KAEG-I [INTL VERSION 2024]: ISA 402 Audit Considerations Relating to an Entity Using a Service Organization

Contents

KAEG-I [INTL VERSION]: ISA 402 Audit Considerations Relating to an Entity Using a Service Organization [ISA | KAEGISA402]

International Standards on Auditing: ISA 402.15-17

ISA Application and Other Explanatory Material: ISA 402.A24-A39

How do we comply with the standards?

1 Understand the service organization's activities and internal controls

2 Test the operating effectiveness of controls

2.1 Obtain evidence through one or more acceptable approaches

2.2 Consider the extent of evidence provided by the Type 2 SOC 1 report

2.3 Determine whether tests of controls are relevant and sufficient

2.3.1 Determine whether controls and results are relevant to significant assertions

2.3.1.1 Consider whether the nature and extent of relevant tests of controls provide sufficient appropriate evidence

2.3.1.2 Consider whether the timing of relevant tests of controls provides sufficient appropriate audit evidence

2.3.2 Consider whether the results of relevant tests of controls provide sufficient appropriate evidence

2.3.3 Evaluate the impact of relevant control deficiencies and any modified opinion

3 Perform communications if we identify significant deficiencies

Type 1 and Type 2 Reports That Exclude the Services of a Subservice Organization

International Standards on Auditing: ISA 402.18

ISA Application and Other Explanatory Material: ISA 402.A40

How do we comply with the standards?

1 Understand how the user entity uses service and subservice organizations

Fraud, Non-Compliance with Laws and Regulations, and Uncorrected Misstatements in Relation to Activities at a Service Organization

International Standards on Auditing: ISA 402.19

ISA Application and Other Explanatory Material: ISA 402.A41

How do we comply with the standards?

1 Inquire about items that could impact the financial statements

Reporting by the User Auditor

International Standards on Auditing: ISA 402.20-22

ISA Application and Other Explanatory Material: ISA 402.A42-A44

How do we comply with the standards?

1 Do not refer to the service auditor's report in our audit opinion

2 Determine whether we sufficiently understand how the entity uses the service organization

ISA 402 Audit Considerations Relating to an Entity Using a Service Organization

View the Full Chapter for this Standard

ISA 402 *Audit Considerations Relating to an Entity Using a Service Organization*

(Effective for audits of financial statements for periods beginning on or after December 15, 2009)

Introduction, Objectives and Definitions

International Standards on Auditing: ISA 402.01-08

Introduction

Scope of this ISA

1. This International Standard on Auditing (ISA) deals with the user auditor's responsibility to obtain sufficient appropriate audit evidence when a user entity uses the services of one or more service organizations. Specifically, it expands on how the user auditor applies ISA 315 (Revised 2019)[1] and ISA 330[2] in obtaining an understanding of the user entity, including the entity's system of internal control relevant to the preparation of the financial statements, sufficient to identify and assess the risks of material misstatement and in designing and performing further audit procedures responsive to those risks.

_____

1 ISA 315 (Revised 2019), *Identifying and Assessing the Risks of Material Misstatement*

2 ISA 330, *The Auditor's Responses to Assessed Risks*

2. Many entities outsource aspects of their business to organizations that provide services ranging from performing a specific task under the direction of an entity to replacing an entity's entire business units or functions, such as the tax compliance function. Many of the services provided by such organizations are integral to the entity's business operations; however, not all those services are relevant to the audit.

3. Services provided by a service organization are relevant to the audit of a user entity's financial statements when those services, and the controls over them, are part of the user entity's information system, relevant to the preparation of the financial statements. Most controls at the service organization are likely to be part of the user entity's information system relevant to the preparation of the financial statements, or related controls, such as controls over the safeguarding of assets. A service organization's services are part of a user entity's information system, if these services affect any of the following:

> (a) How information relating to significant classes of transactions, account balances and disclosures flows through the user entity's information system, whether manually or using IT, and whether obtained from within or outside the general ledger and subsidiary ledgers. This includes when the service organization's services affect how:

(i) Transactions of the user entity are initiated, and how information about them is recorded, processed, corrected as necessary, and incorporated in the general ledger and reported in the financial statements; and

(ii) Information about events or conditions, other than transactions, is captured, processed and disclosed by the user entity in the financial statements.

(b) The accounting records, specific accounts in the user entity's financial statements and other supporting records relating to the flows of information in paragraph 3(a);

(c) The financial reporting process used to prepare the user entity's financial statements from the records described in paragraph 3(b), including as it relates to disclosures and to accounting estimates relating to significant classes of transactions, account balances and disclosures; and

(d) The entity's IT environment relevant to (a) to (c) above.

4. The nature and extent of work to be performed by the user auditor regarding the services provided by a service organization depend on the nature and significance of those services to the user entity and the relevance of those services to the audit.

5. This ISA does not apply to services provided by financial institutions that are limited to processing, for an entity's account held at the financial institution, transactions that are specifically authorized by the entity, such as the processing of checking account transactions by a bank or the processing of securities transactions by a broker. In addition, this ISA does not apply to the audit of transactions arising from proprietary financial interests in other entities, such as partnerships, corporations and joint ventures, when proprietary interests are accounted for and reported to interest holders.

Effective Date

6. This ISA is effective for audits of financial statements for periods beginning on or after December 15, 2009.

Objectives

7. The objectives of the user auditor, when the user entity uses the services of a service organization, are:

(a) To obtain an understanding of the nature and significance of the services provided by the service organization and their effect on the user entity's system of internal control, sufficient to provide an appropriate basis for the identification and assessment of the risks of material misstatement; and

(b) To design and perform audit procedures responsive to those risks.

Definitions

8. For purposes of the ISAs, the following terms have the meanings attributed below:

(a) Complementary user entity controls - Controls that the service organization assumes, in the design of its service, will be implemented by user entities, and which, if necessary to achieve control objectives, are identified in the description of its system.

(b) Report on the description and design of controls at a service organization (referred to in this ISA as a type 1 report) - A report that comprises:

(i) A description, prepared by management of the service organization, of the service organization's system, control objectives and related controls that have been designed and implemented as at a specified date; and

(ii) A report by the service auditor with the objective of conveying reasonable assurance that includes the service auditor's opinion on the description of the service organization's system, control objectives and related controls and the suitability of the design of the controls to achieve the specified control objectives.

(c) Report on the description, design, and operating effectiveness of controls at a service organization (referred to in this ISA as a type 2 report) - A report that comprises:

(i) A description, prepared by management of the service organization, of the service organization's system, control objectives and related controls, their design and implementation as at a specified date or throughout a specified period and, in some cases, their operating effectiveness throughout a specified period; and

(ii) A report by the service auditor with the objective of conveying reasonable assurance that includes:

a. The service auditor's opinion on the description of the service organization's system, control objectives and related controls, the suitability of the design of the controls to achieve the specified control objectives, and the operating effectiveness of the controls; and

b. A description of the service auditor's tests of the controls and the results thereof.

(d) Service auditor - An auditor who, at the request of the service organization, provides an assurance report on the controls of a service organization.

(e) Service organization - A third-party organization (or segment of a third-party organization) that provides services to user entities that are part of those entities' information systems relevant to financial reporting.

(f) Service organization's system - The policies and procedures designed, implemented and maintained by the service organization to provide user entities with the services covered by the service auditor's report.

(g) Subservice organization - A service organization used by another service organization to perform some of the services provided to user entities that are part of those user entities' information systems relevant to financial reporting.

(h) User auditor - An auditor who audits and reports on the financial statements of a user entity.

(i) User entity - An entity that uses a service organization and whose financial statements are being audited.

Obtain an Understanding of the Services Provided by a Service Organization, Including Internal Control

International Standards on Auditing: ISA 402.09-14 Requirements

Obtaining an Understanding of the Services Provided by a Service Organization, Including Internal Control

9. When obtaining an understanding of the user entity in accordance with ISA 315 (Revised),[3] the user auditor shall obtain an understanding of how a user entity uses the services of a service organization in the user entity's operations, including: (Ref: Para. A1-A2)

(a) The nature of the services provided by the service organization and the significance of those services to the user entity, including the effect thereof on the user entity's internal control; (Ref: Para. A3-A5)

(b) The nature and materiality of the transactions processed or accounts or financial reporting processes affected by the service organization; (Ref: Para. A6)

(c) The degree of interaction between the activities of the service organization and those of the user entity; and (Ref: Para. A7)

(d) The nature of the relationship between the user entity and the service organization, including the relevant contractual terms for the activities undertaken by the service organization. (Ref: Para. A8-A11)

---

3 ISA 315 (Revised), paragraph 11

10. When obtaining an understanding of the entity's system of internal control in accordance with ISA 315 (Revised 2019), the user auditor shall identify controls in the control activities component[103] at the user entity from those that relate to the services provided by the service organization, including those that are applied to the transactions processed by the service organization, and evaluate their design and determine whether they have been implemented.[104] (Ref: Para. A12-A14)

---

103 ISA 315 (Revised 2019), paragraphs 26(a)

104 ISA 315 (Revised 2019), paragraph 26(d)

11. The user auditor shall determine whether a sufficient understanding of the nature and significance of the services provided by the service organization and their effect on the user entity's system of internal control has been obtained to provide an appropriate basis for the identification and assessment of the risks of material misstatement.

12. If the user auditor is unable to obtain a sufficient understanding from the user entity, the user auditor shall obtain that understanding from one or more of the following procedures:

(a) Obtaining a type 1 or type 2 report, if available;

(b) Contacting the service organization, through the user entity, to obtain specific information;

(c) Visiting the service organization and performing procedures that will provide the necessary information about the relevant controls at the service organization; or

(d) Using another auditor to perform procedures that will provide the necessary information about controls at the service organization. (Ref: Para. A15-A20)

Using a Type 1 or Type 2 Report to Support the User Auditor's Understanding of the Service Organization

13. In determining the sufficiency and appropriateness of the audit evidence provided by a type 1 or type 2 report, the user auditor shall be satisfied as to:

(a) The service auditor's professional competence and independence from the service organization; and

(b) The adequacy of the standards under which the type 1 or type 2 report was issued. (Ref: Para. A21)

14. If the user auditor plans to use a type 1 or type 2 report as audit evidence to support the user auditor's understanding about the design and implementation of controls at the service organization, the user auditor shall:

(a) Evaluate whether the description and design of controls at the service organization is at a date or for a period that is appropriate for the user auditor's purposes;

(b) Evaluate the sufficiency and appropriateness of the evidence provided by the report for the understanding of the controls at the service organization; and

(c) Determine whether complementary user entity controls identified by the service organization are relevant to the user entity and, if so, obtain an understanding of whether the user entity has designed and implemented such controls. (Ref: Para. A22-A23)

ISA Application and Other Explanatory Material: ISA 402.A1-A23

Application and Other Explanatory Material

Obtaining an Understanding of the Services Provided by a Service Organization, Including Internal Control

Sources of Information (Ref: Para. 9)

A1. Information on the nature of the services provided by a service organization may be available from a wide variety of sources, such as:

- User manuals.
- System overviews.
- Technical manuals.
- The contract or service level agreement between the user entity and the service organization.
- Reports by service organizations, the internal audit function or regulatory authorities on controls at the service organization.
- Reports by the service auditor, including management letters, if available.

A2. Knowledge obtained through the user auditor's experience with the service organization, for example, through experience with other audit engagements, may also be helpful in obtaining an understanding of the nature of the services provided by the service organization. This may be particularly helpful if the services and controls at the service organization over those services are highly standardized.

Nature of the Services Provided by the Service Organization (Ref: Para. 9(a))

A3. A user entity may use a service organization such as one that processes transactions and maintains related accountability, or records transactions and processes related data. Service organizations that provide such services include, for example, bank trust departments that invest and service assets for employee benefit plans or for others; mortgage bankers that service mortgages for others; and application service providers that provide packaged software applications and a technology environment that enables customers to process financial and operational transactions.

A4. Examples of service organization services that are relevant to the audit include:

- Maintenance of the user entity's accounting records.
- Management of assets.
- Initiating, recording or processing transactions as agent of the user entity.

Considerations Specific to Smaller Entities

A5. Smaller entities may use external bookkeeping services ranging from the processing of certain transactions (for example, payment of payroll taxes) and maintenance of their accounting records to the preparation of their financial statements. The use of such a service organization for the preparation of its financial statements does not relieve management of the smaller entity and, where appropriate, those charged with governance of their responsibilities for the financial statements.[6]

_____

6 ISA 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing,* paragraphs 4 and A4 - A5

Nature and Materiality of Transactions Processed by the Service Organization (Ref: Para. 9(b))

A6. A service organization may establish policies and procedures that affect the user entity's internal control. These policies and procedures are at least in part physically and operationally separate from the user entity. The significance of the controls of the service organization to those of the user entity depends on the nature of the services provided by the service organization, including the nature and materiality of the transactions it processes for the user entity. In certain situations, the transactions processed and the accounts affected by the service organization may not appear to be material to the user entity's financial statements, but the nature of the transactions processed may be significant and the user auditor may determine that an understanding of those controls is necessary in the circumstances.

The Degree of Interaction between the Activities of the Service Organization and the User Entity (Ref: Para. 9(c))

A7. The significance of the controls of the service organization to those of the user entity also depends on the degree of interaction between its activities and those of the user entity. The degree of interaction

refers to the extent to which a user entity is able to and elects to implement effective controls over the processing performed by the service organization. For example, a high degree of interaction exists between the activities of the user entity and those at the service organization when the user entity authorizes transactions and the service organization processes and does the accounting for those transactions. In these circumstances, it may be practicable for the user entity to implement effective controls over those transactions. On the other hand, when the service organization initiates or initially records, processes, and does the accounting for the user entity's transactions, there is a lower degree of interaction between the two organizations. In these circumstances, the user entity may be unable to, or may elect not to, implement effective controls over these transactions at the user entity and may rely on controls at the service organization.

Nature of the Relationship between the User Entity and the Service Organization (Ref: Para. 9(d))

A8. The contract or service level agreement between the user entity and the service organization may provide for matters such as:

- The information to be provided to the user entity and responsibilities for initiating transactions relating to the activities undertaken by the service organization;
- The application of requirements of regulatory bodies concerning the form of records to be maintained, or access to them;
- The indemnification, if any, to be provided to the user entity in the event of a performance failure;
- Whether the service organization will provide a report on its controls and, if so, whether such report would be a type 1 or type 2 report;
- Whether the user auditor has rights of access to the accounting records of the user entity maintained by the service organization and other information necessary for the conduct of the audit; and
- Whether the agreement allows for direct communication between the user auditor and the service auditor.

A9. There is a direct relationship between the service organization and the user entity and between the service organization and the service auditor. These relationships do not necessarily create a direct relationship between the user auditor and the service auditor. When there is no direct relationship between the user auditor and the service auditor, communications between the user auditor and the service auditor are usually conducted through the user entity and the service organization. A direct relationship may also be created between a user auditor and a service auditor, taking into account the relevant ethical and confidentiality considerations. A user auditor, for example, may use a service auditor to perform procedures on the user auditor's behalf, such as:

(a) Tests of controls at the service organization; or

(b) Substantive procedures on the user entity's financial statement transactions and balances maintained by a service organization.

Considerations Specific to Public Sector Entities

A10. Public sector auditors generally have broad rights of access established by legislation. However, there may be situations where such rights of access are not available, for example, when the service organization is located in a different jurisdiction. In such cases, a public sector auditor may need to obtain an understanding of the legislation applicable in the different jurisdiction to determine whether

appropriate access rights can be obtained. A public sector auditor may also obtain or ask the user entity to incorporate rights of access in any contractual arrangements between the user entity and the service organization.

A11. Public sector auditors may also use another auditor to perform tests of controls or substantive procedures in relation to compliance with law, regulation or other authority.

Understanding the Controls Relating to Services Provided by the Service Organization (Ref: Para. 10)

A12. The user entity may establish controls over the service organization's services that may be tested by the user auditor and that may enable the user auditor to conclude that the user entity's controls are operating effectively for some or all of the related assertions, regardless of the controls in place at the service organization. If a user entity, for example, uses a service organization to process its payroll transactions, the user entity may establish controls over the submission and receipt of payroll information that could prevent or detect material misstatements. These controls may include:

- Comparing the data submitted to the service organization with reports of information received from the service organization after the data has been processed.
- Recomputing a sample of the payroll amounts for clerical accuracy and reviewing the total amount of the payroll for reasonableness.

A13. In this situation, the user auditor may perform tests of the user entity's controls over payroll processing that would provide a basis for the user auditor to conclude that the user entity's controls are operating effectively for the assertions related to payroll transactions.

A14. As noted in ISA 315 (Revised),[7] in respect of some risks, the user auditor may judge that it is not possible or practicable to obtain sufficient appropriate audit evidence only from substantive procedures. Such risks may relate to the inaccurate or incomplete recording of routine and significant classes of transactions and account balances, the characteristics of which often permit highly automated processing with little or no manual intervention. Such automated processing characteristics may be particularly present when the user entity uses service organizations. In such cases, the user entity's controls over such risks are relevant to the audit and the user auditor is required to obtain an understanding of, and to evaluate, such controls in accordance with paragraphs 9 and 10 of this ISA.

_____

7 ISA 315 (Revised), paragraph 30

Further Procedures When a Sufficient Understanding Cannot Be Obtained from the User Entity (Ref: Para. 12)

A15. The user auditor's decision as to which procedure, individually or in combination, in paragraph 12 to undertake, in order to obtain the information necessary to provide a basis for the identification and assessment of the risks of material misstatement in relation to the user entity's use of the service organization, may be influenced by such matters as:

- The size of both the user entity and the service organization;
- The complexity of the transactions at the user entity and the complexity of the services provided by the service organization;

- The location of the service organization (for example, the user auditor may decide to use another auditor to perform procedures at the service organization on the user auditor's behalf if the service organization is in a remote location);
- Whether the procedure(s) is expected to effectively provide the user auditor with sufficient appropriate audit evidence; and
- The nature of the relationship between the user entity and the service organization.

A16. A service organization may engage a service auditor to report on the description and design of its controls (type 1 report) or on the description and design of its controls and their operating effectiveness (type 2 report). Type 1 or type 2 reports may be issued under International Standard on Assurance Engagements (ISAE) 3402[8] or under standards established by an authorized or recognized standards setting organization (which may identify them by different names, such as Type A or Type B reports).

_____

8 ISAE 3402, *Assurance Reports on Controls at a Service Organization*

A17. The availability of a type 1 or type 2 report will generally depend on whether the contract between a service organization and a user entity includes the provision of such a report by the service organization. A service organization may also elect, for practical reasons, to make a type 1 or type 2 report available to the user entities. However, in some cases, a type 1 or type 2 report may not be available to user entities.

A18. In some circumstances, a user entity may outsource one or more significant business units or functions, such as its entire tax planning and compliance functions, or finance and accounting or the controllership function to one or more service organizations. As a report on controls at the service organization may not be available in these circumstances, visiting the service organization may be the most effective procedure for the user auditor to gain an understanding of controls at the service organization, as there is likely to be direct interaction of management of the user entity with management at the service organization.

A19. Another auditor may be used to perform procedures that will provide the necessary information about the relevant controls at the service organization related to services provided to the user entity. If a type 1 or type 2 report has been issued, the user auditor may use the service auditor to perform these procedures as the service auditor has an existing relationship with the service organization. The user auditor using the work of another auditor may find the guidance in ISA 220 (Revised)[9] useful as it relates to determining the competence and capabilities of the other auditor (including that auditor's independence), the direction and supervision of the other auditor, the nature, timing and extent of the work assigned to the other auditor, and evaluating the sufficiency and appropriateness of the audit evidence obtained.

_____

9 ISA 220 (Revised), *Quality Management for an Audit of Financial Statements*.

A20. A user entity may use a service organization that in turn uses a subservice organization to provide some of the services provided to a user entity that are part of the user entity's information system relevant to financial reporting. The subservice organization may be a separate entity from the service organization or may be related to the service organization. A user auditor may need to consider controls at the subservice organization. In situations where one or more subservice organizations are used, the interaction between the activities of the user entity and those of the service organization is expanded to include the interaction between the user entity, the service organization and the subservice organizations.

The degree of this interaction, as well as the nature and materiality of the transactions processed by the service organization and the subservice organizations are the most important factors for the user auditor to consider in determining the significance of the service organization's and subservice organization's controls to the user entity's controls.

Using a Type 1 or Type 2 Report to Support the User Auditor's Understanding of the Service Organization (Ref: Para. 13-14)

A21. The user auditor may make inquiries about the service auditor to the service auditor's professional organization or other practitioners and inquire whether the service auditor is subject to regulatory oversight. The service auditor may be practicing in a jurisdiction where different standards are followed in respect of reports on controls at a service organization, and the user auditor may obtain information about the standards used by the service auditor from the standard setting organization.

A22. A type 1 or type 2 report, along with information about the user entity, may assist the user auditor in obtaining an understanding of:

(a) The aspects of controls at the service organization that may affect the processing of the user entity's transactions, including the use of subservice organizations;

(b) The flow of significant transactions through the service organization to determine the points in the transaction flow where material misstatements in the user entity's financial statements could occur;

(c) The control objectives at the service organization that are relevant to the user entity's financial statement assertions; and

(d) Whether controls at the service organization are suitably designed and implemented to prevent, or detect and correct processing errors that could result in material misstatements in the user entity's financial statements.

A type 1 or type 2 report may assist the user auditor in obtaining a sufficient understanding to identify and assess the risks of material misstatement. A type 1 report, however, does not provide any evidence of the operating effectiveness of the controls.

A23. A type 1 or type 2 report that is as of a date or for a period that is outside of the reporting period of a user entity may assist the user auditor in obtaining a preliminary understanding of the controls implemented at the service organization if the report is supplemented by additional current information from other sources. If the service organization's description of controls is as of a date or for a period that precedes the beginning of the period under audit, the user auditor may perform procedures to update the information in a type 1 or type 2 report, such as:

- Discussing the changes at the service organization with user entity personnel who would be in a position to know of such changes;
- Reviewing current documentation and correspondence issued by the service organization; or
- Discussing the changes with service organization personnel.

How do we comply with the Standards?

[ISA | KAEGHDWC]

1 Consider the effect on a user entity's internal controls when a service organization is used [ISA | 3980]

What do we do?

IF a user entity uses a service organization that is part of the user entity's information systems, THEN consider the effect on the user entity's internal controls and the availability of audit evidence.

Why do we do this?

Many entities 'outsource' part of their business processes and internal controls to service organizations. Proper identification of a user entity's use of a service organization helps us understand a user entity's internal controls over financial reporting. We treat the processes and controls performed by service organizations in the same manner as we treat processes and controls performed internally by the user entity'.

Execute the Audit

What do we do as a part of planning and risk assessment related to service organizations? [ISA | 3980.1300]

As part of planning and risk assessment related to service organizations, we:

- Identify the relevant service organizations
- Obtain an understanding of the controls at the service organization that are relevant to the user entity's internal control
- Determine whether we have obtained a sufficient understanding of how the user entity uses the service organization
- Perform certain inquiries
- Determine the adequacy of the standards

1.1 Identify relevant service organizations [ISA | 3981]

What do we do?

Identify the relevant service organizations used by the entity

Why do we do this?

Entities can outsource aspects of their business to organizations that provide services ranging from performing a specific task under the direction of an entity to replacing an entity's entire business unit or function, such as the tax compliance function. Identifying relevant service organizations used by the user entity is a part of understanding an entity's internal control that helps us plan the audit.

Execute the Audit

What is a service organization? [ISA | 3981.13212]

A service organization provides services to a user entity that may become part of that user entity's information systems.

What do we mean by the 'user entity' in relation to service organizations? [ISA | 3981.1300]

The user entity is the entity that has engaged a service organization and whose financial statements are being audited. In our case, the user entity is our audit client and we are known as the user auditor.

What type of services can a service organization provide? [ISA | 3981.1400]

A service organization can provide a number of different types of day to day transactional processing to a user entity, such as payroll processing, cloud computing services, investment management or maintenance of accounting records. In performing these services, the service organization performs activities and related controls that the user entity would normally perform.

Although most controls at the service organization are likely to relate to financial reporting and the account level controls, there may be other controls that may also be relevant to the audit, such as controls over the safeguarding of assets.

For example, an entity may use a service organization to:

- process payroll
- provide inventory storage
- provide shipping services
- perform the tax compliance function
- perform distribution services
- provide valuation over pension plan assets, which the entity uses to determine its unfunded pension liability
- service mortgages

What is a service auditor? [ISA | 3981.13213]

The service auditor is the auditor who reports on controls of a service organization.

Are all service organizations relevant to the user entity's internal control over financial reporting? [ISA | 3981.13214]

No. Not all service organizations or services performed by a service organization are relevant to the user entity's internal control over financial reporting.

For example, an entity might outsource actuarial services; however, in this case, the nature of the actuarial services represents management's use of an expert, and the actuary is not a part of the entity's information system or control environment.

The same may be true of a bank who processes routine transactions (e.g. deposits and withdrawals). In this case, the bank's services are limited to executing an entity's transactions that are specifically initiated and authorized by the entity.

When is a service organization relevant to the entity's internal controls over financial reporting? [ISA | 3981.1500]

A service organization is relevant to the entity's internal controls over financial reporting when those services, and the related controls, are part of the entity's information system, including the IT environment (see activity 'Understand information and communication' for further information on obtaining an understanding of information and communication). This is the case when they affect any of the following:

- The classes of transactions, account balances, and disclosures in the entity's operations that are significant to the entity's financial statements
- The procedures, both automated (within IT) and manual, by which the entity's transactions are initiated, recorded, processed, and reported from their occurrence to their inclusion in the financial statements
- The related accounting records, whether electronic or manual, supporting information, and specific accounts in the entity's financial statements involved in initiating, recording, processing and reporting the entity's transactions
- How the entity's information system captures other events and conditions that are significant to the financial statements
- The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures

Who is responsible for identifying the relevant service organizations? [ISA | 3981.1700]

Since service organizations can be a part of the entity's internal controls over financial reporting, the entity is responsible for identifying all of the service organizations it uses, including subservice organizations, and determining which ones are relevant to the entity's financial reporting. See question 'What is a subservice organization?' for information on the definition of a subservice organization.

Why do we understand the services a service organization provides to the user entity? [ISA | 3981.1800]

Service organizations can offer multiple services; however, the user entity may only use a portion of the services offered by the service organization. As a result, we understand which services are being used by the user entity.

> For example, a user entity contracts with a service organization to provide cloud computing infrastructure services for their payroll application system, but not day to day payroll transaction processing. In that case, the user entity and the engagement team understands the processes and controls related to the cloud computing infrastructure services used by the user entity.

When do we identify the relevant service organizations? [ISA | 3981.1900]

We start identifying service organizations during risk assessment. Early identification allows us to identify specific risks that may impact how we plan and execute our audit. As risk assessment is an iterative process, we remain alert throughout the audit for any new service organizations engaged by the entity.

What if we identify a relevant service organization that management has not identified? [ISA | 3981.2000]

This may be indicative of deficiencies in the entity's internal controls, including those in the CERAMIC components - see question 'What are CERAMIC components?' for information on what CERAMIC components are.

1.2 Obtain an understanding of the controls at the service organization that are relevant to the user entity's internal control [ISA | 3982]

What do we do?

Obtain an understanding of the controls at the service organization that are relevant to the user entity's internal control.

Why do we do this?

Obtaining an understanding of the entity's use of a service organization and subservice organizations allows us to understand how the controls at the service organization are relevant to the user entity's internal control.

Execute the Audit

What do we do to understand how a user entity uses the services of a service organization and test the design of internal controls at the service organization? [ISA | 3982.1300]

To obtain an understanding of how a user entity uses the services of a service organization and evaluate the design and implementation of any relevant controls we:

- Understand how the user entity uses service and subservice organizations
- Understand the service organization's activities and internal controls

1.2.1 Understand how the user entity uses service and subservice organizations [ISA | 3983]

What do we do?

Obtain an understanding of how a user entity uses the services of a service organization, including any subservice organizations

Why do we do this?

Obtaining an understanding over how the entity uses service organizations, including any subservice organizations, allows us to identify key information for risk assessment, including all five components of the entity's internal control.

Service organizations can offer multiple services; however, the user entity may only use a portion of the services offered by the service organization. As a result, we understand which services are being used by the user entity.

Execute the Audit

What do we obtain an understanding over when a user entity uses a service organization? [ISA | 3983.1300]

When a user entity uses a service organization, we obtain an understanding over:

- the nature of the services provided by the service organization and the significance of those services to the user organization, including their effect on the user organization's internal control
- the nature and materiality of the transactions processed or accounts or financial reporting processes affected by the service organization
- the degree of interaction between the activities of the service organization and those of the user organization, and
- the nature of the relationship between the user organization and the service organization, including the relevant contractual terms for the activities undertaken by the service organization.

How do we obtain an understanding of the nature and significance of services? [ISA | 3983.1400]

We may use a variety of sources of information to help us understand the nature and significance of the services provided by the service organization including:

- user manuals
- system overviews
- technical manuals
- the contract or service level agreement between the entity and the service organization showing the services to be provided
- reports by service auditors, internal auditors or regulatory authorities on controls at the service organization
- System and Organization Control (SOC) reports
- visit the service organization
- inquiring of management

We may also be able to leverage the knowledge we obtained through past experience with the service organization, including prior year SOC reports, particularly if the services and controls at the service organization over those services are highly standardized.

How do we obtain an understanding of the nature and materiality of transactions? [ISA | 3983.13246]

Our understanding of the process can provide insight into the transactions processed by the service organization.

We think about the quantitative and qualitative aspects of the transactions processed and the accounts or financial reporting processes affected by the service organization. The nature of the transactions processed and the accounts affected by the service organization may not be quantitatively material, but may still be significant based on the nature of those transactions or accounts.

How do we obtain an understanding of the degree of interaction? [ISA | 3983.13247]

Our understanding of the process can provide insight into the degree of interaction between the service organization and the user entity.

What is 'degree of interaction'? [ISA | 3983.13244]

Degree of interaction is the extent to which the user organization is involved in the process to initiate, execute, process and record transaction that flow through the service organization.

A high degree of interaction exists when the user entity authorizes transactions and the service organization processes and accounts for those transactions. In this case, the user entity may be able to implement effective process-level controls over those transactions.

When there is a high degree of interaction, we may consider controls at the user entity to address the risks inherent in using the service organization. We determine the appropriateness of the design and implementation of those controls to conclude whether or not all risks have been mitigated to a sufficiently low level.

A low degree of interaction exists when the service organization initiates or initially records, processes, and accounts for the entity's transactions. In this case, the user entity may not be able to practically implement effective process-level controls.

How do we obtain an understanding of the nature of the relationship? [ISA | 3983.1700]

We may obtain an understanding of the nature of the relationship, including the relevant contractual terms for the activities undertaken by the service organization, by reviewing the contract or service level agreement between the user entity and the service organization. Relevant sections of the service level agreement can highlight factors, such as:

- the scope of services provided by the service organization
- whether the service organization provides a Type 1 or Type 2 SOC 1 report
- the information the service organization agrees to provide to the user entity
- defined responsibilities for initiating transactions relating to the activities performed by the service organization and information to be provided by the user entity
- the application of regulatory requirements concerning the form of records to be maintained, or access to them
- clauses that require the service organization to maintain internal control over financial reporting consistent with a recognized framework (e.g., COSO 2013)
- the indemnification, if any, the service organization will provide to the user entity in the event of a performance failure on the part of the service organization.
- terms that govern the resolution of any errors identified in the processing of transactions or other data
- clauses that require timely communication of identified discrepancies
- whether the user auditor has rights of access to the accounting records of the entity maintained by the service organization and other information relevant to the conduct of the audit,
- whether the agreement allows for direct communication between the user auditor and the service auditor
- terms that govern the timing of SOC 1 reporting and/or access to the service auditor
- acceptable deviation rates (if any)
- clauses that may impact how the user entity designs complementary user entity controls (CUECs) (e.g., clauses that limit the service organization's responsibility for errors)
- clauses that may impact how the user entity monitors the controls at the service organization

We may also corroborate this understanding by having discussions with the user entity and considering any other information from the service organization (e.g., user manuals, service guides, service organization provided training modules, etc.).

What is a subservice organization? [ISA | 3983.1800]

A subservice organization is an organization that a service organization uses to perform some of the services provided to the user entity. These services may also be relevant to the user entities' internal control over financial reporting. A subservice organization may be a separate entity from the service organization or may be related to the service organization.

We could also think of subservice organizations as the entities that service organizations outsource some of their operations to.

Service auditors will identify these subservice organizations in the SOC 1 reports.

When is a subservice organization relevant to the entity's internal controls over financial reporting? [ISA | 3983.1900]

Just like a service organization, a subservice organization is relevant to the entity's internal controls over financial reporting when those services, and the related controls, are part of the user entity's information system, including the IT environment relevant to financial reporting (see activity 'Understand information and communication' for further information on obtaining an understanding information and communication). This is the case when they affect any of the following:

- The classes of transactions, account balances, and disclosures in the entity's operations that are significant to the entity's financial statements
- The procedures, both automated (within IT) and manual, by which the entity's transactions are initiated, recorded, processed, and reported from their occurrence to their inclusion in the financial statements
- The related accounting records, whether electronic or manual, supporting information, and specific accounts in the entity's financial statements involved in initiating, recording, processing and reporting the entity's transactions
- How the entity's information system captures other events and conditions that are significant to the financial statements
- The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures

What are our responsibilities over subservice organizations? [ISA | 3983.13248]

When a service organization uses a subservice organization, we treat these subservice organizations the same as other service organizations.

We include the activities performed by the subservice organization in our understanding of the processes and controls at the user entity. In the end, we obtain sufficient information about the types of transactions that the subservice organization processes, the materiality of those transactions and the ultimate impact to the user entity's financial statements arising from those transactions. Understanding the activities performed by the subservice organization may identify additional RMMs which we then address in our audit.

How will the SOC 1 report inform a user entity that relevant controls are in place at a subservice organization? [ISA | 3983.13245]

When a service organization uses a subservice organization, the service auditor will identify the subservice organizations that may be relevant within the SOC 1 report. The servicer auditor may use either the inclusive method or the carve-out method.

Inclusive method	When the service auditor *includes* the subservice organization's relevant control objectives and related controls in the service organization's description of its system and the scope of the service auditor's engagement.
Carve-out method	When the service auditor *excludes* the subservice organization's relevant control objectives and related controls in the service organization's description of its system and the scope of the service auditor's engagement.

1.2.2 Understand the service organization's activities and internal controls [ISA | 3984]

What do we do?

Obtain an understanding of the activities performed and any relevant controls placed in operation by the service organization AND identify any relevant control deficiencies.

Why do we do this?

As part of our risk assessment procedures, we obtain an understanding of business processes and the financial reporting process. This includes understanding the entity's use of service organizations, which may be obtained through a variety of sources. This understanding provides the information to identify and assess risks of material misstatement (RMMs) and design further audit procedures.

Since risks can stem from any part of the process used to initiate, authorize, record and report transactions, we understand the business processes and the financial reporting process of the entity including activities that occur within the entity and outside the entity (i.e., at relevant service organizations).

Execute the Audit

How do we obtain an understanding of the activities performed by the service organization and how the internal controls placed in operation by the service organization relate to the user entity? [ISA | 3984.1300]

As part of understanding an entity's business processes, we obtain an understanding of the relevant activities that occur at the service organization, including subservice organizations, and how and where those activities fit into the user entity's overall process.

We may use a variety of sources of information to help us obtain a sufficient understanding, including the scope of work and the services and processed covered by the service organization, which may include:

- SOC reports (Type 1 or Type 2 SOC 1 report), if available
- user manuals
- system overviews
- technical manuals
- the contract or service level agreement between the entity and the service organization showing the services to be provided
- reports by service auditors, internal auditors or regulatory authorities on controls at the service organization
- contacting the service organization or visiting the service organization to perform inquiries and other procedures
- using another auditor to perform agreed upon procedures or other attestation procedures that will supply us the information to plan the audit
- reviewing the audit programs of the service auditor. In some cases, it may be appropriate to issue instructions to the service auditor as to the scope of the audit work.
- reviewing additional audit documentation of the service auditor relating to significant findings or issues in the engagement completion document.

We may also be able to leverage the knowledge we obtained through past experience with the service organization, including prior year SOC reports, particularly if the services and controls at the service organization over those services are highly standardized.

We coordinate any interactions with the service organization through the user entity - i.e., our audit client.

How do we determine which additional procedures to perform to understand the services provided and the internal controls over financial reporting relevant to the user entity? [ISA | 3984.13249]

The type and extent of additional procedures we perform, individually or in combination, are influenced by matters such as:

- Significance of the services provided by the service organization
- Complexity of the transactions at the entity and the complexity of the services provided by the service organization
- Location of the service organization
- Size of the entity and the service organization
- Nature of relationship between the entity and the service organization

Can a user entity establish their own processes and controls over the activities performed by a service organization? [ISA | 3984.13250]

Yes. In some cases, the user entity may establish their own processes and controls addressing process risk points related to the activities of the service organization.

For example, if the entity uses a service organization to process its payroll transactions, the user entity may establish controls over the submission and receipt of payroll information that could

prevent, or detect and correct, material misstatements that could occur at the service organization. These controls may include the following:

- Comparing the data submitted to the service organization with reports of information received from the service organization after the data has been processed
- Recalculating all or a sample of the payroll amounts for clerical accuracy and reviewing the total amount of the payroll for reasonableness

If we plan to rely solely on the user entity's controls over the service organization activities, we determine that all relevant process risk points are addressed.

When are control activities at the service organization relevant to the entity? [ISA | 3984.6313]

Control activities at the service organization are relevant to the entity when they are determined to be relevant control activities (see activity 'Determine which control activities are relevant to the audit').

What do we do when controls at the service organization are relevant to the entity? [ISA | 3984.6400]

If we are relying on the design and implementation and/or operating effectiveness of control(s) at the service organization, we obtain an understanding of relevant controls at the service organization, including subservice organizations, and how and where those controls fit into the user entity's overall process.

We also obtain an understanding of relevant controls at the user entity that relate to the services provided by the service organization, including those that are applied to the transactions processed by the service organization. This includes considering complementary user entity controls (CUECs), complementary subservice organization controls (CSOCs) and information.

What are Complementary User Entity Controls (CUECs)? [ISA | 3984.13251]

CUECs are controls that the service organization assumes, in the design of the service organization's system, will be implemented by user entities and are necessary to achieve the control objectives stated in the SOC 1 report.

What do we do with the CUECs? [ISA | 3984.1400]

We are responsible for obtaining an understanding of the controls designed and implemented by the user entity that address the CUECs, and determining that the implemented controls appropriately respond to CUECs identified as necessary to achieve the control objectives stated in the SOC 1 report. Controls that address the CUECs will vary from user entity to user entity based on how the user entity uses the service organization as well as the nature and significance of the transactions processed on the user entity's behalf.

How do we determine which CUECs are relevant to the user entity? [ISA | 3984.13252]

The SOC 1 report may link CUECs directly to relevant control objectives. This helps aid our understanding of which CUECs relate to which control objectives.

Management is responsible for implementing controls that address each CUEC deemed necessary by the service organization for each relevant control objective, but how management implements controls to address each CUEC may vary. For example, if one relevant control objective has four associated CUECs, management may implement one process level control to address all four CUECs.

What do we do if certain CUECs linked to a relevant control objective are not relevant to the user entity? [ISA | 3984.6312]

When certain CUECs linked to a relevant control objective are not relevant to the user entity, we document the rationale and the procedures performed to reach that conclusion.

What procedures do we perform when the service auditor uses the carve-out method? [ISA | 3984.13256]

When service organizations use the carve-out method to report on subservice organizations, service organizations will identify complementary subservice organization controls (CSOCs) that the service organization assumes will be implemented by those subservice organizations and that are necessary to achieve the control objectives.

We then determine whether there is a SOC 1 report covering the subservice organization that addresses the CSOCs. If there is no SOC 1 report issued for the subservice organization, we can instead:

- Test the controls that the user entity has implemented over the activities of the subservice organization
- Test the controls ourselves at the subservice organization
- Use another auditor which may include obtaining an agreed-upon procedures or other relevant attestation report that tests the controls in place at the subservice organization

What is the difference between the term 'attestation report' and 'assurance report'? [ISA | 3984.159206]

The terms 'attestation report' and 'assurance report' have the same meaning but are used by different standard setters. In this chapter, the PCAOB and AICPA use the term 'attestation report', whereas the ISA uses the term 'assurance report'.

Throughout this chapter, these terms are used interchangeably.

What are complementary subservice organization controls? [ISA | 3984.13253]

Complementary subservice organization controls (CSOCs) are controls that the service organization assumes in the design of the service organization's system that will be implemented by the subservice organization and are necessary to achieve the service organization's control objectives.

How do we determine which CSOCs are relevant to the subservice organization? [ISA | 3984.13254]

The service organization SOC 1 report will identify the relevant CSOCs that the service organization assumes will be implemented by the sub-service organization to achieve specified control objectives.

How do we determine that the CSOCs are designed, implemented and operating effectively at the subservice organization? [ISA | 3984.13257]

We obtain and evaluate the Type 1 or Type 2 SOC 1 report for the subservice organization to determine that relevant control objectives to address CSOCs have been suitably designed and implemented (Type 1 SOC 1) and suitably designed, implemented and operating effectively (Type 2 SOC 1).

How do we document our understanding of the process and control activities performed by the service organization? [ISA | 3984.13255]

There are several ways to demonstrate our understanding of the process that exists at the service organization, which may include flowcharting, creating a narrative and/or leveraging information from

a SOC 1 report. For example, we may choose to document the process through a flowchart at the control objective level for each of the relevant control objectives. In many cases, we may determine that reading and including the SOC 1 report and identifying the relevant control objectives is sufficient.

If we are relying on process control activities, we confirm that the PRPs within the process that relate to activities at the service organization are addressed by control objectives in the SOC 1 report. We also identify PRPs around the relevant handoffs of data between the service organization and the entity (e.g., inputs and outputs), as well as any and complementary user entity controls.

How does the service organization's activities influence the audit evidence we obtain? [ISA | 3984.13268]

When audit evidence is not available from records held at the user entity, we perform further audit procedures to obtain sufficient appropriate audit evidence or using another auditor to perform those procedures at the service organization on our behalf.

For example, when the service organization maintains material elements of the accounting records of the user entity, direct access to those records may be necessary in order for the user auditor to obtain sufficient appropriate audit evidence relating to the operations of controls over those records or to substantiate transactions and balances recorded in them, or both.

How do we obtain an understanding of the service organization's internal controls if the user entity outsources one or more significant parts of an entity's business or functions and a report on the controls at the service organization is not available? [ISA | 3984.1500]

When significant parts of an entity's business or functions are outsourced, a report on controls at the service organization may not be available. In that case, visiting the service organization may be the most effective method to gain an understanding of the controls at the service organization.

What if we plan to use a Type 1 or Type 2 SOC 1 report as audit evidence to support our understanding about the design and implementation of controls at the service organization? [ISA | 3984.13258]

If we plan to use a Type 1 or Type 2 SOC 1 report as evidence, we:

- evaluate whether the description and design of controls in the Type 1 SOC 1 report is as of a date, or in the case of a Type 2 SOC 1 report, evaluate whether the description, design and operating effectiveness is for a period, that is appropriate for the user auditor's purposes
- evaluate the sufficiency and appropriateness of the evidence provided by the report for the understanding of the controls at the service organization; and
- determine whether complementary user entity controls (CUECs) and complementary subservice organization controls (CSOCs) identified by the service organization are relevant to the user entity's financial statements (i.e., relate to risks we have identified as RMMs where we will test controls) and, if so, obtain an understanding of whether the user entity has designed and implemented such controls.
- identify and evaluate any relevant control deficiencies from the report

What is a SOC 1 report? [ISA | 3984.13259]

A SOC 1 report addresses the controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting. SOC 1 Type 1 and Type 2 reports provide a description of the service organization's system, control objectives and related controls, and in the case of a Type 2 report, tests of operating effectiveness of controls to achieve controls objectives.

What is a Type 1 service auditor's report? [ISA | 3984.13260]

A Type 1 service auditor's report provides an opinion about whether the controls at the service organization are appropriately designed and implemented to achieve the specified control objectives and whether they are placed in operation as of a specific date. However, a Type1 service auditor's report does not provide any evidence of the operating effectiveness of the relevant controls.

What is a Type 2 service auditor's report? [ISA | 3984.13261]

A Type 2 service auditor's report provides an opinion about whether the controls at the service organization are appropriately designed and implemented to achieve the specified control objectives and whether they are operating effectively throughout a specified period of time.

What is a SOC 2 report? [ISA | 3984.7262]

A SOC 2 - SOC for Service Organizations: Trust Services Criteria reports on a service organization's controls relevant to one or more of the following trust categories: security, availability, processing integrity, confidentiality and privacy of the information processed by a system. The report provides information and a service auditor's opinion on whether controls were designed and operated effectively (in the case of a Type 2) to achieve the service organization's system commitments and requirements in accordance with the AICPA trust criteria.

Like SOC 1 reports, there are Type 1 and Type 2 SOC 2 reports. A Type 1 SOC 2 report expresses an opinion on the design and implementation of relevant controls as of a specified date, while a Type 2 SOC 2 report expresses an opinion on the design, implementation and operating effectiveness of these controls throughout a specified period.

Can we use Type 2 SOC 2 reports when relying on internal controls at a service organization? [ISA | 3984.7263]

This type of report may be used as audit evidence if the system that is the subject matter of the report is relevant to the user entity's ICFR. Refer to Type 2 SOC 2 FAQs located on the Work Papers and Related Guidance page https://alex.kpmg.com/AROWeb/bridge/25081/27887?d=US,INTL on Alex (under "Related Guidance") for additional guidance.

What additional considerations are there if the entity outsources cloud computing? [ISA | 3984.13262]

When entities use service organizations for cloud computing, we treat them in the same way as any other service organization in our audit.

Due to the heightened risk that cloud computing can have on an entity's internal control over financial reporting, the involvement of specific team members with expertise in IT (IT Audit specific team members) is highly encouraged.

What is cloud computing? [ISA | 3984.13263]

Cloud computing is using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

Entities may hire cloud computing service organizations to provide and manage the entity's information technology capabilities.

What are some examples of cloud services? [ISA | 3984.13264]

Examples of cloud services include:

Cloud services	Description of services
Software as a Service	Provides software applications to the entity that reside on the cloud and not on the entity's hardware. An example of software as a service can be a service organization that provides human resource software applications, including payroll applications.
Platform as a Service	Provides the platform for the entity to develop and deploy cloud software applications which the entity owns and controls. An example of platform as a service can be a service organization that builds and supplies an IT environment on which the user entity can install their own applications and data sets.
Infrastructure as a Service	Provides the entity the ability to rent processing, storage, networks, and other computing resources where the entity controls the software application and operating systems. An example can be when a service organization offers storage solutions, e.g. data warehouse, to user organization to store their financial reporting information.

How do we identify if an entity uses cloud computing services? [ISA | 3984.13265]

We identify whether an entity uses a service organization to provide cloud computing services through gaining an understanding of their IT environment, which includes understanding the processes they use to identify cloud services being used throughout the entity and how they monitor when new cloud services are established.

Why do we identify whether the entity uses cloud computing services during the planning phase of our audit? [ISA | 3984.13266]

Cloud computing is becoming an important IT strategy for entities as this can be more cost effective, readily available and easily deployed throughout an entity. The following are some key characteristics of using cloud computing services that might be considered risks:

- Cloud services can result in significant changes to the entity's business processes and internal control over financial reporting
- Cloud environments being implemented with minimal involvement of the entity's IT department. Hence, the identification of whether an entity uses cloud services may be challenging to identify.
- Cloud computing service providers using multiple sub-service providers
- Software applications and data are easily transportable when using cloud services and may move back and forth between the cloud service provider's environment and those subservice providers environments.

Due to the risks that cloud computing can present and the impact to internal controls over financial reporting, we consider the following:

- As the identification of cloud computing services can be challenging, we obtain a robust understanding of the entity's control and governance processes over who at the entity is authorized to enter into arrangements with service providers
- Data migration from the entity's system to a cloud environment may occur outside of the entity's control environment. We obtain an understanding of how data is controlled and migrated to the cloud environment.
- We obtain an understanding of the cloud service arrangement and the impact to relevant process level controls and general IT controls to determine the nature, timing and extent of audit procedures to perform. The technology associated with cloud services may seem to simplify the management of IT, but it can add complexity to change management and configuration controls and can impact data integrity.
- We understand the flow of information and data to and from the service organization. The use of cloud computing involves the rapid movement of data which can result in less clarity about the flow of information and data.
- The cloud service provider may not provide a Type 1 or Type 2 SOC 1 report or may provide another attestation report not intended for internal control over financial reporting. If the cloud service provider does issue a Type 1 or Type 2 SOC 1 report, the report may carve-out a number of subservice organizations. This can impact our audit approach and how we plan to obtain sufficient audit evidence.
- Due to the ease of obtaining and changing cloud services, there is a greater risk of change during the gap period between the cloud service providers report date and the entity's reporting date, even if that gap period is short
- Cloud service providers may store the entity's data on servers in data centers located throughout the world. Hence, the entity considers compliance with local laws and regulations.

Due to the heightened risk that cloud computing can have on an entity's internal control over financial reporting, it is beneficial to have discussions with the entity early in the planning process. The involvement of specific team members with expertise in IT (IT Audit specific team members) is highly encouraged.

How might we determine whether the entity's use of a cloud computing service impacts the financial statements? [ISA | 3984.13267]

In addition to gaining an understanding of the entity's IT environment and business processes, we may be able to determine whether the entity's use of a cloud computing service impacts the entity's financial statements by asking management certain questions. It is particularly helpful to include specific team members with expertise in IT (IT Audit specific team members) in these inquiries.

The following are examples of the types of questions we can ask:

Review of cloud service arrangements	Has management reviewed the terms of each cloud service arrangement? Is there a process to review performance against contracts and service level agreements?

Risks associated with cloud computing	Have the risks associated with cloud computing arrangements been evaluated by management including the entity's Internal Audit department?
Impact to process level and IT controls	What has the entity done to understand the impact to relevant process level controls and general IT controls?
Understanding the relevant controls	Does the entity understand how the relevant controls impact the entity's internal control?
Retrieving relevant data	Is the entity able to retrieve data that may be relevant to the audit? For example, if the engagement team is planning on performing substantive analytical procedures to test relevant assertions related to revenue, can revenue data be retrieved by the entity?
Restrictions on data transfer	Are there any restrictions on data transfer? For example, if the data is located in a foreign country, are there restrictions on transferring data across borders?
Personally identifiable information	Does the entity understand how the service organization uses, retains and discloses personally identifiable information and other highly confidential information given that the entity's data, and the systems processing the data, may move from data center to data center around the world without the knowledge of the entity?
Future changes	How does the entity plan to monitor future changes to these processes given the easily changeable nature of cloud services?
Governance model for cloud enablement	Does the entity have a governance model that considers the decisions to be made and controls to be put in place for cloud enablement of business processes?
Updating existing internal control documentation	Has the entity updated its internal control documentation to reflect the new or changed business processes and general IT control processes?
Adequacy of monitoring and risk assessment controls	Has the entity assessed the impact of its use of cloud service providers on the adequacy of its monitoring and

	risk assessment controls and implemented new or revised controls?
Governance process over entering into arrangements	What governance process has the entity implemented to validate that only authorized personnel are able to enter into arrangements with a service organization given that cloud services may be procured outside the IT department, rapidly and usually without internal technology investment and deployment?
Compliance with local laws and regulations	Given that cloud service organizations may store the entity's data in data centers located in various jurisdictions around the world, has the entity considered compliance with local laws and regulations restricting the transfer of information across borders? Is data able to be obtained and recovered in a timely manner?
Skillset of IT personnel	Do the current IT personnel have the skillset to manage the implementation and daily interaction with and monitoring of the cloud service model? Will there be changes to the IT department? For example, will new IT resources be used, will there be retraining or will there be a reduction in headcount?
Controls over migration to the cloud	Has the entity considered controls over migration of its existing system to the 'cloud' environment?
Physical security over data	Where will the data be housed, and have physical security, access to servers and infrastructure been considered?
Skillset and capacity	Does the entity have the appropriate skillset and capacity to deal with secure connections for the volume of data and transactions being processed with the service providers?
Access to programs and data	Will access to the cloud based application be integrated with internal systems and therefore use internal logical access controls or be part of the cloud service provider's logical access controls? What changes will be made to access to programs and data controls both internally and at the service provider? For example, who will be granted super user access? Will other parties be provided access? How will user access be administered and will the cloud service provider provide

	security monitoring over logging and monitoring of access, including timely discovery, assessment, and reporting of breaches?
Program change controls	What changes will be made to program change controls? For example, will a web portal be set up to allow the entity's programmers to make changes to programs being hosted by the service provider?

1.3 Determine whether we sufficiently understand how the entity uses the service organization [ISA | 3985]

What do we do?

Determine whether we have obtained a sufficient understanding of the nature and significance of the services provided by the service organization

Why do we do this?

Obtaining a sufficient understanding of the services provided by the service organization allows us to effectively identify process risk points and identify risks of material misstatements.

Execute the Audit

How do we determine whether we have obtained a sufficient understanding of the nature and significance of the services provided by the service organization? [ISA | 3985.1300]

We have obtained a sufficient understanding when we have a complete understanding of how transactions are initiated, authorized, processed and recorded.

In making this determination, we consider all the available information we have collected about the nature and significance of the services provided by a service organization and the effect on the user entity's internal control relevant to the audit and whether it provides an appropriate basis for the identification and assessment of the risks of material misstatement.

What do we do if we have not obtained a sufficient understanding of the nature and significance of the services provided by the service organization? [ISA | 3985.1400]

We look to any other available sources, which may include performing the following:

- Obtaining and reading a Type 1 or Type 2 report, if available
- Contacting the service organization, using the entity, to obtain such an understanding

- Using another auditor to perform agreed-upon or other attestation procedures that will supply us the information to plan the audit. We coordinate this effort with the user entity.
- Visiting the service organization and performing procedures, such as a walkthrough, to obtain an understanding
- Reviewing the audit programs of the service auditor. In some cases, it may be appropriate to issue instructions to the service auditor as to the scope of the audit work.
- Reviewing additional audit documentation of the service auditor relating to significant findings or issues in the engagement completion document

What do we do if we are still unable to obtain a sufficient understanding of the nature and significance of the services provided by the service organization? [ISA | 3985.1500]

We determine whether we issue a qualified opinion or disclaim our opinion. In determining whether we issue a qualified opinion or disclaim our opinion, we perform the activities in the chapter on modifications to the opinion (AU-C 705, ISA 705) or we perform the activities in the chapter on departures from unqualified opinions and other reporting circumstances (AS 3105) for further information.

1.4 Perform certain inquiries [ISA | 3995]

What do we do?

Perform certain inquiries to determine whether we can place reliance on the service auditor's report, AUP report or other attestation report.

Why do we do this?

When we plan to rely on the work performed by a service auditor, there are certain inquiries we perform to determine if we can place reliance on the report. If we cannot place reliance on the report, there could be changes in our audit plan and audit execution.

Execute the Audit

What inquiries do we perform as part of determining whether we can place reliance on the report? [ISA | 3995.1300]

We perform the following inquiries to determine whether we can place reliance on a report:

- We inquire of the service auditor's and other auditor's professional reputation, competence and independence
- We inquire of the user entity's management whether they are aware of non-compliance with laws and regulations, including illegal acts and fraud, at the service organization that could impact the financial statements
- We inquire of the user entity's management of the time period covered

1.4.1 Inquire about the service auditor's and other auditor's professional reputation, competence and independence [ISA | 3996]

What do we do?

Inquire of the service auditor's and other auditor's professional reputation, competence and independence.

Why do we do this?

We perform inquiries related to the service auditor and other auditor when we plan on relying on a service auditor's report (e.g. Type 1 or Type 2 SOC report, agreed-upon procedures or other attestation report). We perform this during audit planning because this is one of the steps in determining whether we can place reliance on the service auditor's or other auditor's report. If we cannot place reliance on the service auditor's or other auditor's report, there could be changes in our audit plan and execution.

Execute the Audit

How do we obtain information about a service auditor's or other auditor's professional reputation and competence? [ISA | 3996.1300]

We obtain information about the service auditor's and other auditor's professional reputation and competence by making inquiries of the following:

- The Public Company Accounting Oversight Board (PCAOB), the American Institute of Certified Public Accountants (AICPA), the applicable state society of certified public accountants and/or the local chapter, or in the case of a non-US auditor, his corresponding professional organization.
- Other practitioners
- Bankers and other credit grantors
- Other appropriate sources, including professional organizations
- Other appropriate regulatory agency, if applicable

We may already have insights into the professional reputation and competence of the service auditor or other auditor based on our previous experience or their standing in the marketplace (see activities 'Understand the component auditor's professional reputation ' and 'Understand the component auditor's professional competence ' for information on how we assess the professional reputation and competence of the service auditor). We use our judgment to determine the extent of procedures we might perform to determine the reputation and competence for these larger and more well-known firms. This can include looking to publicly available inspection results, performing inquiries of the service auditor or use our experience as a successor auditor.

How do we determine whether a service auditor or other auditor is independent? [ISA | 3996.1400]

Relevant professional standards state that service auditors to be independent from the service organization (see activity 'Understand the component auditor's independence and compliance with ethical requirements ' for information on how we understand the independence of the service auditor

or other auditor). Unless we identify contradicting evidence, a service auditor's or other auditor's report implies that the service auditor or other auditor is independent of the service organization as the report issued by the service auditor is titled "Independent Service Auditor's Report" and the report issued by the other auditor is titled "Independent Accountant's Report".

When do we perform these procedures and make inquiries about the service auditor or other auditor? [ISA | 3996.1500]

We perform these procedures and make inquiries during audit planning, before we choose to use a Type 1 or Type 2 SOC 1, AUP report or other attestation report. We also remain alert for any information that may indicate a change in our initial assessment throughout the audit.

What do we do if the service auditor or other auditor has a poor professional reputation, is not competent, or is not independent? [ISA | 3996.1600]

When the service auditor or other auditor has a poor professional reputation, is not deemed to be competent, or is not independent, we cannot rely on the report they issue. Instead, we test the relevant controls in a different manner. This can include:

- Testing the controls that the user entity has implemented over the activities of the service organization
- Testing the controls ourselves at the service organization
- Using another auditor which may include obtaining an agreed-upon procedures or other relevant attestation report from another auditor that includes tests of the operating effectiveness of the relevant controls

1.4.2 Inquire about items that could impact the financial statements [ISA | 3997]

What do we do?

Inquire of the user entity's management whether they are aware of any uncorrected misstatements, fraud and non-compliance with laws and regulations, including illegal acts, that could impact the financial statements.

Why do we do this?

If we plan to place reliance on the SOC 1 report, we obtain an understanding of whether the entity is aware of any fraud, non-compliance with laws and regulations, including illegal acts, and uncorrected misstatements that could impact the entity's financial statements. These can be communicated to the entity by the service organization or may become known to the entity some other way.

If we cannot place reliance on the SOC 1 report, there could be changes in our audit plan and audit execution.

Execute the Audit

What do we do if we become aware of uncorrected misstatements, fraud or non-compliance with laws and regulations, including illegal acts through inquiries of the entity? [ISA | 3997.1300]

After we obtain a clear understanding of the uncorrected misstatements, fraud, non-compliance with laws and regulations, including illegal acts, occurring at the service organization, we determine the impact on our audit. This may involve further discussions with both the entity as well as the service organization.

What is the impact to the audit when there are uncorrected misstatements, actual or suspected fraud or non-compliance with laws and regulations, including illegal acts that impact the entity? [ISA | 3997.1400]

The impacts on our audit may include:

- identifying a new risk of material misstatement in addition to the ones identified in our risk assessment process,
- modifying a risk of material misstatement we previously identified,
- no longer planning to rely on the relevant controls at the service organization which can impact the nature, timing and extent of audit procedures,
- considering what management has done to address these issues and whether they implemented any compensating controls at the entity, or
- modifying our auditor's report

See the chapters on fraud (ISA 240 , AU-C 240 , AS 2401), laws and regulations (ISA 250 , AU-C 250 , AS 2405) and evaluating misstatements (ISA 450 , AU-C 450 , AS 2810) for further information.

1.4.3 Inquire of the time period [ISA | 3998]

What do we do?

Inquire of management the time period covered by the service auditor's report and how management has assessed the time period covered

Why do we do this?

Service auditor reports may not cover the entire audit period. We determine what period of the fiscal year is covered by the service auditor report and how much of the period is not covered. The period that is not covered is called the gap period.

Identifying the significance of the gap period during planning helps us properly plan a response.

Execute the Audit

When do we inquire of management on how they have assessed the time period covered by the service auditor's report? [ISA | 3998.1300]

We inquire of management during audit planning and risk assessment.

When the entity expects there to be a gap period, we also inquire about how management has assessed the time period covered. This may include understanding the entity's risk assessment and the design and implementation of relevant monitoring controls that are in place to address the gap period.

1.5 Evaluate the service auditor [ISA | 3999]

What do we do?

Evaluate specific information about the service auditor

Why do we do this?

Evaluating specific information about the service auditor allows us to determine upfront whether or not we can rely on the service auditor's report. Non-reliance on a service auditor's report can impact the nature, timing and extent of our audit procedures so it is beneficial to identify potential issues early.

Execute the Audit

What specific information about the service auditor do we evaluate before we use them? [ISA | 3999.1300]

We evaluate whether the service auditor has followed the adequate professional standards in issuing the service auditor's report.

1.5.1 Determine the adequacy of the standards [ISA | 4000]

What do we do?

Determine the adequacy of the standards under which the service auditor's report was issued.

Why do we do this?

If the service auditor hasn't followed adequate professional standards in producing the Type 1 or Type 2 report, we may not be able to rely on the report.

Execute the Audit

What professional standards are adequate for us to use a service auditor's report? [ISA | 4000.1300]

Service auditor reports may be issued under:

- AICPA AT-C 320 Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting;
- International Standard on Assurance Engagements 3402, Assurance Reports on Controls at a Service Organization (ISAE 3402)); and/or
- Other recognized assurance standards where the report provides evidence relevant to a user entity's internal control over financial reporting

How do we determine which professional standards are used by the service auditor? [ISA | 4000.1400]

We determine which professional standards are used by the service auditor by reading the service auditor's report.

Responding to the Assessed Risks of Material Misstatement

International Standards on Auditing: ISA 402.15-17

Responding to the Assessed Risks of Material Misstatement

15. In responding to assessed risks in accordance with ISA 330, the user auditor shall:

(a) Determine whether sufficient appropriate audit evidence concerning the relevant financial statement assertions is available from records held at the user entity; and, if not,

(b) Perform further audit procedures to obtain sufficient appropriate audit evidence or use another auditor to perform those procedures at the service organization on the user auditor's behalf. (Ref: Para. A24-A28)

Tests of Controls

16. When the user auditor's risk assessment includes an expectation that controls at the service organization are operating effectively, the user auditor shall obtain audit evidence about the operating effectiveness of those controls from one or more of the following procedures:

(a) Obtaining a type 2 report, if available;

(b) Performing appropriate tests of controls at the service organization; or

(c) Using another auditor to perform tests of controls at the service organization on behalf of the user auditor. (Ref: Para. A29-A30)

Using a Type 2 Report as Audit Evidence that Controls at the Service Organization Are Operating Effectively

17. If, in accordance with paragraph 16(a), the user auditor plans to use a type 2 report as audit evidence that controls at the service organization are operating effectively, the user auditor shall determine whether the service auditor's report provides sufficient appropriate audit evidence about the effectiveness of the controls to support the user auditor's risk assessment by:

(a) Evaluating whether the description, design and operating effectiveness of controls at the service organization is at a date or for a period that is appropriate for the user auditor's purposes;

(b) Determining whether complementary user entity controls identified by the service organization are relevant to the user entity and, if so, obtaining an understanding of whether the user entity has designed and implemented such controls and, if so, testing their operating effectiveness;

(c) Evaluating the adequacy of the time period covered by the tests of controls and the time elapsed since the performance of the tests of controls; and

(d) Evaluating whether the tests of controls performed by the service auditor and the results thereof, as described in the service auditor's report, are relevant to the assertions in the user entity's financial statements and provide sufficient appropriate audit evidence to support the user auditor's risk assessment. (Ref: Para. A31-A39)

ISA Application and Other Explanatory Material: ISA 402.A24-A39

Responding to the Assessed Risks of Material Misstatement (Ref: Para. 15)

A24. Whether the use of a service organization increases a user entity's risk of material misstatement depends on the nature of the services provided and the controls over these services; in some cases, the use of a service organization may decrease a user entity's risk of material misstatement, particularly if the user entity itself does not possess the expertise necessary to undertake particular activities, such as initiating, processing, and recording transactions, or does not have adequate resources (for example, an IT system).

A25. When the service organization maintains material elements of the accounting records of the user entity, direct access to those records may be necessary in order for the user auditor to obtain sufficient appropriate audit evidence relating to the operations of controls over those records or to substantiate transactions and balances recorded in them, or both. Such access may involve either physical inspection of records at the service organization's premises or interrogation of records maintained electronically from the user entity or another location, or both. Where direct access is achieved electronically, the user auditor may thereby obtain evidence as to the adequacy of controls operated by the service organization over the completeness and integrity of the user entity's data for which the service organization is responsible.

A26. In determining the nature and extent of audit evidence to be obtained in relation to balances representing assets held or transactions undertaken by a service organization on behalf of the user entity, the following procedures may be considered by the user auditor:

(a) Inspecting records and documents held by the user entity: the reliability of this source of evidence is determined by the nature and extent of the accounting records and supporting documentation retained by the user entity. In some cases, the user entity may not maintain independent detailed records or documentation of specific transactions undertaken on its behalf.

(b) Inspecting records and documents held by the service organization: the user auditor's access to the records of the service organization may be established as part of the contractual arrangements between the user entity and the service organization. The user auditor may also use another auditor, on its behalf, to gain access to the user entity's records maintained by the service organization.

(c) Obtaining confirmations of balances and transactions from the service organization: where the user entity maintains independent records of balances and transactions, confirmation from the service organization corroborating the user entity's records may constitute reliable audit evidence concerning the existence of the transactions and assets concerned. For example, when multiple service organizations are used, such as an investment manager and a custodian, and these service organizations maintain independent records, the user auditor may confirm balances with these organizations in order to compare this information with the independent records of the user entity.

If the user entity does not maintain independent records, information obtained in confirmations from the service organization is merely a statement of what is reflected in the records maintained by the service organization. Therefore, such confirmations do not, taken alone, constitute reliable audit evidence. In these circumstances, the user auditor may consider whether an alternative source of independent evidence can be identified.

(d) Performing analytical procedures on the records maintained by the user entity or on the reports received from the service organization: the effectiveness of analytical procedures is likely to vary by assertion and will be affected by the extent and detail of information available.

A27. Another auditor may perform procedures that are substantive in nature for the benefit of user auditors. Such an engagement may involve the performance, by another auditor, of procedures agreed upon by the user entity and its user auditor and by the service organization and its service auditor. The findings resulting from the procedures performed by another auditor are reviewed by the user auditor to determine whether they constitute sufficient appropriate audit evidence. In addition, there may be requirements imposed by governmental authorities or through contractual arrangements whereby a service auditor performs designated procedures that are substantive in nature. The results of the application of the required procedures to balances and transactions processed by the service organization may be used by user auditors as part of the evidence necessary to support their audit opinions. In these circumstances, it may be useful for the user auditor and the service auditor to agree, prior to the performance of the procedures, to the audit documentation or access to audit documentation that will be provided to the user auditor.

A28. In certain circumstances, in particular when a user entity outsources some or all of its finance function to a service organization, the user auditor may face a situation where a significant portion of the audit evidence resides at the service organization. Substantive procedures may need to be performed at the service organization by the user auditor or another auditor on its behalf. A service auditor may provide a type 2 report and, in addition, may perform substantive procedures on behalf of the user auditor. The involvement of another auditor does not alter the user auditor's responsibility to obtain sufficient appropriate audit evidence to afford a reasonable basis to support the user auditor's opinion. Accordingly, the user auditor's consideration of whether sufficient appropriate audit evidence has been obtained and whether the user auditor needs to perform further substantive procedures includes the user auditor's involvement with, or evidence of, the direction, supervision and performance of the substantive procedures performed by another auditor.

Tests of Controls (Ref: Para. 16)

A29. The user auditor is required by ISA 330[10] to design and perform tests of controls to obtain sufficient appropriate audit evidence as to the operating effectiveness of controls in certain circumstances. In the context of a service organization, this requirement applies when:

(a) The user auditor's assessment of risks of material misstatement includes an expectation that the controls at the service organization are operating effectively (that is, the user auditor intends to rely on the operating effectiveness of controls at the service organization in determining the nature, timing and extent of substantive procedures); or

(b) Substantive procedures alone, or in combination with tests of the operating effectiveness of controls at the user entity, cannot provide sufficient appropriate audit evidence at the assertion level.

_____

10 ISA 330, paragraph 8

A30. If a type 2 report is not available, a user auditor may contact the service organization, through the user entity, to request that a service auditor be engaged to provide a type 2 report that includes tests of the operating effectiveness of the relevant controls or the user auditor may use another auditor to perform procedures at the service organization that test the operating effectiveness of those controls. A user auditor may also visit the service organization and perform tests of controls if the service organization agrees to it. The user auditor's risk assessments are based on the combined evidence provided by the work of another auditor and the user auditor's own procedures.

Using a Type 2 Report as Audit Evidence that Controls at the Service Organization Are Operating Effectively (Ref: Para. 17)

A31. A type 2 report may be intended to satisfy the needs of several different user auditors; therefore tests of controls and results described in the service auditor's report may not be relevant to assertions that are significant in the user entity's financial statements. The relevant tests of controls and results are evaluated to determine that the service auditor's report provides sufficient appropriate audit evidence about the effectiveness of the controls to support the user auditor's risk assessment. In doing so, the user auditor may consider the following factors:

(a) The time period covered by the tests of controls and the time elapsed since the performance of the tests of controls;

(b) The scope of the service auditor's work and the services and processes covered, the controls tested and tests that were performed, and the way in which tested controls relate to the user entity's controls; and

(c) The results of those tests of controls and the service auditor's opinion on the operating effectiveness of the controls.

A32. For certain assertions, the shorter the period covered by a specific test and the longer the time elapsed since the performance of the test, the less audit evidence the test may provide. In comparing the period covered by the type 2 report to the user entity's financial reporting period, the user auditor may conclude that the type 2 report offers less audit evidence if there is little overlap between the period covered by the type 2 report and the period for which the user auditor intends to rely on the report. When this is the case, a type 2 report covering a preceding or subsequent period may provide additional audit evidence. In other cases, the user auditor may determine it is necessary to perform, or use another auditor to perform, tests of controls at the service organization in order to obtain sufficient appropriate audit evidence about the operating effectiveness of those controls.

A33. It may also be necessary for the user auditor to obtain additional evidence about significant changes to the controls at the service organization outside of the period covered by the type 2 report or determine additional audit procedures to be performed. Relevant factors in determining what additional audit evidence to obtain about controls at the service organization that were operating outside of the period covered by the service auditor's report may include:

- The significance of the assessed risks of material misstatement at the assertion level;

- The specific controls that were tested during the interim period, and significant changes to them since they were tested, including changes in the information system, processes, and personnel;
- The degree to which audit evidence about the operating effectiveness of those controls was obtained;
- The length of the remaining period;
- The extent to which the user auditor intends to reduce further substantive procedures based on the reliance on controls; and
- The effectiveness of the control environment and the user entity's process to monitor the system of internal control.

A34. Additional audit evidence may be obtained, for example, by extending tests of controls over the remaining period or testing the user entity's process to monitor the system of internal control.

A35. If the service auditor's testing period is completely outside the user entity's financial reporting period, the user auditor will be unable to rely on such tests for the user auditor to conclude that the user entity's controls are operating effectively because they do not provide current audit period evidence of the effectiveness of the controls, unless other procedures are performed.

A36. In certain circumstances, a service provided by the service organization may be designed with the assumption that certain controls will be implemented by the user entity. For example, the service may be designed with the assumption that the user entity will have controls in place for authorizing transactions before they are sent to the service organization for processing. In such a situation, the service organization's description of controls may include a description of those complementary user entity controls. The user auditor considers whether those complementary user entity controls are relevant to the service provided to the user entity.

A37. If the user auditor believes that the service auditor's report may not provide sufficient appropriate audit evidence, for example, if a service auditor's report does not contain a description of the service auditor's tests of controls and results thereon, the user auditor may supplement the understanding of the service auditor's procedures and conclusions by contacting the service organization, through the user entity, to request a discussion with the service auditor about the scope and results of the service auditor's work. Also, if the user auditor believes it is necessary, the user auditor may contact the service organization, through the user entity, to request that the service auditor perform procedures at the service organization. Alternatively, the user auditor, or another auditor at the request of the user auditor, may perform such procedures.

A38. The service auditor's type 2 report identifies results of tests, including exceptions and other information that could affect the user auditor's conclusions. Exceptions noted by the service auditor or a modified opinion in the service auditor's type 2 report do not automatically mean that the service auditor's type 2 report will not be useful for the audit of the user entity's financial statements in assessing the risks of material misstatement. Rather, the exceptions and the matter giving rise to a modified opinion in the service auditor's type 2 report are considered in the user auditor's assessment of the testing of controls performed by the service auditor. In considering the exceptions and matters giving rise to a modified opinion, the user auditor may discuss such matters with the service auditor. Such communication is dependent upon the user entity contacting the service organization, and obtaining the service organization's approval for the communication to take place.

Communication of deficiencies in internal control identified during the audit

A39. The user auditor is required to communicate in writing significant deficiencies identified during the audit to both management and those charged with governance on a timely basis.[11] The user auditor is also required to communicate to management at an appropriate level of responsibility on a timely basis other deficiencies in internal control identified during the audit that, in the user auditor's professional judgment, are of sufficient importance to merit management's attention.[12] Matters that the user auditor may identify during the audit and may communicate to management and those charged with governance of the user entity include:

- Any controls within the entity's process to monitor the system of internal control that could be implemented by the user entity, including those identified as a result of obtaining a type 1 or type 2 report;
- Instances where complementary user entity controls are noted in the type 1 or type 2 report and are not implemented at the user entity; and
- Controls that may be needed at the service organization that do not appear to have been implemented or that are not specifically covered by a type 2 report.

---

11 ISA 265, *Communicating Deficiencies in Internal Control to Those Charged with Governance and Management,* paragraphs 9 - 10

12 ISA 265, paragraph 10

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Understand the service organization's activities and internal controls [ISA | 3984]

What do we do?

Obtain an understanding of the activities performed and any relevant controls placed in operation by the service organization AND identify any relevant control deficiencies.

Why do we do this?

As part of our risk assessment procedures, we obtain an understanding of business processes and the financial reporting process. This includes understanding the entity's use of service organizations, which may be obtained through a variety of sources. This understanding provides the information to identify and assess risks of material misstatement (RMMs) and design further audit procedures.

Since risks can stem from any part of the process used to initiate, authorize, record and report transactions, we understand the business processes and the financial reporting process of the entity including activities that occur within the entity and outside the entity (i.e., at relevant service organizations).

Execute the Audit

How do we obtain an understanding of the activities performed by the service organization and how the internal controls placed in operation by the service organization relate to the user entity? [ISA | 3984.1300]

As part of understanding an entity's business processes, we obtain an understanding of the relevant activities that occur at the service organization, including subservice organizations, and how and where those activities fit into the user entity's overall process.

We may use a variety of sources of information to help us obtain a sufficient understanding, including the scope of work and the services and processed covered by the service organization, which may include:

- SOC reports (Type 1 or Type 2 SOC 1 report), if available
- user manuals
- system overviews
- technical manuals
- the contract or service level agreement between the entity and the service organization showing the services to be provided
- reports by service auditors, internal auditors or regulatory authorities on controls at the service organization
- contacting the service organization or visiting the service organization to perform inquiries and other procedures
- using another auditor to perform agreed upon procedures or other attestation procedures that will supply us the information to plan the audit
- reviewing the audit programs of the service auditor. In some cases, it may be appropriate to issue instructions to the service auditor as to the scope of the audit work.
- reviewing additional audit documentation of the service auditor relating to significant findings or issues in the engagement completion document.

We may also be able to leverage the knowledge we obtained through past experience with the service organization, including prior year SOC reports, particularly if the services and controls at the service organization over those services are highly standardized.

We coordinate any interactions with the service organization through the user entity - i.e., our audit client.

How do we determine which additional procedures to perform to understand the services provided and the internal controls over financial reporting relevant to the user entity? [ISA | 3984.13249]

The type and extent of additional procedures we perform, individually or in combination, are influenced by matters such as:

- Significance of the services provided by the service organization
- Complexity of the transactions at the entity and the complexity of the services provided by the service organization
- Location of the service organization
- Size of the entity and the service organization
- Nature of relationship between the entity and the service organization

Can a user entity establish their own processes and controls over the activities performed by a service organization? [ISA | 3984.13250]

Yes. In some cases, the user entity may establish their own processes and controls addressing process risk points related to the activities of the service organization.

For example, if the entity uses a service organization to process its payroll transactions, the user entity may establish controls over the submission and receipt of payroll information that could prevent, or detect and correct, material misstatements that could occur at the service organization. These controls may include the following:

- Comparing the data submitted to the service organization with reports of information received from the service organization after the data has been processed
- Recalculating all or a sample of the payroll amounts for clerical accuracy and reviewing the total amount of the payroll for reasonableness

If we plan to rely solely on the user entity's controls over the service organization activities, we determine that all relevant process risk points are addressed.

When are control activities at the service organization relevant to the entity? [ISA | 3984.6313]

Control activities at the service organization are relevant to the entity when they are determined to be relevant control activities (see activity 'Determine which control activities are relevant to the audit').

What do we do when controls at the service organization are relevant to the entity? [ISA | 3984.6400]

If we are relying on the design and implementation and/or operating effectiveness of control(s) at the service organization, we obtain an understanding of relevant controls at the service organization, including subservice organizations, and how and where those controls fit into the user entity's overall process.

We also obtain an understanding of relevant controls at the user entity that relate to the services provided by the service organization, including those that are applied to the transactions processed by the service organization. This includes considering complementary user entity controls (CUECs), complementary subservice organization controls (CSOCs) and information.

What are Complementary User Entity Controls (CUECs)? [ISA | 3984.13251]

CUECs are controls that the service organization assumes, in the design of the service organization's system, will be implemented by user entities and are necessary to achieve the control objectives stated in the SOC 1 report.

What do we do with the CUECs? [ISA | 3984.1400]

We are responsible for obtaining an understanding of the controls designed and implemented by the user entity that address the CUECs, and determining that the implemented controls appropriately respond to CUECs identified as necessary to achieve the control objectives stated in the SOC 1 report. Controls that address the CUECs will vary from user entity to user entity based on how the user entity uses the service organization as well as the nature and significance of the transactions processed on the user entity's behalf.

How do we determine which CUECs are relevant to the user entity? [ISA | 3984.13252]

The SOC 1 report may link CUECs directly to relevant control objectives. This helps aid our understanding of which CUECs relate to which control objectives.

Management is responsible for implementing controls that address each CUEC deemed necessary by the service organization for each relevant control objective, but how management implements controls

to address each CUEC may vary. For example, if one relevant control objective has four associated CUECs, management may implement one process level control to address all four CUECs.

What do we do if certain CUECs linked to a relevant control objective are not relevant to the user entity? [ISA | 3984.6312]

When certain CUECs linked to a relevant control objective are not relevant to the user entity, we document the rationale and the procedures performed to reach that conclusion.

What procedures do we perform when the service auditor uses the carve-out method? [ISA | 3984.13256]

When service organizations use the carve-out method to report on subservice organizations, service organizations will identify complementary subservice organization controls (CSOCs) that the service organization assumes will be implemented by those subservice organizations and that are necessary to achieve the control objectives.

We then determine whether there is a SOC 1 report covering the subservice organization that addresses the CSOCs. If there is no SOC 1 report issued for the subservice organization, we can instead:

- Test the controls that the user entity has implemented over the activities of the subservice organization
- Test the controls ourselves at the subservice organization
- Use another auditor which may include obtaining an agreed-upon procedures or other relevant attestation report that tests the controls in place at the subservice organization

What is the difference between the term 'attestation report' and 'assurance report'? [ISA | 3984.159206]

The terms 'attestation report' and 'assurance report' have the same meaning but are used by different standard setters. In this chapter, the PCAOB and AICPA use the term 'attestation report', whereas the ISA uses the term 'assurance report'.

Throughout this chapter, these terms are used interchangeably.

What are complementary subservice organization controls? [ISA | 3984.13253]

Complementary subservice organization controls (CSOCs) are controls that the service organization assumes in the design of the service organization's system that will be implemented by the subservice organization and are necessary to achieve the service organization's control objectives.

How do we determine which CSOCs are relevant to the subservice organization? [ISA | 3984.13254]

The service organization SOC 1 report will identify the relevant CSOCs that the service organization assumes will be implemented by the sub-service organization to achieve specified control objectives.

How do we determine that the CSOCs are designed, implemented and operating effectively at the subservice organization? [ISA | 3984.13257]

We obtain and evaluate the Type 1 or Type 2 SOC 1 report for the subservice organization to determine that relevant control objectives to address CSOCs have been suitably designed and implemented (Type 1 SOC 1) and suitably designed, implemented and operating effectively (Type 2 SOC 1).

How do we document our understanding of the process and control activities performed by the service organization? [ISA | 3984.13255]

There are several ways to demonstrate our understanding of the process that exists at the service organization, which may include flowcharting, creating a narrative and/or leveraging information from a SOC 1 report. For example, we may choose to document the process through a flowchart at the control objective level for each of the relevant control objectives. In many cases, we may determine that reading and including the SOC 1 report and identifying the relevant control objectives is sufficient.

If we are relying on process control activities, we confirm that the PRPs within the process that relate to activities at the service organization are addressed by control objectives in the SOC 1 report. We also identify PRPs around the relevant handoffs of data between the service organization and the entity (e.g., inputs and outputs), as well as any and complementary user entity controls.

How does the service organization's activities influence the audit evidence we obtain? [ISA | 3984.13268]

When audit evidence is not available from records held at the user entity, we perform further audit procedures to obtain sufficient appropriate audit evidence or using another auditor to perform those procedures at the service organization on our behalf.

For example, when the service organization maintains material elements of the accounting records of the user entity, direct access to those records may be necessary in order for the user auditor to obtain sufficient appropriate audit evidence relating to the operations of controls over those records or to substantiate transactions and balances recorded in them, or both.

How do we obtain an understanding of the service organization's internal controls if the user entity outsources one or more significant parts of an entity's business or functions and a report on the controls at the service organization is not available? [ISA | 3984.1500]

When significant parts of an entity's business or functions are outsourced, a report on controls at the service organization may not be available. In that case, visiting the service organization may be the most effective method to gain an understanding of the controls at the service organization.

What if we plan to use a Type 1 or Type 2 SOC 1 report as audit evidence to support our understanding about the design and implementation of controls at the service organization? [ISA | 3984.13258]

If we plan to use a Type 1 or Type 2 SOC 1 report as evidence, we:

- evaluate whether the description and design of controls in the Type 1 SOC 1 report is as of a date, or in the case of a Type 2 SOC 1 report, evaluate whether the description, design and operating effectiveness is for a period, that is appropriate for the user auditor's purposes
- evaluate the sufficiency and appropriateness of the evidence provided by the report for the understanding of the controls at the service organization; and
- determine whether complementary user entity controls (CUECs) and complementary subservice organization controls (CSOCs) identified by the service organization are relevant to the user entity's financial statements (i.e., relate to risks we have identified as RMMs where we will test controls) and, if so, obtain an understanding of whether the user entity has designed and implemented such controls.
- identify and evaluate any relevant control deficiencies from the report

What is a SOC 1 report? [ISA | 3984.13259]

A SOC 1 report addresses the controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting. SOC 1 Type 1 and Type 2 reports provide a

description of the service organization's system, control objectives and related controls, and in the case of a Type 2 report, tests of operating effectiveness of controls to achieve controls objectives.

What is a Type 1 service auditor's report? [ISA | 3984.13260]

A Type 1 service auditor's report provides an opinion about whether the controls at the service organization are appropriately designed and implemented to achieve the specified control objectives and whether they are placed in operation as of a specific date. However, a Type1 service auditor's report does not provide any evidence of the operating effectiveness of the relevant controls.

What is a Type 2 service auditor's report? [ISA | 3984.13261]

A Type 2 service auditor's report provides an opinion about whether the controls at the service organization are appropriately designed and implemented to achieve the specified control objectives and whether they are operating effectively throughout a specified period of time.

What is a SOC 2 report? [ISA | 3984.7262]

A SOC 2 - SOC for Service Organizations: Trust Services Criteria reports on a service organization's controls relevant to one or more of the following trust categories: security, availability, processing integrity, confidentiality and privacy of the information processed by a system. The report provides information and a service auditor's opinion on whether controls were designed and operated effectively (in the case of a Type 2) to achieve the service organization's system commitments and requirements in accordance with the AICPA trust criteria.

Like SOC 1 reports, there are Type 1 and Type 2 SOC 2 reports. A Type 1 SOC 2 report expresses an opinion on the design and implementation of relevant controls as of a specified date, while a Type 2 SOC 2 report expresses an opinion on the design, implementation and operating effectiveness of these controls throughout a specified period.

Can we use Type 2 SOC 2 reports when relying on internal controls at a service organization? [ISA | 3984.7263]

This type of report may be used as audit evidence if the system that is the subject matter of the report is relevant to the user entity's ICFR. Refer to Type 2 SOC 2 FAQs located on the Work Papers and Related Guidance page https://alex.kpmg.com/AROWeb/bridge/25081/27887?d=US,INTL on Alex (under "Related Guidance") for additional guidance.

What additional considerations are there if the entity outsources cloud computing? [ISA | 3984.13262]

When entities use service organizations for cloud computing, we treat them in the same way as any other service organization in our audit.

Due to the heightened risk that cloud computing can have on an entity's internal control over financial reporting, the involvement of specific team members with expertise in IT (IT Audit specific team members) is highly encouraged.

What is cloud computing? [ISA | 3984.13263]

Cloud computing is using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

Entities may hire cloud computing service organizations to provide and manage the entity's information technology capabilities.

What are some examples of cloud services? [ISA | 3984.13264]

Examples of cloud services include:

Cloud services	Description of services
Software as a Service	Provides software applications to the entity that reside on the cloud and not on the entity's hardware. An example of software as a service can be a service organization that provides human resource software applications, including payroll applications.
Platform as a Service	Provides the platform for the entity to develop and deploy cloud software applications which the entity owns and controls. An example of platform as a service can be a service organization that builds and supplies an IT environment on which the user entity can install their own applications and data sets.
Infrastructure as a Service	Provides the entity the ability to rent processing, storage, networks, and other computing resources where the entity controls the software application and operating systems. An example can be when a service organization offers storage solutions, e.g. data warehouse, to user organization to store their financial reporting information.

How do we identify if an entity uses cloud computing services? [ISA | 3984.13265]

We identify whether an entity uses a service organization to provide cloud computing services through gaining an understanding of their IT environment, which includes understanding the processes they use to identify cloud services being used throughout the entity and how they monitor when new cloud services are established.

Why do we identify whether the entity uses cloud computing services during the planning phase of our audit? [ISA | 3984.13266]

Cloud computing is becoming an important IT strategy for entities as this can be more cost effective, readily available and easily deployed throughout an entity. The following are some key characteristics of using cloud computing services that might be considered risks:

- Cloud services can result in significant changes to the entity's business processes and internal control over financial reporting
- Cloud environments being implemented with minimal involvement of the entity's IT department. Hence, the identification of whether an entity uses cloud services may be challenging to identify.
- Cloud computing service providers using multiple sub-service providers

- Software applications and data are easily transportable when using cloud services and may move back and forth between the cloud service provider's environment and those subservice providers environments.

Due to the risks that cloud computing can present and the impact to internal controls over financial reporting, we consider the following:

- As the identification of cloud computing services can be challenging, we obtain a robust understanding of the entity's control and governance processes over who at the entity is authorized to enter into arrangements with service providers
- Data migration from the entity's system to a cloud environment may occur outside of the entity's control environment. We obtain an understanding of how data is controlled and migrated to the cloud environment.
- We obtain an understanding of the cloud service arrangement and the impact to relevant process level controls and general IT controls to determine the nature, timing and extent of audit procedures to perform. The technology associated with cloud services may seem to simplify the management of IT, but it can add complexity to change management and configuration controls and can impact data integrity.
- We understand the flow of information and data to and from the service organization. The use of cloud computing involves the rapid movement of data which can result in less clarity about the flow of information and data.
- The cloud service provider may not provide a Type 1 or Type 2 SOC 1 report or may provide another attestation report not intended for internal control over financial reporting. If the cloud service provider does issue a Type 1 or Type 2 SOC 1 report, the report may carve-out a number of subservice organizations. This can impact our audit approach and how we plan to obtain sufficient audit evidence.
- Due to the ease of obtaining and changing cloud services, there is a greater risk of change during the gap period between the cloud service providers report date and the entity's reporting date, even if that gap period is short
- Cloud service providers may store the entity's data on servers in data centers located throughout the world. Hence, the entity considers compliance with local laws and regulations.

Due to the heightened risk that cloud computing can have on an entity's internal control over financial reporting, it is beneficial to have discussions with the entity early in the planning process. The involvement of specific team members with expertise in IT (IT Audit specific team members) is highly encouraged.

How might we determine whether the entity's use of a cloud computing service impacts the financial statements? [ISA | 3984.13267]

In addition to gaining an understanding of the entity's IT environment and business processes, we may be able to determine whether the entity's use of a cloud computing service impacts the entity's financial statements by asking management certain questions. It is particularly helpful to include specific team members with expertise in IT (IT Audit specific team members) in these inquiries.

The following are examples of the types of questions we can ask:

Review of cloud service arrangements	Has management reviewed the terms of each cloud service arrangement? Is there a process to review performance against contracts and service level agreements?
Risks associated with cloud computing	Have the risks associated with cloud computing arrangements been evaluated by management including the entity's Internal Audit department?
Impact to process level and IT controls	What has the entity done to understand the impact to relevant process level controls and general IT controls?
Understanding the relevant controls	Does the entity understand how the relevant controls impact the entity's internal control?
Retrieving relevant data	Is the entity able to retrieve data that may be relevant to the audit? For example, if the engagement team is planning on performing substantive analytical procedures to test relevant assertions related to revenue, can revenue data be retrieved by the entity?
Restrictions on data transfer	Are there any restrictions on data transfer? For example, if the data is located in a foreign country, are there restrictions on transferring data across borders?
Personally identifiable information	Does the entity understand how the service organization uses, retains and discloses personally identifiable information and other highly confidential information given that the entity's data, and the systems processing the data, may move from data center to data center around the world without the knowledge of the entity?
Future changes	How does the entity plan to monitor future changes to these processes given the easily changeable nature of cloud services?
Governance model for cloud enablement	Does the entity have a governance model that considers the decisions to be made and controls to be put in place for cloud enablement of business processes?

Updating existing internal control documentation	Has the entity updated its internal control documentation to reflect the new or changed business processes and general IT control processes?
Adequacy of monitoring and risk assessment controls	Has the entity assessed the impact of its use of cloud service providers on the adequacy of its monitoring and risk assessment controls and implemented new or revised controls?
Governance process over entering into arrangements	What governance process has the entity implemented to validate that only authorized personnel are able to enter into arrangements with a service organization given that cloud services may be procured outside the IT department, rapidly and usually without internal technology investment and deployment?
Compliance with local laws and regulations	Given that cloud service organizations may store the entity's data in data centers located in various jurisdictions around the world, has the entity considered compliance with local laws and regulations restricting the transfer of information across borders? Is data able to be obtained and recovered in a timely manner?
Skillset of IT personnel	Do the current IT personnel have the skillset to manage the implementation and daily interaction with and monitoring of the cloud service model? Will there be changes to the IT department? For example, will new IT resources be used, will there be retraining or will there be a reduction in headcount?
Controls over migration to the cloud	Has the entity considered controls over migration of its existing system to the 'cloud' environment?
Physical security over data	Where will the data be housed, and have physical security, access to servers and infrastructure been considered?
Skillset and capacity	Does the entity have the appropriate skillset and capacity to deal with secure connections for the volume of data and transactions being processed with the service providers?
Access to programs and data	Will access to the cloud based application be integrated with internal systems and therefore use internal logical access

	controls or be part of the cloud service provider's logical access controls? What changes will be made to access to programs and data controls both internally and at the service provider? For example, who will be granted super user access? Will other parties be provided access? How will user access be administered and will the cloud service provider provide security monitoring over logging and monitoring of access, including timely discovery, assessment, and reporting of breaches?
Program change controls	What changes will be made to program change controls? For example, will a web portal be set up to allow the entity's programmers to make changes to programs being hosted by the service provider?

2 Test the operating effectiveness of controls [ISA | 3986]

What do we do?

IF we plan to rely on the controls at a service organization, THEN obtain sufficient appropriate audit evidence over the operating effectiveness of controls.

Why do we do this?

In order for us to rely on the controls at the service organization, we obtain sufficient appropriate evidence about their operating effectiveness, including the operating effectiveness of the related CUECs and CSOCs in combination with our own procedures. Failing to do so could result in a lack of or insufficient evidence to support our audit opinion.

Execute the Audit

When do we test the operating effectiveness of controls related to service organizations? [ISA | 3986.1400]

Our decisions about testing operating effectiveness are made in the same way as those made about testing any other control relevant to the entity.

When we are performing an integrated audit, we review the Type 2 SOC 1 report to determine whether the relevant control are operating effectively to achieve the control objective and also decide whether we can place reliance on those control objectives in designing our substantive procedures. However, for a financial statement audit, we may decide not to place reliance on controls.

How do we test the operating effectiveness of internal controls related to a service organization? [ISA | 3986.1500]

When we decide to test the operating effectiveness of controls related to service organizations, we:

- Obtain evidence through one or more acceptable approaches

- Consider the extent of evidence provided by the Type 2 SOC 1 report
- Determine whether tests of controls are relevant and sufficient

In reaching our conclusions about the effectiveness of the controls related to service organizations (i.e., our ultimate assessment of control risk), we consider the totality of audit evidence we have obtained.

2.1 Obtain evidence through one or more acceptable approaches [ISA | 3987]

What do we do?

Obtain evidence over the operating effectiveness of controls at a service organization through one or more acceptable approaches.

Why do we do this?

In testing the operating effectiveness of controls related to service organizations, we obtain evidence about the operating effectiveness of controls at the service organization. The standards provide certain acceptable approaches for obtaining that evidence. Failing to use one or more of these specific approaches could result in a lack of or insufficient evidence to support our audit opinion.

Execute the Audit

How do we obtain evidence over the operating effectiveness of controls at a service organization? [ISA | 3987.1300]

We obtain audit evidence over the operating effectiveness of controls from one or more of the following procedures:

Approach	Further considerations when using approach
Obtain a Type 2 SOC 1 report	• A service organization may provide multiple services to the entity so we obtain a Type 2 SOC 1 report for each service the entity is using. • We cannot use a Type 1 SOC 1 as it does not provide evidence over the operating effectiveness of controls.
Test controls that the entity has implemented over the activities of the service organization	In order for this to be sufficient, the user entity maintains controls that operate at the appropriate level of precision, which address the same risks as the controls at the service organization (i.e., these controls can be duplicative to the controls at the service organization).

Test controls at the service organization ourselves or by using an other auditor	This may include obtaining an agreed-upon procedures or other relevant attestation report from an other auditor that includes tests of the operating effectiveness of the relevant controls. When using an other auditor, we perform the activities in the chapter on group audits (ISA 600 and AU-C 600) or we perform the activities in the chapter on part of the audit performed by other independent auditors (AS 1205)

What type of controls might an entity have in place over the service organization if a Type 2 SOC 1 report is not available or is not sufficient? [ISA | 3987.1400]

The entity may establish its own controls that are designed to address the process risk points related to the service organization's activities. These controls may be tested and enable us to place reliance on the entity's controls as opposed to controls at the service organization.

For example, if the entity uses a service organization to process its payroll transactions, the entity may:

- Establish reconciliation controls over the submission of payroll information to the service organization compared to the receipt of payroll information submitted back to the entity by the service organization, and
- Reperform the service organization's payroll calculations to validate their accuracy.

If the entity has appropriate controls in place covering each of the process risk points related to the service organization activities, we may perform tests of the operating effectiveness of the entity's controls over payroll processing as opposed to those controls at the service organization.

2.2 Consider the extent of evidence provided by the Type 2 SOC 1 report [ISA | 3988]

What do we do?

Consider the extent of evidence provided by the Type 2 SOC 1 report, including complementary user entity controls and use of subservice organizations.

Why do we do this?

We can use a Type 2 SOC 1 report as audit evidence that controls at the service organization are operating effectively, when that report provides sufficient appropriate audit evidence about the effectiveness of the controls to support our risk assessment. If not, we obtain evidence using a different approach. It is also important that management can make an independent assessment of their ICFR. Otherwise, we may fail to support our audit opinion.

Execute the Audit

What is a Type 2 service auditor's report? [ISA | 3988.13261]

A Type 2 service auditor's report provides an opinion about whether the controls at the service organization are appropriately designed and implemented to achieve the specified control objectives and whether they are operating effectively throughout a specified period of time.

What is a Type 2 SOC 1 report? [ISA | 3988.13527]

A Type 2 SOC 1 report is written documentation on the internal controls that are likely to be relevant to the user entities' internal control over financial reporting and includes the Type 2 service auditor's report. The Type 2 SOC 1 reports provides a description of the service organization's system, control objectives and the related controls that are tested to meet the control objective and whether they are operating effectively throughout a specified time period.

What sections of the Type 2 SOC 1 report are relevant to the audit? [ISA | 3988.13528]

Type 2 SOC 1 reports are issued under attestation standards issued by a relevant standard setting organization (e.g., AICPA, IASB, or others). The service auditor's report in a Type 2 SOC 1 provides an opinion about whether management's description fairly presents the system, whether the controls at the service organization are appropriately designed to achieve the specified control objectives and whether they are operating effectively throughout a specified period of time. The reports will generally follow a consistent format and provides information that can be used by auditors in planning and performing our audits.

A Type 2 SOC 1 report may contain the following sections:

- Independent Service Auditors Report (opinion)
- Management's Assertion
- Description of the System
- Control Objectives, Related Controls and Independent Service Auditor's Tests of Controls and Results of Tests
- Other Supplemental Information

The table below highlights some of the key information included within each section of the Type 2 SOC 1 report, and how we can use that information in our audit:

Information included in the SOC report	How we can use the information from the SOC report
Independent Service Auditors Report	
Identification of any information included in the document containing the report (opinion) that is not covered by the report.	Can help us understand what is included that is not being assessed by the service auditor. When we intend to rely on such information, we evaluate the impact of the service auditor excluding such information from the opinion/report, and consider whether it is necessary to perform alternative procedures.

Identification of any subservice organizations and whether the carve-out method or inclusive method was used.	We can use this information to identify subservice organizations, and whether or not the subservice organization is addressed through the carve-out or inclusive method. Use of the carve-out method indicates that another SOC 1 report assesses the sufficiency of controls and the operating effectiveness at the subservice organization.
A statement that the work was performed in accordance with the applicable attestation standards and the body establishing such standards.	Clarifies what attestation standards were applied in the performance of the procedures and ultimately provides us a basis for assessing the sufficiency of the standards under which the report was prepared.
The service auditor's opinion	Can help us determine that the opinion is consistent with our expectations and whether it provides assurance over the control objectives that are relevant to our audit. We also consider any qualifications or modifications to the opinion and their impact on our audit. This section also includes the description of the system that is included in the scope of the examination, the function of the system and the timing and the period tow which the description relates. This can help us understand the scope of the information that is being assessed by the service auditor and the relevant period.
Management's Assertion *	
Management's Assertion (* 'management' refers to management of the service organization)	Represents management's assertions regarding the information included in the report and may include: • the description of services in the report fairly presents how the system was designed to process user entity transactions • summary of changes to service organizations system during the period • management's assessment of the design and operation of controls This may also include other matters or indicate that some items have been omitted from the report. For example, it may state that certain control objectives are addressed in a different report that should be read in conjunction with the identified report.

	Management's assertion also represents service organization management acknowledging that they are responsible for the internal control at the service organization.
Description of the System	
Description of the System	Can help us understand the process and assess the sufficiency and relevance of controls at the service organization to the user entity.
Control Objectives, Related Controls and Independent Service Auditor's Tests of Controls and Results of Tests	
A list of control objectives	Control objectives included in the report are to cover a broad range of users of the report so some control objectives may or may not be relevant to our audit. We look to those control objectives that are relevant to our audit.
A summary of controls, including CEUCs to address each control objective	Allows us to draw a conclusion about whether the controls are appropriately responsive to the control objective.
A description of the service auditor's test procedures and results	Provides us information on how the controls were tested (i.e., nature) and whether a sample was selected or the entire population was selected (i.e., extent) along with any deviations. This information can be helpful as we evaluate whether the tests of controls are relevant and sufficient.
Deviations	Provides us information on deviations identified by the service auditor, the extent of testing that led to the identification of the exception (including the number of samples tested), and the number and nature of deviations identified. This information can be helpful as we evaluate whether the exceptions or deviations represent control deficiencies relevant to our audit.
Other supplemental information	
Other information	Service organization management may include other information, at their discretion, within this section of the report. Often additional information will be provided around exceptions and responses to exceptions, CUECs, or matters related to the scope of the report (for example, if management intends

	for a different SOC report to address a different set of risks not included in the report). This supplemental information may help us understand the information included in other sections of the report. However, this information is not covered by the service auditor's report, has not been subject to procedures applied in the service auditor's examination and they express no opinion on it so we cannot rely on Other Information provided by management of the service organization.

Do we focus on control objectives or the individual controls when evaluating the SOC report? [ISA | 3988.13529]

Ultimately, we focus on both. However, control objectives provide a good starting point to identify the areas of the SOC report where the controls are likely to be relevant to our audit. As a result, we may document the relevant control objectives from the SOC report in our audit documentation and the document the evaluation of individual controls within the control objective.

What if controls within a relevant control objective are not relevant? [ISA | 3988.13530]

When there are certain controls within a relevant control objective that are not relevant to the user entity, we identify those controls and document our rationale for why they are not relevant.

> For example, a user entity may know that the service organization processes their transactions using only system ABC. When a control objective includes controls over two different systems (e.g., system ABC and XYZ) and the service auditor tests separate controls specified by the service organization that are unique to each system, we may conclude that the controls that address system XYZ are not relevant to the audit.

However, service auditors generally consider the suite of the controls that are necessary to address each control objective in reaching their overall conclusions. Since we are less informed controls at the service organization than the service auditor, we think carefully about the controls before determining when one or more are not relevant as they may be a key part of how the ultimate control objective that is relevant to our audit is addressed.

In situations where we are unable to determine whether a related control within a relevant control objective is relevant to the user entity based on the information provided by the Type 2 SOC 1 report, we assume the control is relevant and the control is necessary for those controls that are directly responsive to risks at the user entity to operate effectively.

How do we obtain a Type 2 SOC 1 report? [ISA | 3988.1400]

We typically obtain a Type 2 SOC 1 report directly from the user entity, including those for relevant subservice organizations.

When the entity doesn't have a process in place to obtain the Type 2 SOC 1 report from their service organization, this may be an indicator of possible control deficiencies in their monitoring component of internal controls.

What if we obtain the Type 2 SOC 1 report from the service organization's website? [ISA | 3988.13531]

There may be instances in which we use the service organization's website to obtain the Type 2 SOC 1 report. When we do this, the service organization may request us to acknowledge non-reliance on the Type 2 SOC 1 report or commit the firm to indemnifications. We don't acknowledge either as this results in the report providing us no audit evidence and possibly commit the firm to indemnifications. If we will use the Type 2 SOC 1 report, we obtain the Type 2 SOC 1 report without restrictions.

Can management rely on a service auditor's report issued by KPMG when assessing internal controls over financial reporting? [ISA | 3988.13534]

Management can rely on a service auditor's report issued by KPMG, except when management engages KPMG to perform the SOC engagement and plans to rely on the SOC report for purposes of assessing ICFR.

How do we determine whether the Type 2 SOC 1 report provides sufficient evidence? [ISA | 3988.1500]

Ultimately, we read the entire Type 2 SOC 1 report and consider whether it provides enough information about the nature, timing and extent of the testwork performed to conclude that the relevant controls are operating effectively for purposes of our audit.

What if the service auditor or other auditor issues an agreed-upon procedures or other attestation report? [ISA | 3988.1600]

If an agreed-upon procedures or other attestation report is issued by the service auditor or another auditor, we determine whether the procedures performed are sufficient for our purposes by considering the following:

- Do the controls tested by the service auditor address the right process risk points and relevant assertions for the risks of material misstatement?
- Did the service auditor have sufficient sample sizes for control testwork?
- Is the nature, timing and extent of procedures sufficient for the control being tested?
- The impact to the control environment from any control deficiencies identified
- Performing inquiries over the service auditor's or other auditor's professional reputation, competence and independence

What if the service auditor issues an agreed-upon procedures report to specified parties? [ISA | 3988.13535]

If we plan to use an agreed-upon procedures report, we determine that the procedures are appropriate for our purpose.

If we are a specified party in a restricted use agreed-upon procedures report, we agree upon the procedures performed and determine whether the procedures performed are sufficient for our purposes. If we are not a specified party in a restricted use agreed-upon procedures report, we may request to be added as a specified party. When the report is restricted to specified parties and we are not one of those parties we may not use the report as audit evidence. When the report is not restricted to specified parties, we may use the report as audit evidence when we have determined that the procedures are appropriate for our purpose.

What are our responsibilities if the SOC 1 report contains CUECs? [ISA | 3988.1700]

For those control objectives that we plan to rely on, we also test the design and implementation and operating effectiveness of management's controls to address relevant complementary user entity controls (CUECs).

How do we determine which CUECs are relevant to the user entity? [ISA | 3988.13252]

The SOC 1 report may link CUECs directly to relevant control objectives. This helps aid our understanding of which CUECs relate to which control objectives.

Management is responsible for implementing controls that address each CUEC deemed necessary by the service organization for each relevant control objective, but how management implements controls to address each CUEC may vary. For example, if one relevant control objective has four associated CUECs, management may implement one process level control to address all four CUECs.

How do we test CUECs? [ISA | 3988.13538]

CUECs are controls at the entity that we test in the same manner as any other control.

Can we rely on a Type 2 SOC 1 report to obtain evidence that the information provided by the service organization is sufficiently relevant and reliable? [ISA | 3988.13539]

If the Type 2 SOC 1 report only has a general statement that the service auditor has tested controls over the accuracy and completeness of the information, we cannot simply rely on those controls.

Without the ability to determine what controls were tested by the service auditor over the accuracy and completeness of the information and the relevant data elements, we are assuming that proper testing was performed without any information on nature, timing and extent of procedures.

However, if the Type 2 SOC 1 report specifies which information they have tested for accuracy and completeness, then we can rely on those controls specific to that information.

What do we do if the Type 2 SOC 1 report does not specify that information used by management was tested for accuracy and completeness or we do not obtain a Type 2 SOC 1 report? [ISA | 3988.13540]

When the Type 2 SOC 1 report does not specify the information for which controls have been tested for accuracy and completeness or we do not obtain a Type 2 SOC 1 report, there may be other procedures we can perform, which may include a combination of:

- Requesting management to inquire of the service organization and/or service auditor to understand how the control objectives and related control activities included in the Type 2 SOC 1 report address the accuracy and completeness of the information, including the relevant data elements.
- Reviewing the control objectives and tests of controls performed by the service auditor to determine if the accuracy and completeness of relevant data elements in the information used by management are addressed by the control objective and tests of controls.
- Reviewing the control objectives to determine if the Type 2 SOC 1 report includes a control objective, control activities and tests of controls related to the accuracy and completeness of the output produced by the service organization.
- Reviewing the 'Management's Description' in the Type 2 SOC 1 report to determine if the information is specified as being produced for user entities.

- Inspecting the service level agreement between the service organization and the user entity to determine if the information is listed as part of the service organization's output delivered to the user entity

However, inquiry alone is not sufficient.

What other procedures can we perform if we determine that the Type 2 SOC 1 report does not provide evidence over the accuracy and completeness of information that is being used by management or we do not plan on using the Type 2 SOC 1 report to obtain evidence? [ISA | 3988.13542]

Other procedures we can perform include:

- Visiting the service organization and testing the relevant controls at the service organization
- Using the work of another auditor
- Testing the control activities that the user entity has implemented over the accuracy and completeness of the information
- Direct testing the information or using another auditor to perform these procedures. When direct testing, we perform the activities in the chapter on audit evidence (ISA 500, AU-C 500).

What resources are available to help us evaluate a SOC 1 report? [ISA | 3988.13543]

Member firms may have set up local centralized teams or offshore services to review Type 1 and Type 2 SOC 1 reports.

What are our responsibilities when we use centralized teams or offshore services? [ISA | 3988.8618]

Although centralized teams or offshore services provide assistance to the engagement team, we are still responsible for:

- Reading the entire SOC 1 report
- Understanding how the service organization is used by the entity
- Understanding the controls at the service organization that are relevant to the entity's internal control
- Testing the operating effectiveness of CUECs
- Identifying the relevant CSOCs and validating that they are operating effectively at the subservice organization.
- Reviewing their documentation in the workflow

2.3 Determine whether tests of controls are relevant and sufficient [ISA | 3989]

What do we do?

Determine whether the specific tests of controls and related results in the Type 2 SOC 1 report are relevant to the user entity AND whether the nature, timing and extent of such tests of controls are sufficient.

Why do we do this?

As Type 2 SOC 1 reports may be intended to satisfy the needs of many users, we determine whether the Type 2 SOC 1 report is relevant to the entity we audit. If the procedures performed in the Type 2 SOC 1 report do not sufficiently test the specific controls that impact the entity's internal controls over financial reporting, then we do not place reliance on the report and perform additional testwork.

Execute the Audit

How do we determine the relevance and sufficiency of the tests of controls in the service auditor's report to the entity? [ISA | 3989.1300]

We determine the relevance and sufficiency of the tests of controls in the Type 2 SOC 1 report by considering the following items:

- Whether the tests of controls and results are relevant to the assertions that are significant to the entity's financial statements
- Whether the results of relevant tests of controls in the Type 2 SOC 1 report provide audit evidence to support our risk assessment
- Whether relevant control deficiencies or a modified opinion impact our use of the service auditor's report

2.3.1 Determine whether controls and results are relevant to significant assertions [ISA | 3990]

What do we do?

Determine whether the tests of controls and results in the Type 2 SOC 1 report are relevant to the assertions that are significant in the user entity's financial statements.

Why do we do this?

When testing the operating effectiveness of controls at a service organization, we determine whether the test of controls are sufficient to the relevant assertions based on the entity specific RMMs and PRPs and if the testing is sufficient based on the nature, timing and extent of the procedures performed. Otherwise, we may not obtain sufficient evidence to support our audit opinion.

Execute the Audit

What do we consider when determining whether the test of controls and results are relevant to the assertions that are significant to the entity's financial statements? [ISA | 3990.1300]

We consider the following items when we determine whether the tests of controls and results are relevant to the assertions that are significant to the entity's financial statements

- Whether the nature and extent of relevant tests of controls provide sufficient appropriate evidence
- Whether the timing of relevant tests of controls provides sufficient appropriate evidence

Which assertions are significant to the entity's financial statements? [ISA | 3990.1400]

Those assertions we have identified as relevant assertions for a significant account or disclosure are considered significant to the entity's financial statements. They represent those assertions which have an associated risk of material misstatement.

2.3.1.1 Consider whether the nature and extent of relevant tests of controls provide sufficient appropriate evidence [ISA | 3991]

What do we do?

Consider whether the nature and extent of the relevant tests of controls and results in the Type 2 SOC 1 report provide sufficient appropriate evidence.

Why do we do this?

When we design and perform our procedures over the operating effectiveness of a control, we consider the risk associated with the control to be tested. As the risk increases, we obtain more persuasive audit evidence. The level of evidence can vary based on the nature and extent of procedures to be performed - so we evaluate the nature and extent of testing performed by the service auditor, to determine whether it is appropriately responsive to the risk related to the control.

Execute the Audit

What does the 'nature' of control procedures refer to? [ISA | 3991.1300]

Nature	The type of control evidence obtained.

What do we consider when evaluating the 'nature' of the control testing performed by the service auditor?

We consider the type of procedures applied by the service auditor, which should include procedures akin to the procedures we would perform in the testing of controls (inquiry, observation, inspection, reperformance).

What does the 'extent' refer to in the context of a service organization? [ISA | 3991.13582]

The extent of evidence refers to the quantity of evidence the service auditor obtains. While the Type 2 SOC 1 report does not necessarily disclose the number of sample items the service auditor has tested, the report does disclose whether the items tested represent all or a selection of the items in the population. The responsibility to select the appropriate sample size resides with the service auditor.

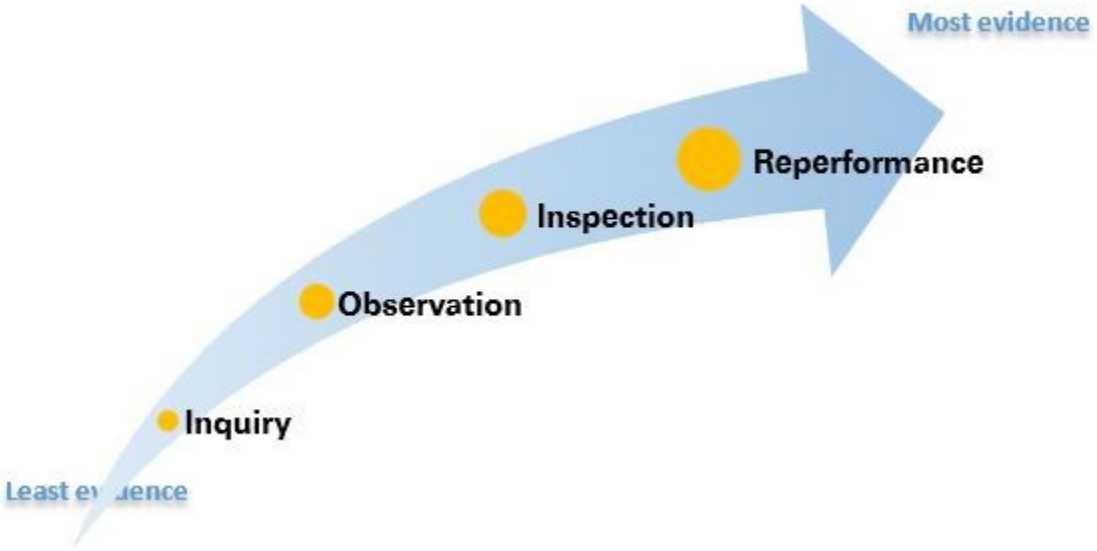
What do we consider when evaluating the 'extent' of the control testing performed by the service auditor?

The responsibility to select the appropriate sample size resides with the service auditor and should be based on their methodology. We consider if the extent of evidence is sufficient based on the sufficiency of controls selected for testing by the service auditor (e.g., if the service auditor tested

controls that appear to appropriately achieve the control objective) and if the method used to test the control is sufficient (e.g., if the service auditor tested the full population or a sample of items).

How might the nature of procedures vary when testing operating effectiveness? [ISA | 3991.1400]

The following diagram shows the different procedures we can perform to test the operating effectiveness of controls. The procedures are presented in order of the level of audit evidence they ordinarily provide, from least to most.



How do we determine whether the nature of tests of controls at the service organization is appropriate? [ISA | 3991.1600]

When determining whether the nature of tests of controls at the service organization is appropriate, we consider the level of risk (i.e., inherent risk) associated with the RMMs being addressed at the service organization. That level of risk informs us about the type, persuasiveness and the quantity of evidence.

Some types of tests, by their nature, produce greater evidence of the effectiveness of controls, such as reperformance, while others produce less evidence, such as inquiry.

When we evaluate the nature of tests of controls at the service organization, we may consider the service auditor's procedures and whether they are consistent with procedures we would have performed if we tested the control ourselves.

Is inquiry alone sufficient to test the operating effectiveness of a control?

No. Inquiry alone does not provide sufficient evidence. However, the responses to inquiries may point us toward other techniques - e.g. observation and inspection.

2.3.1.2 Consider whether the timing of relevant tests of controls provides sufficient appropriate audit evidence [ISA | 3992]

What do we do?

Consider whether the timing of the relevant tests of controls and results in the Type 2 SOC 1 report is appropriate.

Why do we do this?

When we place reliance on the controls at the service organization, the time period covered by the Type 2 SOC 1 report is a key aspect we consider. If the testing doesn't cover a sufficient period of time, we can't place reliance on the controls at the service organization without performing additional procedures.

Execute the Audit

What do we mean by the 'timing' of tests of controls? [ISA | 3992.1300]

The timing of the tests of controls refers to the time period or the date through which the controls were tested.

How do we determine whether the timing of tests of controls at the service organization is appropriate? [ISA | 3992.1400]

When determining whether the timing of test of controls at the service organization is appropriate, we look to the period covered by the service auditor's report as compared to the period of the financial statements to identify whether there is a gap period.

What is a gap period?

The gap period is the time between the date through which the controls were tested in the service auditor's report and the user entity's year-end (e.g. the time period of the entity's financial reporting period that is not covered by the service auditor's report).

> For example, the service auditor's report for payroll processing covers the period from October 1 to September 30 however the entity's financial reporting period is from January 1 to December 31. The gap period is from October 1 to December 31.

What do we do when we have a gap period? [ISA | 3992.1500]

When we have a gap period, whether significant or not, we understand whether there have been any significant changes to the controls at the service organization and any subservice organizations.

We may perform additional procedures to address the gap period, after considering:

- the significance of the activities of the service organization and subservice organizations,
- whether there are errors that have been identified in the service organization's or the subservice organization's processing,
- the significance of the gap period,
- the nature and significance of any changes to the controls at the service organization and subservice organization during the gap period; and
- the effectiveness of the control environment and monitoring controls at the user entity.

Although a key factor, the length of the gap is only one factor in determining its significance. A relatively short period of time could still be considered to be a significant gap when the activities of the service organization are significant.

How do we understand and assess changes during the gap period? [ISA | 3992.1600]

In order to understand whether there have been any significant changes to the controls at the service organization and any subservice organizations, we:

- perform inquiries of management to understand any changes to the controls at the service organization that they are aware of. This may include changes communicated to management from the service organization, changes in personnel at the service organization with whom management interacts, changes in reports or other data received from the service organization, changes in contracts or service level agreements with the service organization or errors identified in the service organization's processing,
- inquire of management whether a bridge letter is available and if so, obtain a copy
- discussing changes with service organization personnel
- evaluate whether the results of any of our other procedures indicate that there have been changes in the controls at the service organization. For example, while testing payroll transactions, we may identify that certain reports from the service organization dated after the service auditor's report date are different. This may indicate there may have been changes to the systems and/or controls of the service organization subsequent to the service auditor's report date.

What is a bridge letter?

A bridge letter, also known as a gap letter, is an unaudited letter the service organization and the subservice organization make available to user entities to identify and address any material changes to the internal control environment that have occurred during the gap period covered by the letter. The bridge letter provides audit evidence in the form of inquiry of the service organization and the subservice organization.

Generally, the gap in the period covered by the service auditor's report and the period under audit should not exceed four months if we intend to rely only on a bridge letter, which is consistent with the length of time conclusions on certain manual controls may be rolled forward based solely on inquiry.

What types of changes during the gap period might impact the procedures we perform?

Changes at the service organization during the gap period that could impact our procedures include:

- Changes related to the service organization's processes and information systems
- Changes in personnel at the service organization
- Changes in the design or implementation of controls to achieve the control objectives
- Changes in reports or other data received from the service organization
- Changes in contracts or service level agreements
- Errors identified in the service organization's processing

What drives us to obtain additional evidence over the operating effectiveness of controls at the service organization? [ISA | 3992.13494]

The following drives us to obtain additional evidence over the operating effectiveness of controls at the service organization:

- procedures performed by management and results,
- procedures performed by us and results; and
- specific risk factors.

When might other procedures performed by management or us and the results lead to obtaining additional evidence? [ISA | 3992.13495]

Management or we may perform procedures in which the results contradict the conclusions reached by the service auditor. Or management or we may perform procedures in which the results indicate either audit misstatements or deficiencies in the controls being performed by the service auditor. In either case, we determine what additional procedures to perform.

What specific risk factors do we consider? [ISA | 3992.13496]

We consider the following risk factors:

- The elapsed time between the time period covered by the tests of controls in the service auditor's report and the as of date
- The significance of the activities of the service organization
- Whether there are errors that have been identified in the service organization's processing
- The nature and significance of any changes in the service organization's controls identified by management or the auditor

When would risk factors lead us to obtain additional evidence over the gap period? [ISA | 3992.1700]

The following are indicators that additional evidence is needed:

Risk Factor	Indicators to obtain additional evidence over the gap period
The elapsed time between the time period covered by the tests of controls in the service auditor's report and the date of the financial statements	The length of the gap period is significant. When the gap period is greater than four months, it is significant and we ordinarily perform additional procedures.
The significance of the activities of the service organization	The activities at the service organization are significant to the user entity. For example: • material business processes are outsourced • the dollar value of accounts impacted by the service organization are multiple times materiality, and • the volume of transactions is large
Whether there are errors that have been identified in the	A high level of errors have been identified in the service organization's processing. A modified opinion was issued by the service auditor.

service organization's processing including any modifications to the service auditor's report	
The nature and significance of any changes in the service organization's controls identified by management or the auditor or noted in a bridge letter	There are significant changes in the service organization's controls, identified by us or the user entity or noted in a bridge letter.

What additional procedures might we perform over the gap period?

Additional procedures that we may perform over the gap period include:

- testing the process level and/or monitoring controls management has in place to address the gap period and not just rely on a bridge letter. The most effective manner to address the gap period is to determine how management addresses the gap period.
- relying on the entity's internal audit function visiting the service organization and testing operating effectiveness of the controls in the gap period, which we evaluate
- visiting the service organization, or engaging an other auditor, to test controls at the service organization during the gap period
- obtaining and evaluating any agreed upon procedures reports or other relevant attestation reports issued by the service auditor that address the gap period.

Each engagement is unique and many factors can impact the procedures we perform to address a gap period.

What if the service auditor's report does not cover any portion of the entity's financial reporting period? [ISA | 3992.1900]

If the service auditor's report does not cover any portion of the entity's financial reporting period under audit, we do not rely on the report.

In these instances, we use a different way to obtain audit evidence, such as:

- testing controls at the user entity, if they exist,
- testing controls directly at the service organization; or
- using another auditor to test controls directly at the service organization.

Can we use a bridge letter to obtain evidence over the gap period for CUECs? [ISA | 3992.2000]

No. CUECs are controls at the entity that we test in the same manner as any other control, including performing appropriate procedures over the rollforward period when we test them at an interim date. Obtaining a bridge letter from the service organization does not provide evidence of the operating effectiveness of CUECs.

2.3.2 Consider whether the results of relevant tests of controls provide sufficient appropriate evidence [ISA | 3993]

What do we do?

Consider whether the results of the relevant tests of controls in the Type 2 SOC 1 report provide sufficient appropriate audit evidence.

Why do we do this?

We consider the nature, timing and extent of evidence obtained from the service organization along with controls at the entity collectively to determine if we have sufficient appropriate audit evidence. If we do not look to the collective evidence, there is a risk that we reach the inappropriate conclusions.

Execute the Audit

How do we evaluate whether the results of the relevant tests of controls in the Type 2 SOC 1 report provide sufficient appropriate audit evidence? [ISA | 3993.1300]

We look to the collective evidence we have collected including the results of nature , timing and extent of such tests of controls to support our assessed level of control risk. We also consider the impact of any deficiencies identified in the Type 2 SOC 1 report, as well as the service auditor's opinion.

What do we do if we believe that the Type 2 SOC 1 report does not provide sufficient appropriate audit evidence? [ISA | 3993.13448]

If we believe that Type 2 SOC 1 report may not provide sufficient appropriate audit evidence, we may supplement the understanding of the service auditor's procedures and conclusions by contacting the service organization, through the user entity, to request a discussion with the service auditor about the scope and results of the service auditor's work.

If necessary, we may also contact the service organization, through the user entity, to request that the service auditor perform procedures at the service organization. Alternatively, we, or another auditor at our request, may perform such procedures.

2.3.3 Evaluate the impact of relevant control deficiencies and any modified opinion [ISA | 3994]

What do we do?

Evaluate the impact of relevant control deficiencies and modified opinion on our use of the service auditor's report.

Why do we do this?

Control deficiencies are present when a control does not operate consistently as designed, is not designed appropriately or is not implemented. Understanding the nature of control deficiencies, including a modified opinion in the service auditor's report, and its causes, can be helpful as we consider the effect of the control deficiencies, including a modified opinion, on our ability to use the service auditor's report and the related documentation. Because service organization activities and controls form part of the entity's processes and internal control over financial reporting, control deficiencies and issues with testing those controls can impact our audit approach and possibly our audit opinion.

Execute the Audit

What do we do if the Type 2 SOC 1 report identifies deviations or exceptions within a relevant control objective? [ISA | 3994.1300]

If a control within a relevant control objective is relevant and has deviations or exceptions, then we accumulate and evaluate these deviations or exceptions like we do other control deficiencies we come across in our audit and include them in the summary of internal control deficiencies (see activity 'Identify and evaluate control deficiencies' for further information). This is not necessary for those controls within a relevant control objective we previously determined were not relevant to the user entity.

How do we document our evaluation of a deviation or an exception identified by the service auditor within a relevant control objective when the relevant control objective was operating effectively as stated in the service auditor's opinion? [ISA | 3994.6314]

If there are controls within a relevant control objective that contain deviations or exceptions, we take each of the deviations or exceptions through the deficiency module. However, as the overall control objective was achieved, that means the service auditor was able to determine that the other relevant control(s) within the control objective operated at an appropriate level of precision to compensate for the risk(s) associated with the deviation(s) or exception(s).

What do we do when a control objective is not achieved and we want to place reliance on any of the related controls? [ISA | 3994.1400]

Although we may be able to rely on relevant controls within a failed control objective that did not contain deviations or exceptions, we expect these circumstances to be limited. Given the interplay of related controls within a control objective, we use caution in these situations since service auditors generally consider the suite of the controls that are necessary to address each control objective in reaching their overall conclusions. Since we are less informed about controls at the service organization than the service auditor, we think carefully before determining whether controls without deviations or exceptions can be relied upon as the controls with deviations or exceptions may be a key part of how the ultimate control objective that is relevant to our audit is addressed.

Consultation with DPP, and in the absence of a local DPP, the risk management partner, is encouraged.

Do we change the risk associated with the control for the CUECs impacted by control deficiencies? [ISA | 3994.1500]

It depends. Engagement teams will make an independent determination for any changes in the risk associated with the user entity's control for CUECs impacted by control deficiencies at the service organization.

What are management's responsibilities when there are deficiencies in the Type 2 SOC 1 report? [ISA | 3994.13423]

Because service organization activities and controls form part of the entity's processes and internal control over financial reporting, management's internal control over financial reporting considers internal controls at a service organization. This typically includes management reviewing Type 2 SOC 1 reports, identifying deficiencies in relevant control objectives and related controls and maintaining a process to mitigate the deficiencies, such as developing their own controls that respond to and address deficiencies noted in the Type 2 SOC 1 report.

What if the service auditor's report has a qualification or other modification? [ISA | 3994.13424]

If the service auditor's report has a qualification or other modification, we understand the reason for the modification to determine the impact to the entity or our audit approach. We may determine that we can still rely on the Type 2 SOC1 report.

Qualifications or other modifications that impact our ability to obtain audit evidence over relevant controls (e.g., the report qualifies that certain controls are not included that are relevant to entity) or could change our decisions in the audit (e.g., qualified opinion denoting controls that are relevant to the entity are not effective and therefore certain control objectives have not been achieved) could impact the entity and/or our audit approach. In some cases, management may have developed their own controls that respond to and address issues noted in the Type 2 SOC 1 report.

Qualifications or other modifications can be identified by reading the service auditor's report and having discussions with management and/or the service auditor.

3 Perform communications if we identify significant deficiencies [ISA | 4004]

What do we do?

IF we identify significant deficiencies when assessing a service organization's controls, THEN perform the communications in accordance with the auditing standards.

Why do we do this?

Communications with those charged with governance and management form an integral part of every audit. We perform these communication because they foster improved financial reporting, which benefits the investors.

Execute the Audit

What are the reasons the communications of control deficiencies matter? [ISA | 4004.1300]

There are several reasons for which our communications matter:

- Communicating control deficiencies to those charged with governance assists them in fulfilling their oversight responsibilities.
- Our communications with management recognize management's responsibility for the preparation and fair presentation of the financial statements, and for the design, implementation and operating effectiveness of internal controls.
- Our communications make management and those charged with governance aware of the entity's control deficiencies, which gives them a better chance to correct them. Improved financial reporting benefits the investors. This means that, ultimately, our communications improve the functioning of the capital markets.
- Communications with management and those charged with governance give them the opportunity to explain why the deficiencies occurred so that we are able to obtain additional information and expand our understanding of the deficiencies. The audit benefits from robust two-way communications with management and those charged with governance.
- Our communications enable management and those charged with governance to understand whether we, in our independent judgment, have reached conclusions that are similar to the conclusions that management reached about the severity of deficiencies that exist as of period-end.

How do we identify significant deficiencies from a Type 2 SOC 1 report? [ISA | 4004.1400]

The service auditor's report does not indicate whether a significant deficiency exists at the service organization. It is the responsibility of the user entity to read the Type 2 SOC 1 report to identify the control objectives at the service organization that have been not achieved and determine the impact to the entity's financial statements.

Management may reach out to the service organization to obtain additional information in making their assessment.

We include each exception or deviation from the SOC 1 report that is relevant to the entity as part of our deficiency assessment. These exceptions and deviations are treated the same as other deficiencies identified during our audit and are included in the summary of control deficiencies and communicated to the entity.

What communications do we make if we identify a significant deficiency? [ISA | 4004.1500]

We communicate all significant deficiencies to management and those charged with governance on a timely basis. When communicating significant deficiencies we perform the activities in the chapter on communicating control deficiencies (AS 1305 , ISA 265 , AU-C 265).

What deficiencies in the Type 2 SOC 1 report do we assess? [ISA | 4004.1600]

As part of our deficiency assessment, we include each deficiency included in the Type 2 SOC 1 report that is relevant to the entity. Relevant deficiencies identified in a Type 2 SOC 1 report are treated the same as other deficiencies identified during our audit and are included in the summary of control deficiencies and communicated to the entity. We and the entity assess the impact to both the financial statement audit and ICFR.

What else do we consider communicating with the entity and those charged with governance related to our reliance on the Type 2 SOC 1 report? [ISA | 4004.1700]

We consider communicating the following matters to the entity and those charged with governance:

- Implementation of monitoring controls by the entity
- Instances where CUECs were not implemented by the entity
- Controls that may be necessary at the service organization that have not been implemented

Type 1 and Type 2 Reports That Exclude the Services of a Subservice Organization

International Standards on Auditing: ISA 402.18

Type 1 and Type 2 Reports that Exclude the Services of a Subservice Organization

18. If the user auditor plans to use a type 1 or a type 2 report that excludes the services provided by a subservice organization and those services are relevant to the audit of the user entity's financial statements, the user auditor shall apply the requirements of this ISA with respect to the services provided by the subservice organization. (Ref: Para. A40)

ISA Application and Other Explanatory Material: ISA 402.A40

Type 1 and Type 2 Reports that Exclude the Services of a Subservice Organization (Ref: Para. 18)

A40. If a service organization uses a subservice organization, the service auditor's report may either include or exclude the subservice organization's relevant control objectives and related controls in the service organization's description of its system and in the scope of the service auditor's engagement. These two methods of reporting are known as the inclusive method and the carve-out method, respectively. If the type 1 or type 2 report excludes the controls at a subservice organization, and the services provided by the subservice organization are relevant to the audit of the user entity's financial statements, the user auditor is required to apply the requirements of this ISA in respect of the subservice organization. The nature and extent of work to be performed by the user auditor regarding the services provided by a subservice organization depend on the nature and significance of those services to the user entity and the relevance of those services to the audit. The application of the requirement in paragraph 9 assists the user auditor in determining the effect of the subservice organization and the nature and extent of work to be performed.

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Understand how the user entity uses service and subservice organizations [ISA | 3983]

What do we do?

Obtain an understanding of how a user entity uses the services of a service organization, including any subservice organizations

Why do we do this?

Obtaining an understanding over how the entity uses service organizations, including any subservice organizations, allows us to identify key information for risk assessment, including all five components of the entity's internal control.

Service organizations can offer multiple services; however, the user entity may only use a portion of the services offered by the service organization. As a result, we understand which services are being used by the user entity.

Execute the Audit

What do we obtain an understanding over when a user entity uses a service organization? [ISA | 3983.1300]

When a user entity uses a service organization, we obtain an understanding over:

- the nature of the services provided by the service organization and the significance of those services to the user organization, including their effect on the user organization's internal control
- the nature and materiality of the transactions processed or accounts or financial reporting processes affected by the service organization
- the degree of interaction between the activities of the service organization and those of the user organization, and
- the nature of the relationship between the user organization and the service organization, including the relevant contractual terms for the activities undertaken by the service organization.

How do we obtain an understanding of the nature and significance of services? [ISA | 3983.1400]

We may use a variety of sources of information to help us understand the nature and significance of the services provided by the service organization including:

- user manuals
- system overviews
- technical manuals
- the contract or service level agreement between the entity and the service organization showing the services to be provided
- reports by service auditors, internal auditors or regulatory authorities on controls at the service organization
- System and Organization Control (SOC) reports
- visit the service organization
- inquiring of management

We may also be able to leverage the knowledge we obtained through past experience with the service organization, including prior year SOC reports, particularly if the services and controls at the service organization over those services are highly standardized.

How do we obtain an understanding of the nature and materiality of transactions? [ISA | 3983.13246]

Our understanding of the process can provide insight into the transactions processed by the service organization.

We think about the quantitative and qualitative aspects of the transactions processed and the accounts or financial reporting processes affected by the service organization. The nature of the transactions processed and the accounts affected by the service organization may not be quantitatively material, but may still be significant based on the nature of those transactions or accounts.

How do we obtain an understanding of the degree of interaction? [ISA | 3983.13247]

Our understanding of the process can provide insight into the degree of interaction between the service organization and the user entity.

What is 'degree of interaction'? [ISA | 3983.13244]

Degree of interaction is the extent to which the user organization is involved in the process to initiate, execute, process and record transaction that flow through the service organization.

A high degree of interaction exists when the user entity authorizes transactions and the service organization processes and accounts for those transactions. In this case, the user entity may be able to implement effective process-level controls over those transactions.

When there is a high degree of interaction, we may consider controls at the user entity to address the risks inherent in using the service organization. We determine the appropriateness of the design and implementation of those controls to conclude whether or not all risks have been mitigated to a sufficiently low level.

A low degree of interaction exists when the service organization initiates or initially records, processes, and accounts for the entity's transactions. In this case, the user entity may not be able to practically implement effective process-level controls.

How do we obtain an understanding of the nature of the relationship? [ISA | 3983.1700]

We may obtain an understanding of the nature of the relationship, including the relevant contractual terms for the activities undertaken by the service organization, by reviewing the contract or service level agreement between the user entity and the service organization. Relevant sections of the service level agreement can highlight factors, such as:

- the scope of services provided by the service organization
- whether the service organization provides a Type 1 or Type 2 SOC 1 report
- the information the service organization agrees to provide to the user entity
- defined responsibilities for initiating transactions relating to the activities performed by the service organization and information to be provided by the user entity
- the application of regulatory requirements concerning the form of records to be maintained, or access to them
- clauses that require the service organization to maintain internal control over financial reporting consistent with a recognized framework (e.g., COSO 2013)
- the indemnification, if any, the service organization will provide to the user entity in the event of a performance failure on the part of the service organization.
- terms that govern the resolution of any errors identified in the processing of transactions or other data

- clauses that require timely communication of identified discrepancies
- whether the user auditor has rights of access to the accounting records of the entity maintained by the service organization and other information relevant to the conduct of the audit,
- whether the agreement allows for direct communication between the user auditor and the service auditor
- terms that govern the timing of SOC 1 reporting and/or access to the service auditor
- acceptable deviation rates (if any)
- clauses that may impact how the user entity designs complementary user entity controls (CUECs) (e.g., clauses that limit the service organization's responsibility for errors)
- clauses that may impact how the user entity monitors the controls at the service organization

We may also corroborate this understanding by having discussions with the user entity and considering any other information from the service organization (e.g., user manuals, service guides, service organization provided training modules, etc.).

What is a subservice organization? [ISA | 3983.1800]

A subservice organization is an organization that a service organization uses to perform some of the services provided to the user entity. These services may also be relevant to the user entities' internal control over financial reporting. A subservice organization may be a separate entity from the service organization or may be related to the service organization.

We could also think of subservice organizations as the entities that service organizations outsource some of their operations to.

Service auditors will identify these subservice organizations in the SOC 1 reports.

When is a subservice organization relevant to the entity's internal controls over financial reporting? [ISA | 3983.1900]

Just like a service organization, a subservice organization is relevant to the entity's internal controls over financial reporting when those services, and the related controls, are part of the user entity's information system, including the IT environment relevant to financial reporting (see activity 'Understand information and communication' for further information on obtaining an understanding information and communication). This is the case when they affect any of the following:

- The classes of transactions, account balances, and disclosures in the entity's operations that are significant to the entity's financial statements
- The procedures, both automated (within IT) and manual, by which the entity's transactions are initiated, recorded, processed, and reported from their occurrence to their inclusion in the financial statements
- The related accounting records, whether electronic or manual, supporting information, and specific accounts in the entity's financial statements involved in initiating, recording, processing and reporting the entity's transactions
- How the entity's information system captures other events and conditions that are significant to the financial statements
- The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures

What are our responsibilities over subservice organizations? [ISA | 3983.13248]

When a service organization uses a subservice organization, we treat these subservice organizations the same as other service organizations.

We include the activities performed by the subservice organization in our understanding of the processes and controls at the user entity. In the end, we obtain sufficient information about the types of transactions that the subservice organization processes, the materiality of those transactions and the ultimate impact to the user entity's financial statements arising from those transactions. Understanding the activities performed by the subservice organization may identify additional RMMs which we then address in our audit.

How will the SOC 1 report inform a user entity that relevant controls are in place at a subservice organization? [ISA | 3983.13245]

When a service organization uses a subservice organization, the service auditor will identify the subservice organizations that may be relevant within the SOC 1 report. The servicer auditor may use either the inclusive method or the carve-out method.

Inclusive method	When the service auditor *includes* the subservice organization's relevant control objectives and related controls in the service organization's description of its system and the scope of the service auditor's engagement.
Carve-out method	When the service auditor *excludes* the subservice organization's relevant control objectives and related controls in the service organization's description of its system and the scope of the service auditor's engagement.

Fraud, Non-Compliance with Laws and Regulations, and Uncorrected Misstatements in Relation to Activities at a Service Organization

International Standards on Auditing: ISA 402.19

Fraud, Non-Compliance with Laws and Regulations, and Uncorrected Misstatements in Relation to Activities at the Service Organization

19. The user auditor shall inquire of management of the user entity whether the service organization has reported to the user entity, or whether the user entity is otherwise aware of, any fraud, non-compliance

with laws and regulations or uncorrected misstatements affecting the financial statements of the user entity. The user auditor shall evaluate how such matters affect the nature, timing and extent of the user auditor's further audit procedures, including the effect on the user auditor's conclusions and user auditor's report. (Ref: Para. A41)

ISA Application and Other Explanatory Material: ISA 402.A41

Fraud, Non-Compliance with Laws and Regulations, and Uncorrected Misstatements in Relation to Activities at the Service Organization (Ref: Para. 19)

A41. A service organization may be required under the terms of the contract with user entities to disclose to affected user entities any fraud, non-compliance with laws and regulations or uncorrected misstatements attributable to the service organization's management or employees. As required by paragraph 19, the user auditor makes inquiries of the user entity management regarding whether the service organization has reported any such matters and evaluates whether any matters reported by the service organization affect the nature, timing and extent of the user auditor's further audit procedures. In certain circumstances, the user auditor may require additional information to perform this evaluation, and may request the user entity to contact the service organization to obtain the necessary information.

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Inquire about items that could impact the financial statements [ISA | 3997]

What do we do?

Inquire of the user entity's management whether they are aware of any uncorrected misstatements, fraud and non-compliance with laws and regulations, including illegal acts, that could impact the financial statements.

Why do we do this?

If we plan to place reliance on the SOC 1 report, we obtain an understanding of whether the entity is aware of any fraud, non-compliance with laws and regulations, including illegal acts, and uncorrected misstatements that could impact the entity's financial statements. These can be communicated to the entity by the service organization or may become known to the entity some other way.

If we cannot place reliance on the SOC 1 report, there could be changes in our audit plan and audit execution.

Execute the Audit

What do we do if we become aware of uncorrected misstatements, fraud or non-compliance with laws and regulations, including illegal acts through inquiries of the entity? [ISA | 3997.1300]

After we obtain a clear understanding of the uncorrected misstatements, fraud, non-compliance with laws and regulations, including illegal acts, occurring at the service organization, we determine the impact on our audit. This may involve further discussions with both the entity as well as the service organization.

What is the impact to the audit when there are uncorrected misstatements, actual or suspected fraud or non-compliance with laws and regulations, including illegal acts that impact the entity? [ISA | 3997.1400]

The impacts on our audit may include:

- identifying a new risk of material misstatement in addition to the ones identified in our risk assessment process,
- modifying a risk of material misstatement we previously identified,
- no longer planning to rely on the relevant controls at the service organization which can impact the nature, timing and extent of audit procedures,
- considering what management has done to address these issues and whether they implemented any compensating controls at the entity, or
- modifying our auditor's report

See the chapters on fraud (ISA 240 , AU-C 240 , AS 2401), laws and regulations (ISA 250 , AU-C 250 , AS 2405) and evaluating misstatements (ISA 450 , AU-C 450 , AS 2810) for further information.

Reporting by the User Auditor

International Standards on Auditing: ISA 402.20-22

Reporting by the User Auditor

20. The user auditor shall modify the opinion in the user auditor's report in accordance with ISA 705 (Revised)[5] if the user auditor is unable to obtain sufficient appropriate audit evidence regarding the services provided by the service organization relevant to the audit of the user entity's financial statements. (Ref: Para. A42)

---

5 ISA 705 (Revised), *Modifications to the Opinion in the Independent Auditor's Report,* paragraph 6

21. The user auditor shall not refer to the work of a service auditor in the user auditor's report containing an unmodified opinion unless required by law or regulation to do so. If such reference is required by law or regulation, the user auditor's report shall indicate that the reference does not diminish the user auditor's responsibility for the audit opinion. (Ref: Para. A43)

22. If reference to the work of a service auditor is relevant to an understanding of a modification to the user auditor's opinion, the user auditor's report shall indicate that such reference does not diminish the user auditor's responsibility for that opinion. (Ref: Para. A44)

ISA Application and Other Explanatory Material: ISA 402.A42-A44

Reporting by the User Auditor (Ref: Para. 20)

A42. When a user auditor is unable to obtain sufficient appropriate audit evidence regarding the services provided by the service organization relevant to the audit of the user entity's financial statements, a limitation on the scope of the audit exists. This may be the case when:

- The user auditor is unable to obtain a sufficient understanding of the services provided by the service organization and does not have a basis for the identification and assessment of the risks of material misstatement;
- A user auditor's risk assessment includes an expectation that controls at the service organization are operating effectively and the user auditor is unable to obtain sufficient appropriate audit evidence about the operating effectiveness of these controls; or
- Sufficient appropriate audit evidence is only available from records held at the service organization, and the user auditor is unable to obtain direct access to these records.

Whether the user auditor expresses a qualified opinion or disclaims an opinion depends on the user auditor's conclusion as to whether the possible effects on the financial statements are material or pervasive.

Reference to the Work of a Service Auditor (Ref: Para. 21-22)

A43. In some cases, law or regulation may require a reference to the work of a service auditor in the user auditor's report, for example, for the purposes of transparency in the public sector. In such circumstances, the user auditor may need the consent of the service auditor before making such a reference.

A44. The fact that a user entity uses a service organization does not alter the user auditor's responsibility under ISAs to obtain sufficient appropriate audit evidence to afford a reasonable basis to support the user auditor's opinion. Therefore, the user auditor does not make reference to the service auditor's report as a basis, in part, for the user auditor's opinion on the user entity's financial statements. However, when the user auditor expresses a modified opinion because of a modified opinion in a service auditor's report, the user auditor is not precluded from referring to the service auditor's report if such reference assists in explaining the reason for the user auditor's modified opinion. In such circumstances, the user auditor may need the consent of the service auditor before making such a reference.

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Do not refer to the service auditor's report in our audit opinion [ISA | 4006]

What do we do?

Do not make reference to service auditor's report as a basis, in part, for our opinion on the user entity's financial statements unless required by law or regulation.

Why do we do this?

Although we can use the SOC 1 report as part of our audit evidence, the service auditor is not responsible for examining any portion of the entity's financial statements as of any specific date or for any specific period. This creates a division of responsibility for both the audit of the financial statements as well as the audit over internal controls over financial reporting.

The fact that an entity uses a service organization does not diminish or alter our responsibility to obtain sufficient appropriate audit evidence to provide a reasonable basis to support our auditors' opinion. Therefore, we do not refer to the service auditor in our opinions on the financial statements or internal control over financial reporting.

Execute the Audit

Are there exceptions in which we can refer to the service auditor in our audit opinion? [ISA | 4006.1300]

Yes. We can refer to the service auditor in our audit opinion if:

- the reference to the work of the service auditor is relevant to understanding our modified opinion, or
- we are required by law or regulation.

In these situations, we also indicate that such reference does not diminish our responsibility for that opinion.

What if we refer to the service auditor's report in our audit opinion?

If we refer to the service auditor's report in our audit opinion on the financial statements, we obtain the consent from the service auditor before making such reference in our opinion.

2 Determine whether we sufficiently understand how the entity uses the service organization [ISA | 3985]

What do we do?

Determine whether we have obtained a sufficient understanding of the nature and significance of the services provided by the service organization

Why do we do this?

Obtaining a sufficient understanding of the services provided by the service organization allows us to effectively identify process risk points and identify risks of material misstatements.

Execute the Audit

How do we determine whether we have obtained a sufficient understanding of the nature and significance of the services provided by the service organization? [ISA | 3985.1300]

We have obtained a sufficient understanding when we have a complete understanding of how transactions are initiated, authorized, processed and recorded.