Third-party risk management – Working with service organizations

Reminders and leading practices for user entities

November 2024

Shape the future with confidence

Table of contents

Summary

“

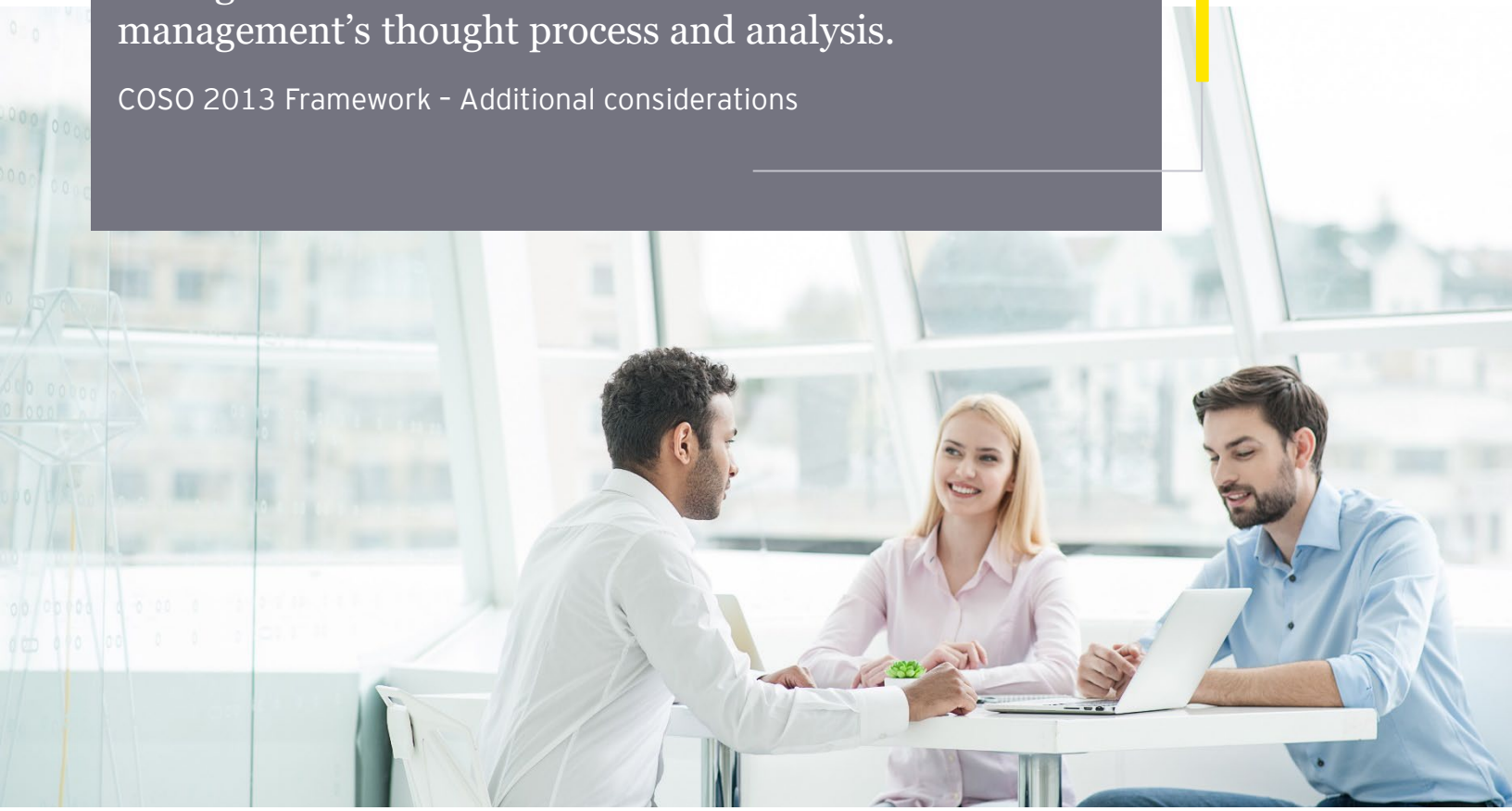
As part of its evaluation of ICFR, management must maintain reasonable support for its assessment. Documentation of the design of the controls management has placed in operation to adequately address the financial reporting risks, including the entity-level and other pervasive elements necessary for effective ICFR, is an integral part of the reasonable support.

SEC Release 33-8810

“

… it is important to keep in mind that controls … cannot be performed entirely in the minds of senior management without some documentation of management’s thought process and analysis.

COSO 2013 Framework - Additional considerations



Summary

When an entity uses one or more service organizations' services in the preparation of its financial statements, including transaction processing and the related information technology (IT) systems, it is outsourcing the operation of part of its internal control environment to another organization. However, the outsourcing does not relieve the entity of its responsibility for those controls. The design and operation of relevant controls at a service organization become part of the entity's system of internal control over financial reporting (ICFR).

This document provides information about the control considerations related to using service organizations for financial reporting purposes. It also provides entities with recommendations on working with these organizations effectively and efficiently and making sure the risks of using the service organizations are appropriately addressed for internal control over financial reporting (ICFR) purposes. Note that although this guide includes references to the Securities and Exchange Commission (SEC) and ICFR, the concepts and tips apply to any entity that uses service organizations.

Key points:

- *Don't be surprised* — Develop a relationship with the service organization so your entity is apprised of any controls-related issues as early as possible
- *Be prepared* —
  - Include key requirements in the contract with the service organization
  - Make sure controls specified by the service organization as needing to be in place at your entity (called "complementary user entity controls" or CUECs) from a prior-period report have been mapped to entity controls for which your entity has gathered evidence of operating effectiveness. The mapping can be updated when the current-period report is received; and
  - Identify the key reports from the service organization your entity relies on and make sure their completeness and accuracy will be covered by tested controls that will be included in a *Report on controls relevant to user entity's internal control over financial reporting* (SOC 1®) report (explained in sections 3 and 4).
- *Watch out for mismatched timing* — Know the period of the expected SOC 1® report. When it does not cover a substantial portion of your entity's fiscal period, identify or implement controls that will provide a basis for controls reliance for the entire fiscal period — or work with the service organization to have additional procedures performed that are audited.
- *Don't just focus on the opinion of the service organization's auditor (called the "service auditor")* — Obtain the current-period SOC 1® report as soon as it is available, and read it to determine:
  - Whether the controls identified address the risks related to the processing performed that are relevant to your entity
  - How the service organization has addressed any deficiencies in the controls that are relevant to your entity
- *Be aware that information in Section V of the SOC 1® report is unaudited* — This section of the report alone is insufficient evidence of remediation or other actions. Either identify entity controls that address the risks related to the deficiencies or talk with the service organization about additional procedures it can perform, which need to be audited.
- *Pay attention to relevant subservice organizations* (i.e., those engaged by the service organization to perform part of the services to be provided by the service organization) — Obtain and evaluate SOC 1® reports for these entities.

Section 1: Use of service organizations

Section 1:
Use of service organizations

Outsourced activities that can be relevant to an entity's ICFR may range from the full outsourcing of a business process, such as payroll or invoice processing, to the use of IT applications, operating systems and IT environment provided by a service organization (e.g., the use of cloud service provider). Typically, when an entity outsources a business process, it is also outsourcing the IT environment.

> "Outsourced Service Providers: Many organizations outsource business functions, delegating their roles and responsibilities for day-to-day management to outside service providers .... While these external parties execute activities for or on behalf of the organization, management cannot abdicate its responsibility to manage the associated risks. It must implement a program to evaluate those activities performed by others on their behalf to assess the effectiveness of the system of internal control over the activities performed by outsourced service providers.
>
> COSO 2013 Framework - Appendices

When the service organization activities are important to an entity's ICFR, including when data and reports are provided by the service organization, it is important to understand the service organization's processes, risks and controls and for those controls to be audited.

> "Users of outsourced services (often referred to as "user organizations") should understand and prioritize the risks associated with those services. User organizations should also understand how the service provider's internal control system manages or mitigates meaningful risks and obtain at least periodic information about the operation of those controls.
>
> COSO Guidance on Monitoring Internal Control Systems, Volume II: Application

When the service organization uses other organizations to provide the some of the services it has been contracted to provide (called "subservice organizations"), the entity's control environment extends to the subservice organizations.

Section 2: Working with a service organization

Section 2:

Working with a service organization

An effective working relationship with a service organization starts with contracting and making sure the entity has a right to audit and/or has input into the next SOC 1® report the service organization will issue. Entities should make sure relevant control objectives are included in the SOC 1® report, such as one that addresses the completeness and accuracy of reports produced by the service organization and used by the entity or one related to key automated functions. Entities may also want language that specifies the qualifications of the service auditor. Entities may ask for the most recently issued SOC 1® report to determine changes to be requested. Other examples of matters the contract should cover include:

- Service organization responsibility for communicating to the entity issues with controls throughout the year
- Coverage period of the SOC 1® report
- Timely release of the SOC 1® report by the service organization and any subservice organizations it has contracted with
- Service organization responsibility for obtaining subservice organization SOC 1® reports and providing them to their auditors
- Service organization responsibility for addressing control deficiencies timely
- Procedures to be performed for all or a part of a period when controls are determined not to be functioning, including obtaining the service auditor's opinion over those procedures

The entity should have a relationship with appropriate individuals at the service organization who can provide information year-round about events at the service organization, such as process changes, system changes and control concerns at the service organization.

> "User organizations may also find other useful sources of information about the design and operation of service organization controls such as through frequent interaction with the service provider, user group forums, and reports by internal auditors or regulatory authorities.
>
> COSO Guidance on Monitoring Internal Control Systems, Volume II: Application

The entity should also create in-house monitoring processes over the services provided by the service organization, such as periodic discussions with the users who provide input to, and receive output from, the service organization to identify possible issues at the service organization. Monitoring and participating in user forums can also provide helpful information and indications of issues.

Section 3: Using a SOC 1® report

Section 3:
Using a SOC 1® report

The entity should understand how the service organization activities fit with those at the entity. Are the activities part of processing a significant class of transactions, or are they solely IT-related? What are the entity's responsibilities with respect to the service organization's processes? Examples of these responsibilities are providing input to the service organization's processes, verifying the reasonableness of output from the service organization, configuring an IT application to operate as the entity wants it to and managing user access processes.

> "Management obtains an understanding of the service organization's activities and whether those activities impact significant classes of transactions, accounts, or disclosures in the company's reporting process. In determining the significance of the service organization's processes to the financial statements ....
>
> If management determines that the service organization's processes are significant to internal control over external financial reporting, then it:
>
> - Identifies the specific control activities performed by the service organization that are relevant to financial statement assertions, and/or
> - Selects and develops control activities internally over the activities performed by the service organization.
>
> COSO 2013 Framework – Internal control over external financial reporting: A compendium of approaches and examples – Control activities

An entity typically obtains information about the processes and controls at a service organization through reports on the service organization's controls. In the US, these reports, which are titled *Reports on controls relevant to user entity's internal control over financial reporting (SOC 1®)*, are prepared by service organizations with independent auditor attestation over the adequacy of the description and design of the controls (Type 1[1] reports). Additional attestation over the operating effectiveness of the controls is included in Type 2 reports. Similar reports are issued under International Standards on Assurance Engagements (ISAE 3402) or individual country standards.

[1] Type 1 SOC 1® reports are as of a point in time and do not include an assertion by management or an opinion by the service auditor about the operating effectiveness of controls. Type 1 reports are of limited usefulness to an entity's evaluation of its ICFR.

The integrated processes of the entity and service organization, along with the risks, need to be documented. Risks identified for these processes can be addressed either by controls at the entity or at the service organization.

Controls at the entity can be identified and evidence gathered to support operating effectiveness during the period and ready to be matched to CUECs included in the current-period SOC 1® report when it is received. Processes and controls at the service organization can be identified through review of the prior-period SOC 1® report and periodic dialogue with individuals at the service organization.

The service organization's processes typically do not change significantly from period to period, which means the risks and controls also generally remain consistent. The entity's documentation of the service organization's processes can be verified and refreshed upon receipt of the current-period SOC 1® report. Understanding and documenting the service organization's processes during the early part of the fiscal period also helps to make sure there will be no gap in controls, and issues with the operation of the entity's controls are determined with sufficient time to remediate them.

Reviewing the prior-period SOC 1® report also permits the entity to make sure the control objectives, controls and testing that are likely to appear in the current-period report will be appropriate for the entity's needs. For example, verifying the inclusion and testing of specific key controls, as well as controls over the completeness and accuracy of data and reports provided by the service organization to the entity, provides time for the service organization to implement missing controls and for the service auditor to complete testing before the current-period SOC 1® report is issued and any lack of sufficient information in the SOC 1® report becomes more difficult to resolve.

A good way for the service organization to address the completeness and accuracy of the data and reports provided to the entities is through a separate control objective and controls that clearly address completeness and accuracy of the data and reports. These controls should be tested by the service auditor. If not, the entity needs to identify or implement controls that address the completeness and accuracy of the data and reports.

Because of the timing of the issuance of SOC 1® reports, it is critical that entities do not wait to perform procedures related to the service organization until the current-period SOC 1® report is received. Periodic contact with individuals at the service organization who can provide insights as to events at the service organization that may, or are, affecting the effective operation of controls is critical. When controls at the service organization do not operate as designed, the issue can affect the internal controls of the entity as well as the reliability of the services provided by the service organization.

Section 4: SOC 1® reports explained

Section 4:

SOC 1® reports explained

Type 2 SOC 1® reports typically have the following sections and information.

Section I: Independent service auditor's report – This section provides, among other things, the service auditor's opinion about whether for the stated period:

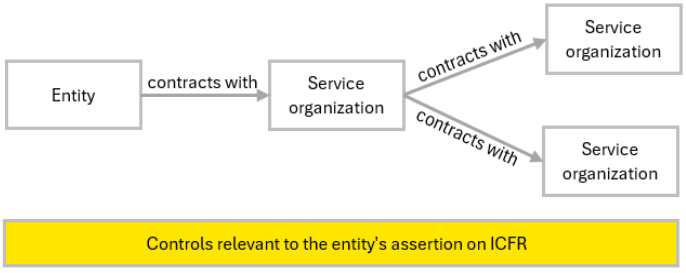
01 Management's description of the service organization's system is fairly presented

02 The controls related to the control objectives were suitably designed

03 The controls related to the control objectives stated in management's description of the service organization's system operated effectively

This section also indicates whether CUECs, in general, need to be in place at user entities for the service organization controls to operate effectively. For example, a service organization's determination of payroll expense for an entity depends on the accuracy of the information about the employees provided by the entity. The service organization report will include a CUEC, such as "The user entity is expected to have controls over the completeness and accuracy of the data provided to the service organization." The specific CUECs are typically listed in Section III of the SOC 1® report.

This section of the SOC 1® report also states whether the service organization uses subservice organizations. (Refer to *Section 6: Other matters* for more information.)



Section II: Management of the service organization's assertion — This section describes, among other items, management's:

- Responsibility for preparing the description of the services provided for the indicated period
- The use of subservice organizations and how the relevant processes and controls at those organizations are addressed in the report
- The expectation of CUECs at user entities
- Confirmation of the adequacy of the description based on the stated criteria, the suitable design of the controls to meet the control objectives and the operating effectiveness of those controls

The service auditor's opinion and management's assertion should be consistent.

Section III: Management of the service organization's description of its system of internal control relevant to user entities' internal control over financial reporting — This section provides general information about the entity's control environment, risk assessment process and monitoring activities as well as a description of its IT systems, processes and control activities used to perform the services. The information included in this section is subject to audit.

Section IV: Management of the service organization's description of its control objectives and related controls and the independent service auditor's description of tests of controls and results — This section provides management's control objectives and controls that address the risks of performing the processes described in Section III as well as a description of the tests of the controls that were performed by the service auditor and the results of those tests.

Section V: Other information provided by management of the service organization — This optional section provides other information that management of the service organization chooses to communicate to user entities, such as backup and recovery activities, responses to control deviations disclosed in the report, and system conversions. The information included in this section is not subject to audit, so it does not provide audited evidence that stated procedures were performed or that controls were remediated.

Reports on service organization controls are typically issued every year for a 12-month period ended between 30 September and 31 October. However, reports for other periods and period ends are also issued. The timing is designed to provide assurance on the service organization's processes and controls for a period covering as much of the reporting period for a typical calendar period-end entity as possible and still issue the report with sufficient time for the entity to evaluate the information in the report before its filing deadlines with regulators, such as the SEC. However, this timing can create challenges if the report discloses issues with the design or operating effectiveness of the service organization's controls that the user entity did not expect. This possibility makes ongoing communication with the service organization important. The typical timing can also create issues of insufficient coverage of the fiscal period when the entity's fiscal year-end doesn't align with the period covered by the SOC 1® report. (Refer to *Section 6: Other matters* for more information.)

Section 5: Addressing issues disclosed in SOC 1® reports

Section 5:

Addressing issues disclosed in SOC 1® reports

Controls at a service organization stand in for controls at the entity. Any issues with a service organization's controls require the user entity to analyze and conclude on their effect on the entity. Control deficiencies at a service organization require the same attention as those identified at the entity for its Section 404 certification and the auditor's report on ICFR.

Issues identified in Type 2 SOC 1® reports appear in one of the following places:

Section I: Independent service auditor's report/Section II: Management of the service organization's assertion — Issues reported in these sections relate to inadequacies in management's description and in the design or operating effectiveness of controls to the extent that, based on materiality of the service organization, the control objectives are not achieved. Information about issues with the description or controls should be included in both management's assertion and the service auditor's opinion. These sections are the only places materially inadequate descriptions or control design deficiencies are reported.

Section IV: Management of the service organization's description of its control objectives and related controls and the independent service auditor's description of tests of controls and results — All testing exceptions (also called deviations) identified by the service auditor are reported here regardless of the service auditor's opinion on whether the controls that are operating effectively meet the control objectives. The service auditor reports all deviations because it cannot determine whether a deviation has significance to a particular user entity. Therefore, the service auditor's description of tests of controls and results includes all deviations, even if the service auditor concludes the related control objective was achieved in the context of the service organization's materiality (i.e., the service auditor's report is unqualified). The entity must evaluate all deviations for their relevance and significance to the entity's ICFR regardless of the service auditor's overall opinion.

The most effective way to address control deviations is for the service organization to remediate them and perform appropriate procedures to address the risk for the period of the control failure. The service auditor should test the remediation and additional procedures and include them in the scope of its auditor's report. Management's unaudited procedures appear in Section V of the SOC 1® report. Because the procedures are unaudited, they do not provide sufficient evidence to permit the entity and its external auditors to evaluate whether the risk has been sufficiently addressed for the period and as of period end.

In these situations, the entity should consider whether they have a basis for the amounts reflected in the financial statements. That basis could be a combination of evidence about the operating effectiveness of service organization controls, entity controls and careful consideration of compensating controls.

Section 6: Other matters

Section 6:
Other matters

SOC 1® reports not "in sync" with the entity's fiscal period

If the entity's fiscal period differs from the period covered by the SOC 1® report by more than three months (assuming a 12-month Type 2 SOC 1® report), the SOC 1® report will likely not provide sufficient evidence of the design and operating effectiveness of the controls at the service organization for the full period. In this case, the entity should make arrangements with the service organization to have its needs met. These arrangements can include:

- The entity's internal auditors visiting the service organization and performing the procedures necessary to obtain the information they need about the entity's processes and risks, and the design and operating effectiveness of the controls that address those risks.
- The service auditor providing a special purpose attestation report about the continuing effectiveness of specific controls of relevance to the entity that updates the SOC 1® report issued by the service organization.
- The entity developing its own controls to address the risks of the entity using the processes at the service organization. This approach may be challenging if the service organization is providing significant IT services because the entity will not likely have visibility into the service organization's control operations.

Some service organizations have accommodated the various fiscal period ends of its user entities by providing rolling six-month reports to cover a 12-month period. The results for the oldest six months drop off, and information and testing for the newest six months are added.

Representations by the management of the service organization about whether the controls described in the SOC 1® report continue to function for a specified period from the end date of the SOC 1® report (often referred to as bridge letters), are typically adequate evidence to cover a three-month period from the end of the SOC 1® report coverage period to the entity's fiscal year end, provided the entity has no evidence that is contrary to the statements made in the bridge letter. Changes in the service organization's controls reported in a bridge letter that are relevant to the entity should be discussed with the service organization and the entity should perform appropriate actions, which may include the testing of new controls by the service auditor.

How an "out-of-sync" SOC 1® report will be handled is best addressed at the time of contracting with the service organization.

Subservice organizations

A service organization may outsource some of the services it provides to an entity to another entity, called a subservice organization. (Refer to the diagram in *Section 4: SOC 1® reports explained*.) The controls at the subservice organization are part of the entity's control environment, similar to those of the service organization. The processes and controls at a subservice organization can be handled in one of two ways: (1) they are included in the service organization's SOC 1® report (called the inclusive method), or (2) the subservice organization issues its own SOC 1® report (called the carve-out method).

Regardless of the method used, the entity must understand the relevant business and IT processes provided by the service organization and related subservice organizations. When the use of a subservice organization is handled by applying the carve-out method, the CUECs (i.e., the controls that the subservice organization needs the service organization to have implemented to permit the subservice organization's controls to operate effectively) should be mapped to the service organization's SOC 1® report.

Section 7: Best practices for working with service organizations to obtain timely process and control information

Section 7:

Best practices for working with service organizations to obtain timely process and control information

☐	Include in the contract with the service organization the right to audit or to influence the content of SOC 1® reports issued by service organization. Also include the service organization's responsibility for obtaining and providing to your entity and your external auditor the SOC 1® reports of subservice organizations hired by the service organization. In addition, include provisions for the procedures to address control issues and who will pay for supplemental procedures that may need to be performed at the service organization.
☐	Establish and maintain a year-round relationship with the service organization. Inquire periodically about whether there are any issues with relevant operations or controls. Be aware of the scheduled SOC 1® report issuance date and monitor it for unexpected delays. Understand the causes of those delays, which may signal one or more issues that will be reported in the SOC 1® report.
☐	Periodically check in with key users at your entity to identify concerns about working with the service organization or the output coming from it.
☐	Document an integrated understanding of the entity's processes and the service organization's transaction and supporting IT processes, as applicable. **Don't wait for the current period SOC 1® report to document this understanding.** Use the prior period SOC 1® report to establish the baseline understanding of the processes and controls and validate it to the current period SOC 1® report when received. Along with the description, the CUECs provide information about processes to be performed by your entity.
☐	Verify that the activities performed by your entity related to the service organization's activities are subject to appropriately designed controls for which evidence of operating effectiveness has been gathered. Some of these controls should map to CUECs defined in the SOC 1® report (an example of such activities is maintaining appropriate access of the entity's users to the service organization's IT systems). Verifying that your entity has appropriate controls to address the CUECs using the prior-period SOC 1® report saves time when the current-period report is received, because your entity and external auditor are prepared.
☐	Use the prior-period SOC 1® report to identify any inadequately described controls or tests of those controls, deviations and the service auditor procedures to audit remediation or other procedures performed by your entity to address the deviations. Work with your external auditor, the service organization and the service auditor to set appropriate current-period expectations for the information to be provided about control deviations and additional procedures to be performed by the service organization and the service auditor if needed.
☐	Make a list of data and reports obtained from the service organization. Using the prior-period SOC 1® report, determine whether it includes service auditor testing of the service organization activities that address completeness and accuracy of these reports. Request the service organization to perform additional procedures and have the service auditor include them in their testing. If agreement cannot be reached, identify or implement additional entity controls to address the completeness and accuracy of the reports.

☐	Obtain and evaluate the current-period SOC 1® report on a timely basis as well as the SOC 1® reports of the subservice organizations. **Don't just read the opinion**, which is based on the service organization's business, not your entity's business. Reviewing, evaluating and addressing the effect of testing deviations is critical. Discuss with the external auditors the implications of testing deviations included in the SOC 1® report and the actions needed to address their effect on your entity's assertion about ICFR (if any), the financial statements, the financial statement audit and the external auditor's opinion on ICFR. Facilitate discussions with the service organization and the service auditor as needed. **Remember:** Procedures performed by the service organization but not subject to audit do not provide sufficient evidence that the risk has been addressed.
☐	Map the CUECs to your entity's controls.
☐	If subservice organizations are used by the service organization for services relevant to your entity, facilitate obtaining the SOC 1® reports issued by the subservice organizations and provide them to the external auditors. ▸ Map the CUECs in the subservice organization's SOC 1® reports to the controls in the service organization's SOC 1® report. ▸ Map the complementary subservice organization controls in the service organization's SOC 1® report to the subservice organization's controls. ▸ Evaluate and address opinion qualifications and testing deviations in subservice organization SOC 1® reports. Facilitate discussions with the service organization, subservice organization and the service auditors as needed.
☐	Consider the period covered by the SOC 1® report compared to your entity's reporting period, and determine any additional procedures needed. A typical procedure for period differences up to three months is to obtain a bridge letter from service organization management and, when applicable, from subservice organization management. In addition, consider any contrary evidence obtained from day-to-day interactions with the service organization.

Appendix: US attestation reports available related to service organizations

Appendix:

US attestation reports available related to service organizations

SOC 1® reports are attestation reports related to controls, including IT general controls, at service organizations relevant to user entities' ICFR. They are prepared in accordance with American Institute of Certified Public Accountants (AICPA) AT-C section 320 and the AICPA Guide, *Service organizations — Reporting on an examination of controls at a service organization relevant to user entities' internal control over financial reporting*. These reports are designed to meet the needs of entities and their external auditors when performing risk assessment procedures and making assertions or providing opinions about ICFR to regulators and others.

SOC 2® reports are attestation reports related to controls at a service organization relevant to security, availability, processing integrity, confidentiality and/or privacy. They are prepared in accordance with AICPA AT-C Section 205, *Assertion-Based Examination Engagements*, and the AICPA Guide, *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy.* These reports include the description of the service organization's system and related controls. They are not designed to be used by entities or their external auditors when making assertions, or providing opinions, about ICFR to regulators and others because SOC 2® reports only pertain to certain aspects of the IT environment.

SOC 3® reports are attestation reports relevant to a service organization's security, availability, processing integrity, confidentiality and/or privacy. They are prepared in accordance with AICPA AT-C Section 205, *Assertion-Based Examination Engagements*. The reports contain management's description of the boundaries of the service organization's system and a copy of the service organization's privacy notice (when applicable), along with a written assertion by the management of the service organization about whether the organization maintained effective controls over the system as it relates to the principle(s) being reported on (i.e., security, availability, processing integrity, confidentiality and/or privacy), based on the applicable trust services criteria. The report also contains a service auditor's report that expresses an opinion on whether the service organization maintained effective controls as it relates to the principle(s) being reported on. No detailed information is provided about either the service organization's processes or controls, so the report is not suitable for use by entities or their external auditors when making assertions or providing opinions about ICFR to regulators or others.

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

SCORE no. 25079-241US

2409-10763-CS
ED None

ey.com