of the examination and the nature of the client and its industry, SOC examinations may range from 100–500 hours or more and often span eight to 10 weeks of focused effort (see "Scoping and pricing considerations in SOC for service organizations engagements"). For that reason, firms should consider not only whether they have personnel with the required skills and competencies but also whether they have sufficient personnel to perform the potential SOC offerings. For example, firms may ask the following questions:

- Are there sufficient personnel with the appropriate skills and competencies to perform the new services, or will extensive training be necessary?
- Are additional personnel likely to be necessary to meet the demand for SOC for service organizations services?
- Will it be necessary to develop a hiring strategy to recruit new personnel with the appropriate skills and competencies?

If current staff do not already have or are not able to obtain the additional skills and competencies necessary to perform SOC for service organizations examinations, the firm may need to hire additional staff that already possess the necessary skills and competencies or engage specialists to aid in performance of SOC examinations.

Possible sources for recruiting new personnel include the following:

- Graduates of master of accountancy programs with a focus on IT systems
- Graduates of IT/cyber assurance or data analytics degree programs
- IT internal auditors
- Financial auditors (but may need to supplement their skills with additional IT competencies)
- Trade associations such as ISACA, Information Systems Security Association (ISSA), and state CPA societies

Recommended certifications for new personnel performing SOC for service organizations examinations include the CPA credential, the Certified Information Technology Profession (CITP®) credential, and other certifications such as Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA), Certified Information Systems Security Professional (CISSP), as well as service-specific certifications such as PCI Qualified Security Assessor (QSA), HITRUST Certified CSF Practitioner (CCSFP), or International Organization for Standardization (ISO) lead auditor.

Firms may also decide to engage a specialist to assist them in offering SOC for service organizations services. When using a specialist, the engagement partner is responsible for determining that the specialist has the necessary competence, capabilities, and objectivity for purposes of the engagement, as well as for evaluating the adequacy of the work performed by the specialist in accordance with relevant professional standards.

Will offering SOC for service organizations services be profitable for the firm?

When determining whether offering SOC for service organizations services will be profitable for the firm, the following tips may be helpful:

1. Identify potential SOC clients

- Existing clients that would benefit from SOC services.
  - Service organizations that provide services that directly tie to user entities' internal control over financial reporting (SOC 1 examinations). Examples of such service organizations include payroll processors, medical claims processors, loan servicing companies, and data centers.
  - Service organizations that receive requests (many in the form of security questionnaires) from numerous customers for information about security controls (SOC 2 examinations)
  - Service organizations whose controls are routinely audited by customer organizations (SOC 1 or SOC 2 examinations).
  - Service organizations that provide cloud services or routinely obtain, process, and transmit customer data (SOC 2 examinations). Examples of such service organizations include those that provide customer support, health care claims management and processing, enterprise IT outsourcing, eCommerce SaaS applications, managed security, financial technology services, and ESG metric services.
  - Service organizations that make contractual data security commitments to customers and business partners (SOC 2 examinations).

  When evaluating whether existing clients who receive nonattest services from the firm could benefit from SOC for service organizations services, consider whether the firm has the required independence to provide those services.
- Potential new clients that may be targeted by the SOC for service organizations service offerings. Identify potential clients considering the same attributes noted in the preceding list item for existing clients.

2. Estimate revenues SOC clients would generate

The firm should determine whether a new SOC practice would generate sufficient revenue to justify adding the service. The amount of revenue may be impacted by the billing strategy employed. Some options include:

- **Value pricing by service** — SOC for service organizations services can be offered in both fixed-fee and time-and-materials pricing options. In many cases, SOC services are quoted to the client on a fixed-fee basis, priced using blended rates, unless the client requests otherwise.
- **Tier offerings** — Consider the firm's service offerings and if there are levels of service to be provided. For example, SOC 2 examinations can be type 1 or type 2 and may or may not include additional subject matters or criteria (SOC 2+ examinations); the firm may also offer readiness assessments. Price the levels accordingly.

  When estimating revenues, also consider cross-selling opportunities or other additional revenue opportunities. In some situations, for example, a firm may be able to provide readiness assessment services to clients prior to the provision of a SOC examination.

3. Estimate the cost of developing a practice and providing SOC for service organizations services

A number of factors may add costs to the development of a new service opportunity, many of which cannot be directly billed to a client. A few of those considerations include:

- **Staffing** —As discussed in the earlier section on staff, there may be additional costs related to training current staff, hiring new personnel with the appropriate skills and competencies, or engaging specialists.
- **Training** — Costs related to continuing education and training to enhance the skills and competencies of firm personnel performing SOC examinations may increase. The "SOC for service organizations learning resources" section of this toolkit provides links to several available resources.

- **Software** — The cost of acquiring appropriate software/tools to increase the efficiency of providing the new SOC for service organizations services, including quality control materials such as work programs and checklists to aid in performing and documenting a SOC examination in accordance with relevant professional standards, should be considered.
- **Marketing** – Developing marketing materials and website content to market the firm's new SOC for service organizations services may be costly, at least initially.
- **Quality control (QC)** – Considering whether the skills and expertise of the firm's new SOC team enable the performance of effective QC reviews over SOC for service organizations services is essential. If no one aside from the engagement partner has the technical expertise and SOC experience required to perform the QC review, a partner relationship may need to be developed to perform QC reviews. See the "Overview of SOC for service organizations engagements" section of this toolkit for discussion of quality control considerations.
- **Peer review** – As mentioned in the "Overview of SOC for service organizations engagements" section, SOC 1 and SOC 2 examinations are "must select" engagements; therefore, they are subject to the peer review. As such, the firm's peer review costs may increase. In addition, the firm should consider whether its existing peer reviewer has the skills, competencies, and requisite expertise to perform a peer review of the firm's SOC 1 and SOC 2 examinations. If not, a new peer reviewer may need to be identified.

Additional considerations when the service organization uses a SOC tool

A number of technology companies offer software solutions (tools) to improve the efficiency with which service organizations can prepare for and undergo SOC 2 examinations. These providers advertise efficiencies that their software will provide to the service auditor. When the service organization uses these tools, it is important to remember that the service auditor is still responsible for performing a SOC 2 examination in accordance with professional standards. The service auditor should evaluate any platform being used and determine whether use of these tools results in a significant decrease in effort before assuming that the cost of performing an examination for a client using the platform will be significantly lower. Examples of how a service organization's use of these tools may affect how the service auditor meets relevant requirements of professional standards can be found on the AICPA website: *FAQs – Effect of the use of software tools on SOC 2 examinations*.

4. Develop a budget to assess profitability

In order to determine if the addition of SOC services will be profitable to the firm, a budget for the potential new service(s) should be developed considering the factors previously identified.

As with any niche practice, CPA firms must be diligent when providing new service offerings. This document outlines some important steps to take when considering the addition of SOC services; however, firms must remain cognizant of their abilities to provide SOC services in a quality manner. When properly executed, the addition of SOC for service organizations services can be a great boon for a firm and a huge benefit to its clients, further solidifying the firm's position as a trusted adviser.

To learn more about SOC for service organizations and potential service offering details, check out the other documents in this toolkit.

SOC for service organizations **implementation checklist**

SOC for service organizations implementation checklist

Once a firm has decided to add SOC for service organizations services (SOC 1®, SOC 2® and SOC 3® examinations) to the firm's service offerings, this checklist may be used to implement a strategy for offering those new services. (This toolkit's "Considerations for adding SOC services to your firm" may aid firm management in deciding whether to add SOC services.)

SOC for Service Organizations Implementation Checklist

Item	Considerations for success
1. Identify and designate a leader for your firm's SOC for service organizations services.	This designated individual will ideally be a CPA with prior experience overseeing or conducting SOC for service organizations services. If the designated individual is not a CPA, it is critical that the designated SOC leader is supported by a licensed CPA who can ensure that professional standards will be met and ultimately sign the opinions.
2. Identify qualified and capable staff to conduct SOC for service organizations engagements.	The performance of quality SOC services requires personnel who possess a unique set of skills and competencies. As discussed in "Considerations for adding SOC for service organizations services to your firm," the requisite skills and competencies necessary to perform a SOC 1 examination differ from those required for a SOC 2 examination. Current staff with a background in financial statement audits may be interested in performing SOC for service organizations examinations, leveraging their experience in evaluating internal controls against the COSO framework. However, COSO experience needs to be supplemented with SOC-specific skills and competencies or experience. Engagement teams comprising both current staff with COSO experience or experience with other control frameworks and newly hired staff or external specialists with SOC-specific expertise will strengthen the firm's roster as current staff gain SOC-specific experience through participation on SOC for service organizations examinations.
3. Determine which SOC services your firm will offer.	Refer to "Overview of SOC for service organizations engagements" for a list of SOC services that could be provided. When determining which SOC services to offer, be sure to consider whether these services will be profitable. See "Considerations for adding SOC for service organizations services to your firm" for additional considerations.

Item	Considerations for success
4. Educate all firm employees on the SOC services that your firm will offer.	Use "Overview of SOC for service organizations engagements" and "Client assessment template: SOC 1 and SOC 2 service opportunities" to educate employees in other service lines within your firm on how to identify client needs for new SOC for service organizations services and cultivate new opportunities. Marketing materials developed to share with clients that talk about the benefits of SOC services may be shared with employees to educate them as well.
5. Identify service organization clients that may need SOC for service organizations engagements.	Review a listing of the firm's service organization clients and understand their potential need for SOC for service organizations services. Partners and managers who are not involved in SOC for service organizations engagements but have relationships with those clients can share their understanding of the types of services the service organization provides. They may also have insight into the maturity of the service organization's system of internal control over the services it performs for user entities. These individuals may also know if the service organization is already receiving SOC for service organizations services somewhere else. This information may be used to identify those service organization clients who could benefit from SOC services so they can be targeted by the firm.
6. Identify a key contact at each existing and potential client with whom to discuss the service organization's need for SOC services.	A key to successfully building a SOC for service organizations services offering is identifying an appropriate contact at the service organization who is able to speak with firm personnel about the service organization's service offerings, IT operations, and security posture. In addition, the individual should be able to discuss requests from customers (user entities), business partners, and others for information about effectiveness of the service organization's internal controls. An effective key contact should also be aware of any market pressures or requests for SOC reporting or information on internal controls at the service organization. Though discussions with the controller, financial reporting manager, or CFO may identify needs for a SOC 1 examination, IT department leaders (who may have a title such as chief information officer (CIO), chief information security officer (CISO), vice president of IT, director of IT, or IT manager) may be better positioned to discuss needs for a SOC 2 examination. For smaller organizations, roles may be limited or overlap. The firm should review the personnel structure with their client contact and use their judgment in determining the person in the best position for these discussions. Non-SOC professionals may find the "Client assessment template: SOC 1 and SOC 2 service opportunities" section of this toolkit useful as a guide when meeting with existing clients to help identify their SOC for service organizations needs.

Item	Considerations for success
7. Evaluate independence and objectivity as part of the client acceptance and continuance process when performing SOC services.	Just as with financial audits, the firm should be careful to protect its independence and objectivity when providing SOC services to its clients. For example, if the firm or a member of the firm's network has designed or developed an information system that is within the scope of the SOC examination, the firm's independence would be impaired under the "Information Systems Services" interpretation (ET section 1.295.145) of the AICPA Code of Professional Conduct). Many security-related services can be provided without compromising independence. However, the firm should be mindful of these considerations as they offer new SOC for service organizations services to their clients.
8. Establish an appropriate quality review process to ensure appropriate conclusions were reached in formulating the service auditor's opinion.	As discussed in the "Overview of SOC for service organizations engagements" section, SOC examinations are usually included in the firm's engagement quality control review process. The firm should determine that quality control reviewers have the appropriate competencies and capabilities to review SOC for service organizations engagements. This includes having SOC experience and sufficient time to complete an effective review. If the only firm leader with appropriate SOC expertise participated in the SOC for service organizations examination being reviewed, the firm may consider partnering with another firm that has the relevant expertise to ensure that appropriate knowledge and expertise is used in the review. Firms that do not use reviewers with sufficient SOC expertise are at risk of missing key security issues, noncompliance with relevant professional standards, issuing an incorrect opinion in connection with the SOC engagement, and other issues.
9. Determine the pricing method that will be used to implement the firm's selected fee and pricing structure for the SOC services your firm will provide.	As noted in "Considerations for adding SOC for service organizations services to your firm," SOC services can be offered in both fixed-fee and time-and-materials pricing options. In many cases, SOC services are quoted to the client on a fixed-fee basis, unless the client requests otherwise.
10. Develop marketing materials and website content to describe the firm's SOC for service organizations offerings.	Marketing materials will help to clearly define and explain the SOC services being offered to both clients and prospects who may be unfamiliar with SOC for service organizations examinations. Once the firm has started performing SOC for service organizations examinations, register for the SOC for service organizations logo for CPAs for use on the firm website and marketing materials to show that the firm offers SOC for Service Organizations services. SOC 1®, SOC 2®, SOC 3® and the associated logos are trademarks, service marks, and certification marks of the AICPA. These trademarks prohibit firms from creating their own SOC logos, seals, or certificates. Read the logo guidelines and terms of use for additional details.

Item	Considerations for success
11. Identify relevant trade associations and other similar organizations and get involved.	IT audit and security trade associations such as ISACA, (ISC)2 and Information Systems Security Association (ISSA) have local chapters in many markets. These chapters are great places to network and meet potential clients and experts who can help supplement staffing or provide expertise for a SOC for service organizations examination, as well as help keep staff up to date on the latest cybersecurity trends. State-level technology associations, the Institute of Internal Auditors (IIA), the AICPA, and state CPA societies also provide networking opportunities that may generate leads.
12. Annually, or more often if considered necessary, evaluate the results of providing the new SOC for service organizations services and consider any changes that might be necessary to expand the SOC market and increase the profitability of providing SOC services.	Regular evaluations help firm leadership determine that the firm is offering the right services. This assessment may require the SOC leader to add new services, eliminate existing services that are not resonating with the firm's client base, or evaluate client relationships and fee structures. The firm should also evaluate staffing levels to ensure that sufficient expertise is available to meet current and anticipated client needs.
13. If not already registered, register with an appropriate peer review program.	A firm that is new to providing attestation services should contact the state board of accountancy or the administering entity for its state's peer review program to determine how and when to enroll in the required peer review program.

Client assessment template:
SOC 1 and SOC 2 services opportunities

Client assessment template: SOC 1® and SOC 2® service opportunities

Partners and managers who are not involved in SOC for service organizations engagements may also have clients or potential clients that would benefit from SOC for service organizations services. This template is designed to help those partners and managers less familiar with this type of SOC engagement identify client needs for new SOC for service organizations services. The following list of questions can assist the firm in gauging a service organization's need for SOC reporting. For existing clients, some of this information may already be available. For each question, the table shows whether the answer may indicate the need for a SOC 1 examination or a SOC 2 examination. This list is not all-inclusive and is intended only as a guide to aid in preparation for the client/prospective client meeting and to assist the service auditor in determining the most applicable opportunities for each client's need.

For a detailed description of SOC examinations, refer to the "Overview of SOC for service organizations engagements," section of the toolkit.

Note: SOC for service organizations services are attestation engagements and will require the firm and the service auditor to maintain independence from the client. The "Overview of SOC for service organizations engagements" provides additional information about independence in a SOC for service organizations engagement.

Client/Prospect Name:

Date of Discussion:

[A checkmark in the SOC 1 and SOC 2 columns notes where a "yes" answer indicates that the engagement may be useful to that client or prospective client.]

Questions to ask a client or prospect that could indicate a need for SOC for service organizations services:	Client/Prospect Answer	Applicable Engagement	
		SOC 1	SOC 2
1. Have you ever been asked for a SOC (SAS No. 70, SSAE No. 16, SSAE No. 18) report?		✓*	✓*
2. Do any of your contracts with customers or business partners mention obtaining a SOC report?		✓*	✓*
3. Do any of your competitors routinely provide SOC reports to customers or business partners?		✓*	✓*

* A "yes" answer indicates that the client or prospective client may benefit from a SOC for service organizations examination. Whether a SOC 1 or SOC 2 report would be more useful depends on the answers to the other questions.

Questions to ask a client or prospect that could indicate a need for SOC for service organizations services:	Client/Prospect Answer	Applicable Engagement	
		SOC 1	SOC 2
4. Are any of the services you provide relevant to your customers' internal control over financial reporting (ICFR)?		✓	
5. Do you hold data that your customers would deem "sensitive"? (e.g. personal health information, personally identifying information, proprietary corporate information, etc.)			✓
6. Have you made commitments to customers or business partners related to the confidentiality or privacy of their information or the security, processing integrity, or availability of your system?			✓
7. Have any of your customers or business partners asked about your information security practices or required you to complete security questionnaires?			✓

After determining that a SOC 1 or SOC 2 examination would be beneficial for the client or prospective client, these additional questions may pinpoint whether a type 1 or type 2 report would best meet the client's needs.

Questions to ask a client or prospective client to differentiate between type 1 and type 2 reports:	Client/Prospect Answer	Applicable Engagement Type	
		Type 1	Type 2
8. Are customers or potential customers only concerned with the design of controls or are they also interested in whether your controls are operating effectively?		Design only	Design and operating effectiveness
9. Has the system, including related controls, been in operation for a sufficient period of time to enable the service auditor to opine on the operating effectiveness of controls?		No	Yes
10. Is sufficient appropriate evidence likely to be available to demonstrate that controls operated effectively during the period?[9]		No	Yes

If it is determined that a type 2 SOC 2 examination would be beneficial for the client or potential client, a SOC 3® report may also be useful. The firm representative may ask the client if they are also looking for a general use report to publish on their website for marketing purposes or to share with prospects not yet under a nondisclosure agreement.

[9] Sufficient appropriate evidence to demonstrate that controls operated effectively during the period may not be available; for example, if the service organization has not formally documented controls and their operation. A complete lack of documentation, however, cannot be overcome by performing a type 1 SOC 1 or type 1 SOC 2 examination. Sufficient evidence must be available to show that the controls were appropriately designed and implemented to support the opinion in a type 1 SOC 1 or type 1 SOC 2 examination.

Scoping and pricing considerations in SOC for service organizations engagements

Scoping and pricing considerations in SOC for service organizations engagements

Typically, the amount a firm charges to perform a SOC for service organizations examination is directly related to the cost of performing the engagement. Costs vary widely and are based on many factors including, but not limited to, the following:

- The nature, size, and complexity of the service organization and attestation or compliance assessment history
- The scope of the engagement, including the following:
  - Services provided by the service organization
  - Nature, size, and complexity of the system being examined
  - Trust services category or categories included in a SOC 2® examination
  - Type of examination (type 1 or type 2)
  - Period covered by the report and frequency of report issuance
  - Use of third parties, including subservice organizations, and how subservice organizations are presented (inclusive or carve out method)
- The makeup of the engagement team, including the following:
  - Skills and competencies of the engagement team
  - Prior experience with the service organization, industry, and objectives (SOC 1® examination) or trust service categories (SOC 2 examination)
  - Labor costs

For these reasons, it is impossible for this document to provide estimates of the cost to perform a particular SOC for service organizations engagement. However, to assist firms with making pricing decisions, the following table discusses in further detail several factors that are likely to affect the cost of a new SOC for service organizations engagement. Consideration of factors such as these may lead to more accurate budgeting when responding to a request for proposal.

Factor	Lower effort/cost	Higher effort/cost
Nature, size, and complexity of the service organization		
Nature and complexity: The nature of the service organization includes its legal structure, the industry in which it operates, and the services it provides.	• Unregulated industry or services • Simple ownership and governance structure • Single location • Centralized operations and internal control structure • Mature controls and control environment	• Highly regulated industry or services • An industry that is at a high risk of cyber attacks • Complex ownership and governance structure with some systems or process performed at a parent company • Multiple locations • Decentralized operations and internal control structure • Immature controls and control environment
Size: Larger organizations may have attributes that could increase the effort required to perform the examination, such as • more complex services, • more complex systems, • more complex business structures, and • increased risk of negative publicity if a security breach occurs or if sensitive customer data is stolen. Larger organizations may also have more resources to allocate to SOC-related tasks, which may decrease the level of effort required by the engagement team.	• Simple business model with a single service offering provided by a single system • Internal audit function that may be used to provide direct assistance to the service auditor • Personnel dedicated to fulfilling requests and responding to service auditor inquiries • Experienced management personnel tasked with monitoring the completion of the SOC for service organizations engagement on a timely basis	• Complex business model or structure with multiple service offerings, business layers, or departments supporting those services, and interconnected systems • Inexperienced management personnel tasked with monitoring the completion of the SOC for service organizations engagement on a timely basis

Factor	Lower effort/cost	Higher effort/cost
Nature, size, and complexity of the service organization		
Other attestation or compliance assessments: Service organizations that have previously undergone some type of attestation engagement or readiness assessment are likely to be better prepared for a SOC for service organizations examination.	• Moderate or extensive experience in undergoing internal or external audits • Prior assessment of controls against a framework similar to the criteria used in the SOC for service organizations engagement • Exceptions, issues, or deficiencies from assessments have been remediated • Recommendations from gap assessment have been implemented	• Little or no experience undergoing internal or external audits • Unremedied exceptions, issues, or deficiencies from prior assessments
Scope of the engagement		
Services provided by the service organization: Service organizations may provide a vast array of services. The number of services within the scope of the engagement and the nature and complexity of those services (including the classes of transactions being processed) affect the amount of effort necessary to complete the engagement.	• Engagement covers a single basic service • Processes simple transactions	• Engagement covers multiple services • Processes complex transactions
Nature and size of the system being examined: The components of a system that are necessary to provide a specific service on which the SOC for service organizations examination is to be performed are affected by the boundaries of the system. The number and nature of components (e.g., infrastructure, software, people, procedures, and data) within the boundaries of the system affect the extent of work to be performed.	• Only a few software applications included within the boundaries of the system • Few interface points • Small staff involved in developing, managing, operating, and securing the system being examined, but enough to allow for adequate segregation of duties and monitoring of controls • Incomplete or haphazard policies and procedures related to the system being examined	• Multiple software applications included within the boundaries of the system • Multiple interface points • Large staff involved in developing, managing, operating, and securing the system being examined with a large number of duties • Increased nature, timing, or extent of procedures to address inadequate segregation of duties • Well-documented policies and procedures related to the system being examined

Factor	Lower effort/cost	Higher effort/cost
Scope of the engagement		
Trust services categories: In a SOC 2 engagement, the service organization may engage the service auditor to report on controls related to one or more of the trust services categories (security, availability, processing integrity, confidentiality, and privacy). The number and type of trust services categories included within the scope of the SOC for service organizations engagement affects the level of effort required to perform the engagement.	• Fewer trust services categories	• More trust services categories • More complex categories such as privacy
Engagement type: Both SOC 1 and SOC 2 examinations are available in two types. • **A type 1 examination addresses the *description of the system and the suitability of design of controls at a point in time*.** • **A type 2 examination addresses the *description of the system, the suitability of design of controls, and the operating effectiveness of controls*.** A **SOC 3** report is typically issued in conjunction with a SOC 2 examination once the examination has been completed and the SOC 2 report issued. The additional effort relates only to the issuance of the SOC 3 report. There is no type 1 report option for a SOC 3 report. The "Overview of SOC for service organizations engagements" in this toolkit discusses SOC 3 reports in more detail.	• Type 1 SOC 1 examination • Type 1 SOC 2 examination	• Type 2 SOC 1 examination • Type 2 SOC 2 examination • SOC 3 report • SOC for service organizations examination performed in conjunction with other audit or compliance efforts or SOC 2+ examination

Factor	Lower effort/cost	Higher effort/cost
Scope of the engagement		
Period addressed by examination and reporting frequency: Unlike a financial statement audit, it is not uncommon for a SOC for service organizations examination to cover a period of less than 12 months. A SOC for service organizations engagement may also be performed more or less frequently than annually.	• Annual reporting	• Reporting on a period longer than 12 months • More than one examination of a period less than 12 months during the year • Extensions or modifications to the period originally agreed to in the terms of engagement
Use of third parties: Most entities, including service organizations, outsource various functions to other organizations (vendors). When the service organization outsources certain activities to vendors, the extent of work to be performed in a SOC for service organizations examination is affected by **whether the vendor(s) used by the service organization is considered a subservice organization(s)**. In that case, the extent of work is further affected by • **the number of subservice organizations;** • **whether management elects to use the inclusive or carve-out method to describe the services provided by the subservice organizations in the SOC report; and** • **whether the subservice organization obtained a SOC report.** Subservice organizations are discussed in more detail in "Overview of SOC for service organizations engagements."	• No or few subservice organizations described using the inclusive method • All or most subservice organizations carved out of the system description • The subservice organization submits a SOC report that addresses the applicable control objectives (SOC 1 examination) or trust services criteria (SOC 2 examination)	• Multiple subservice organizations described using the inclusive method • None or few of the subservice organizations carved out of the system description • The subservice organization does not have a SOC report, which necessitates the performance of additional procedures when testing monitoring activities

Factor	Lower effort/cost	Higher effort/cost
Makeup of the engagement team		
Skills and competencies of the engagement team: More experienced teams usually complete the examination in less time than teams with less experience.	• More experienced engagement team	• Less experienced engagement team • Additional training costs
Personnel costs: The cost of a SOC for service organizations engagement is also affected by personnel costs, both internal and external.	• Lower overhead allocation rates • Use of appropriate staff levels for a given task • Availability of in-house specialists	• Higher overhead allocation rates • Higher salaries for more experienced team members • Top-heavy engagement team • Use of external specialist • Use of another firm
Prior experience: The number of hours it takes to perform an engagement may also be affected by whether or not the firm has prior experience with • **the service organization,** • **the industry in which the service organization operates, and** • **the service organization's control objectives (SOC 1) or the applicable trust service categories (SOC 2).**	• Recurring SOC for service organizations engagement • Prior industry experience (which may mean similar control objectives to those encountered in prior engagements) • Extensive experience with examinations that include all categories of the trust services criteria	• First-time engagement • SOC client operates in industry that is new or unfamiliar to team members • No or only limited experience with examinations that include certain categories of trust services criteria (for example, privacy)

SOC for service organizations **learning resources**

SOC for service organizations learning resources

We have compiled a collection of resources for professionals interested in learning more about controls over financial reporting; controls relevant to security, availability, and processing integrity of the system a service organization uses to process users' data; and controls relevant to the confidentiality and privacy of information the system processes. These resources provide information that may enhance firm personnel's understanding of SOC for service organizations engagements. However, they are not a substitute for experience with engagements of a similar nature and complexity or appropriate training and participation.

Authoritative AICPA guidance

The following resources, organized by engagement type, provide authoritative guidance for service auditors performing SOC for service organizations examinations:

Engagement Type	Description	Tools/reference
SOC 1® — SOC for Service Organizations: ICFR	A SOC 1 examination is performed in accordance with AT-C section 320. A SOC 1 examination is an examination of controls at a service organization that are relevant to user entities' internal control over financial reporting. The service auditor has the option of reporting on the system description and the design and implementation of controls (type 1) or the system description and the design, implementation, and operating effectiveness of controls (type 2).	AT-C section 105, *Concepts Common to All Attestation Engagements*[10] AT-C section 205, *Assertion-Based Examination Engagements*[10] AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*[10] AICPA Guide *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1®)*

[10] The full text of all AT-C sections is available via **AICPA SSAEs – currently effective** on the AICPA website. All AT-C sections can also be found in AICPA Professional Standards.

Engagement Type	Description	Tools/reference
SOC 2® — SOC for Service Organizations: Trust Services Criteria	A SOC 2 examination is performed in accordance with AT-C section 205. The *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* is used to evaluate management's description of the system and the *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* is used to evaluate the design and implementation (type 1) or the design, implementation, and operating effectiveness (type 2) of a service organization's controls. The SOC 2 report focuses on an organization's nonfinancial reporting controls as they relate to one or more of the following categories: security, availability, processing integrity, confidentiality, or privacy of a system.	DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (with Revised Implementation Guidance – 2022)*[11] TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)*[12] AT-C section 105, *Concepts Common to All Attestation Engagements* AT-C section 205, *Assertion-Based Examination Engagements* AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*
SOC 3® — SOC for Service Organizations: Trust Services Criteria for General Use Report	Similar to a SOC 2 examination, the SOC 3 examination is performed in accordance with AT-C section 205. Unlike a SOC 2 report, which is limited to the use of specified parties, a SOC 3 report is usually appropriate for general users. Although a SOC 3 report does not include a complete description of the system, it does include a description of the boundaries of the system examined.	TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (with Revised Points of Focus – 2022)* AT-C section 105, *Concepts Common to All Attestation Engagements* AT-C section 205, *Assertion-Based Examination Engagements* AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*

[11] All DC sections can be found in AICPA Professional Standards.
[12] All TSP sections can be found in AICPA Professional Standards.

AICPA nonauthoritative publications

The following resources provide nonauthoritative guidance for service auditors performing SOC for service organizations examinations:

Resource type	Description	Tools/reference
FAQs for SOC 2® and SOC 3® examinations	Provides nonauthoritative guidance on selected practice matters raised by members in connection with SOC 2 and SOC 3 examinations.	Read the latest FAQs for SOC 2® and SOC 3® examinations
FAQs for using software tools on SOC 2® examinations	Describes risks that arise from the functionality of SOC 2 tools and the service organization's use of such tools.	FAQs – Effect of the use of software tools on SOC 2® examinations
Materiality white paper	Presents materiality considerations for attestation engagements involving aspects of subject matters that cannot be quantitatively measured.	Materiality considerations for attestation engagements
White paper discussing the difference between a SOC 2 examination and a SOC for Cybersecurity examination	Discusses key distinctions between SOC 2 and SOC for Cybersecurity examinations.	Learn about the key distinctions between a SOC 2 examination and SOC for Cybersecurity examination
Brochure comparing SOC 2 and SOC for Cybersecurity	Discusses the differences between SOC 2 and SOC for Cybersecurity examinations and how they can provide insight into an organization's cybersecurity controls.	See how SOC 2® and SOC for Cybersecurity differ and how they can help
SOC communication guidelines	Identifies the recommended use of commonly used terms and trademarks for SOC engagements	AICPA System and Organization Controls communication guidelines
SOC peer review checklists	PRP Sections 21,100 (SOC 1 examination) and 21,150 (SOC 2 examination) present highly summarized checklists with references to authoritative guidance and may be reviewed by the service auditor to understand the expectations of the peer reviewer.	AICPA Peer Review Engagement Checklists and Other Practice Aids

Resource type	Description	Tools/reference
Information for management	Describes management's responsibilities in a SOC 1 or SOC 2 examination, including information to assist management in preparing the system description.	Information for Service Organization Management in a SOC 1® Engagement Information for Service Organization Management in a SOC 2® Engagement
Illustrative SOC reports	Presents illustrative examples of SOC 2 and SOC 3 reports, including assertions and service auditor reports. The SOC 2 example also includes an illustrative system description. An illustrative SOC 1 service auditor's report and illustrative assertion are available in exhibit A and exhibit B of AT-C section 320. A complete illustrative SOC 1 report, including an illustrative description and description of tests and results, is available in appendix A of the AICPA SOC 1 Guide.	Illustrative SOC 2® Report with Illustrative System Description Illustrative SOC 3® Report AT-C 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*[13] AICPA Guide *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1®)*
Additional AICPA SOC 1 resources	The SOC 1 subtopic page on the AICPA website provides several documents relevant to the performance of a SOC 1 examination.	AICPA SOC 1 resources
Additional AICPA SOC 2 resources	The SOC 2 subtopic page on the AICPA website provides several documents relevant to the performance of a SOC 2 examination.	AICPA SOC 2 resources
Additional AICPA SOC 3 resources	The SOC 3 subtopic page on the AICPA website provides several documents relevant to the issuance of a SOC 3 report.	AICPA SOC 3 resources

[13] See footnote 10.

Learning, certification, and credentialing programs

The following programs may help practitioners new to providing SOC for service organizations services better understand SOC engagements or help experienced practitioners continue to build their knowledge base. The knowledge obtained by completing these courses may supplement the knowledge and skills gained through working with an experienced SOC engagement team.

AICPA programs

Program	Description	Tools/reference
AICPA SOC 1, 2, and 3 CPE and learning offerings	Publications, CPE, conferences, and webcasts relevant to the SOC suite of services.	SOC for service organizations learning opportunities
AICPA SOC School	A deep dive into key aspects of planning, executing, and reporting on SOC for service organizations examinations. This course is designed for senior staff and above who specialize in SOC for service organizations examinations.	SOC for service organizations school
AICPA Certified Information Technology Professional (CITP®) credential	The CITP credential was established for CPAs to demonstrate their expertise in disciplines such as IT assurance, risk, security and privacy, analytics, and technology. To obtain the credential, you must pass the CITP exam.	What is the CITP credential?

Other programs

Program	Description	Tools/reference
Information Systems Audit and Control Association (ISACA) Certified Information Systems Auditor (CISA) certification	CISA is a certification that focuses on IT audit expertise. To obtain the credential, the candidate must pass the CISA exam and complete the required work experience.	In a World Full of Auditors, Be a CISA
Cloud Security Alliance (CSA) Certificate of Cloud Security Knowledge (CCSK)	CCSK focuses on cloud security. The CCSK certificate is issued to individuals who demonstrate cloud security knowledge by passing the CCSK exam.	Certificate of Cloud Security Knowledge (CCSK)

Program	Description	Tools/reference
CSA and ISACA Certificate of Cloud Auditing Knowledge (CCAK)	CCAK is focused on cloud auditing. This certificate is issued to individuals who pass the CCAK exam CSA strongly recommends that individuals earn their CCSK before pursuing the CCAK.	Certificate of Cloud Auditing Knowledge
Certified Information Systems Security Professional (CISSP) certification	The CISSP certification administered by (ISC)2 focuses on information security. To obtain the certification, candidates must pass the CISSP exam as well as complete the required work experience.	CISSP certification
The Institute of Internal Auditors (IIA) Certified Internal Auditor (CIA) certification	The CIA credential focuses on internal audit and demonstrates competencies in areas relevant to SOC for Service Organizations examinations such as risk management and internal control. Candidates must pass the CIA exam and complete the required work experience.	CIA certification
Resources to obtain basic cloud understanding	To obtain a basic understanding of the cloud and what it means for business, a general high-level understanding of the cloud is necessary. These reference sources can help to inform that basic understanding.	The LINUX Foundation – Introduction to Cloud Infrastructure Technologies Amazon Web Services (AWS) – Training and Certification eduonix – Learn Cloud Computing from Scratch for Beginners ûdemy – Cloud Computing for Beginners – Infrastructure as a Service
Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, and Oracle Cloud Infrastructure certifications	Major cloud service providers have certification programs that offer the opportunity to learn a broad set of technical skills and cloud expertise. A certification is earned by passing an exam that demonstrates understanding of cloud computing. The knowledge obtained through the preparation for these exams may be particularly useful when providing services for clients that use the services of cloud service providers. There are multiple levels of certification available.	AWS certification Microsoft certifications Google Cloud certifications Oracle Cloud Infrastructure certification path

COSO's ICFR framework

The following provides information about the COSO framework. Originally designed as an internal management framework, the COSO framework is commonly used as a basis for reporting on internal control over financial reporting (ICFR). Beginning with the 2017 update to the AICPA trust services criteria, the COSO framework was incorporated into the criteria used for SOC 2 and SOC 3 examinations.

Title	Description	Tools/reference
COSO *Internal Control – Integrated Framework*	COSO's *Internal Control – Integrated Framework (framework)*[14] is commonly used by organizations to effectively and efficiently develop systems of internal control that adapt to changing business and operating environments, mitigate risks to acceptable levels, and support sound decision-making and governance of the organization. The COSO framework is used by most SEC registrants to evaluate the effectiveness of their internal controls over financial reporting (ICFR); however, the framework can also be used to evaluate internal controls over compliance and operations.	*"Internal Control – Integrated Framework"* AICPA COSO resources

[14] Excerpt from the framework's "Executive Summary." ©2023 Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used by permission. See www.coso.org.

Other process or control frameworks

Many service organizations undergoing SOC 2 and SOC 3 examinations will build their internal control environments based on well-recognized process or control frameworks published by various sponsoring organizations. As a service auditor conducting SOC 2 and SOC 3 examinations, it is important to be aware of these frameworks. Mappings from the trust services criteria to other process or control frameworks can be found on the AICPA website. Firms may be engaged to perform other attestation work related to these frameworks – those engagements are not addressed by this toolkit. The firm should do appropriate due diligence to understand the necessary requirements to perform those engagements.

Title	Description	Tools/reference
International Organization for Standardization (ISO)/ International Electrotechnical commission (IEC) 27000 family of standards	The ISO/IEC 27000 family of standards is framework that presents best practices in information security.	ISO/IEC 27001 and related standards: Information security management ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53	The NIST SP 800-53 framework provides a catalog of security controls and is commonly used by U.S. government agencies and contractors.	NIST SP 800-53 Rev. 5 — Security and Privacy Controls for Information Systems and Organizations
NIST Cybersecurity Framework (CSF)	The NIST CSF framework contains guidelines to help organizations manage cybersecurity-related risks.	NIST CSF
Control Objectives for Information and Related Technologies (COBIT®)	COBIT is an IT control framework created by ISACA which focuses on security, risk management, and information governance.	COBIT 2019 online resource center
CSA Cloud Controls Matrix (CCM)	The CSA CCM is a cybersecurity control framework that focuses on cloud computing.	CCM framework

Information security regulations

Many industries follow specific regulations and several states have enacted privacy, data security, cybersecurity, and data breach notification laws. The following laws and regulations related to information security may be relevant to a SOC 2 or SOC 3 examination; service organizations storing, processing, or transmitting certain types of data may have to meet the minimum security requirements outlined in these regulations. This is not meant to be a comprehensive list; for example, many states have adopted data privacy laws or regulations. Practitioners should be familiar with the regulations with which their clients are required to comply.

Title	Description	Tools/reference
Health Insurance Portability and Accountability Act (HIPAA) Security Rule	The HIPAA Security Rule regulates protection of sensitive patient data, referred to as protected health information (PHI).	HIPAA for Professionals HIPAA Training Materials Health IT Privacy and Security Resources for Providers NIST HIPAA Guide HIPAA and Administrative Simplification, Centers for Medicare & Medicaid Services
General Data Protection Regulation (GDPR)	The GDPR regulates data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside these areas. The regulation has become a model for many other laws across the world. U.S. companies operating in the EU are required to comply with the GDPR.	Complete guide to GDPR compliance
The Payment Card Industry Data Security Standard (PCI DSS)	PCI DSS provides standards for payment card information security and is contractually required for any organization that stores, processes, or transmits cardholder information.	PCI Security Standards Council Document Library PCI Perspectives PCI DSS Maintaining Payment Security

Acknowledgements

The AICPA gratefully acknowledges the following individuals who contributed to the development of this toolkit:

Jim Bourke
Jeff Cook
Jaclyn Dettloff
Christine Figge
Troy Fine
Scott Hicks
Kim Koch
Chris Kradjan
Sean Linton
Laura Naples
John Richardson
Chris Stormer
Scott Woznicki

The AICPA would also like to recognize LBMC, whose work on the AICPA's Private Companies Practice Section Cybersecurity Toolkit was also used in the development of this toolkit.

Founded by AICPA and CIMA, the Association of International Certified Professional Accountants powers leaders in accounting and finance around the globe.