CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

FAQ for Auditors: Service Organizations – When and How to Apply CAS 402

CANADIAN AUDITING STANDARDS (CAS)

MAY 2024

Auditing financial statements of an entity using a third-party organization

DISCLAIMER

This FAQ is intended to assist auditors in the application of Canadian Auditing Standard (CAS) 402, *Audit Considerations Relating to an Entity Using a Service Organization* but is not intended to be a substitute for reading the standard itself. It does not address all requirements in CAS 402 and focuses only on selected requirements. Note that CAS 402 expands on the requirements in CAS 315, *Identifying and Assessing the Risks of Material Misstatement* and CAS 330, *The Auditor's Response to Assessed Risks*.

Background

In today's complex business environment, entities are increasingly outsourcing certain business activities to third-party organizations, which could impact the auditor's assessment of the risks of material misstatement.

The Canadian Public Accountability Board (CPAB) identified in its March 2023 **Regulatory Oversight Report** the increase in range of business activities that are being outsourced by reporting issuers to service organizations as part of its 2022 annual inspection period. The report noted that, "in many instances, third-party service providers are involved in running a significant portion of the reporting issuer's operations, processing transactions or holding assets." Inspection findings noted that auditors did not always obtain a sufficient understanding of the services provided by third-party organizations and their effect on the reporting issuer's internal controls. This understanding is needed to ensure risks of material misstatement are identified, assessed, and appropriately addressed.

24-3386

Although CPAB's report is focused on audits of reporting issuers, entities of all sizes and complexity are increasingly outsourcing business functions or activities to third-party organizations. As business processes evolve, services performed by third-party organizations may not always be as simple as those services traditionally performed, such as payroll services or custody of traditional assets. Further, third-party organizations may not be as sophisticated; their system of internal controls may be less mature, including the design, implementation, and operation of appropriate controls within that system. In November 2023, CPAB released examples of **observed findings** related to audits of entities using service organizations, highlighting these challenges and the importance of a tailored audit response.

All auditors need to be aware of this changing landscape and the impact of an entity's use of third-party service organizations on the audit of their financial statements.

Purpose

The purpose of this FAQ is to assist auditors of financial statements in:

- evaluating whether a third-party organization is considered a service organization as per CAS 402
- understanding the requirements of CAS 402, if a service organization is identified, for example, obtaining 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 in accordance with CAS 315; and
  - design and perform audit procedures responsive to those risks in accordance with CAS 330
- discussing the implications of using third-party organizations with management, as described in the **Appendix: Audit Client Briefing**

Important considerations in using this FAQ

This FAQ:

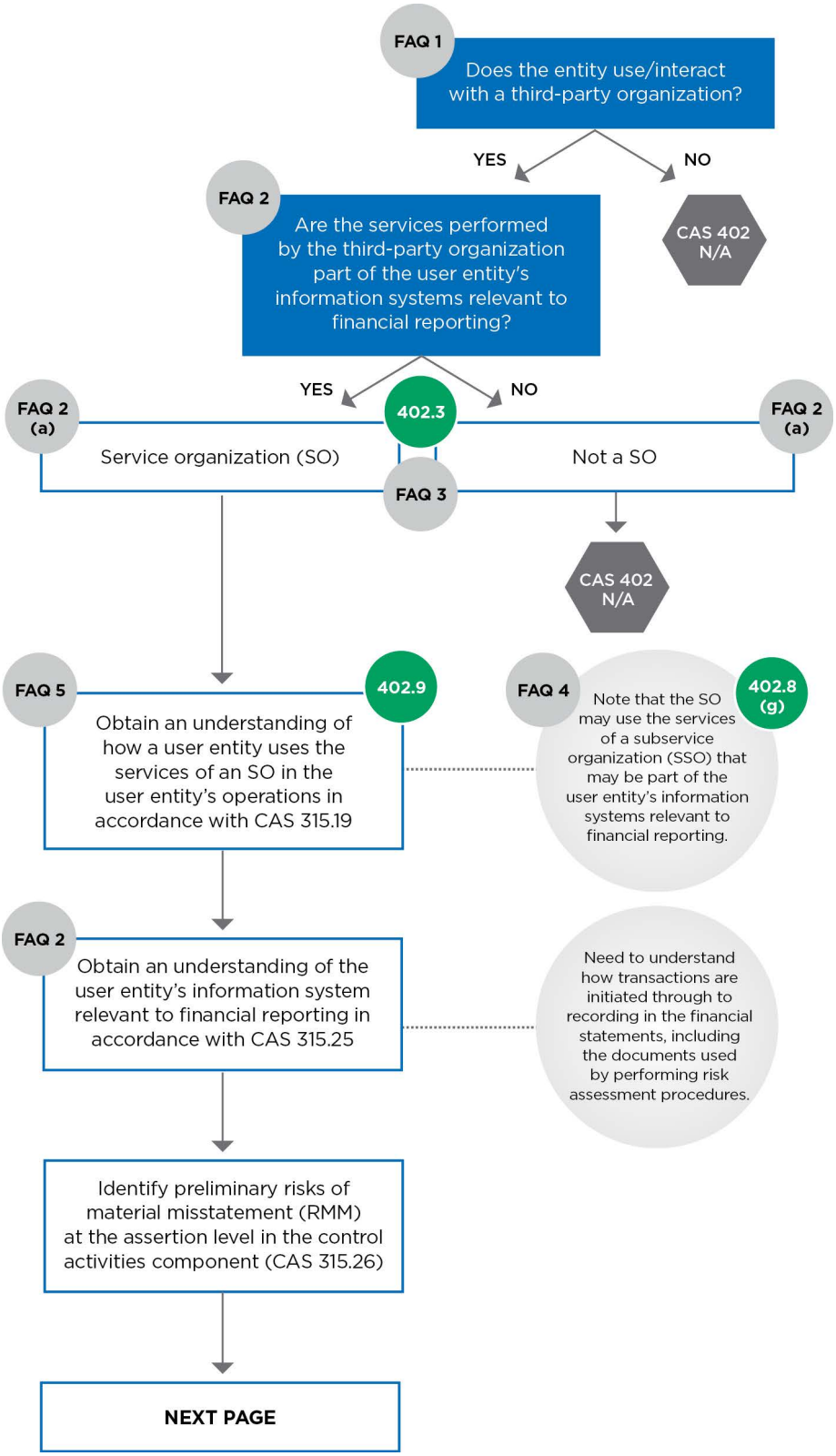
- provides an overview of steps and questions to consider when evaluating third-party organizations and service organizations as defined by CAS 402
- provides an overview of key requirements of CAS 402 in a flowchart format, with the FAQ reference number added to the flowchart (see below) for ease of navigation
- addresses matters when applying the standard that may require clarity and is not all-encompassing
- provides a "tear-away" appendix (**Audit Client Briefing**) that auditors may use to help facilitate discussions with management regarding service organizations and the requirements of CAS 402

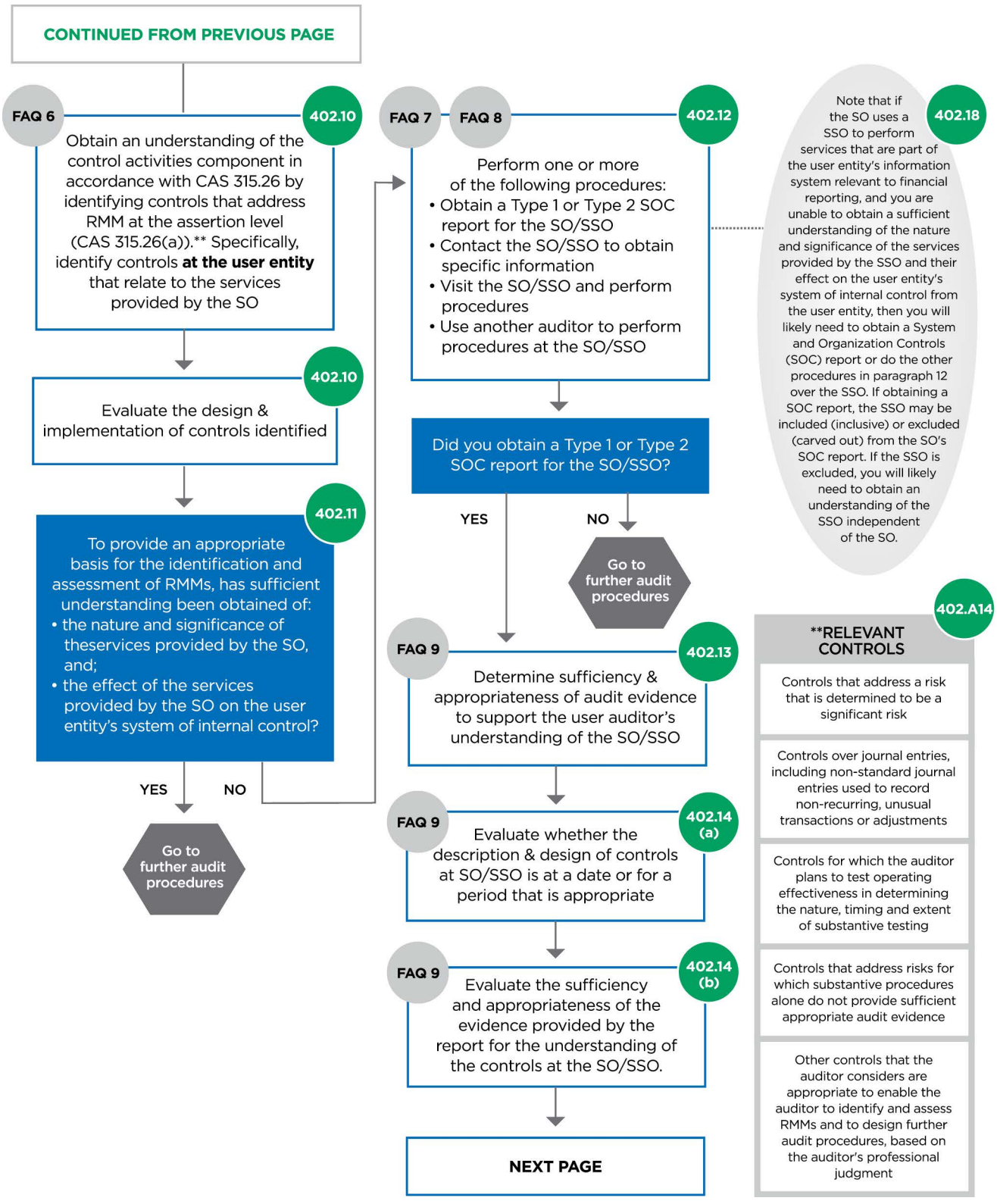
Note: This FAQ does not replace the need to read the entire CAS 402, CAS 315 or CAS 330, including application and other explanatory material.

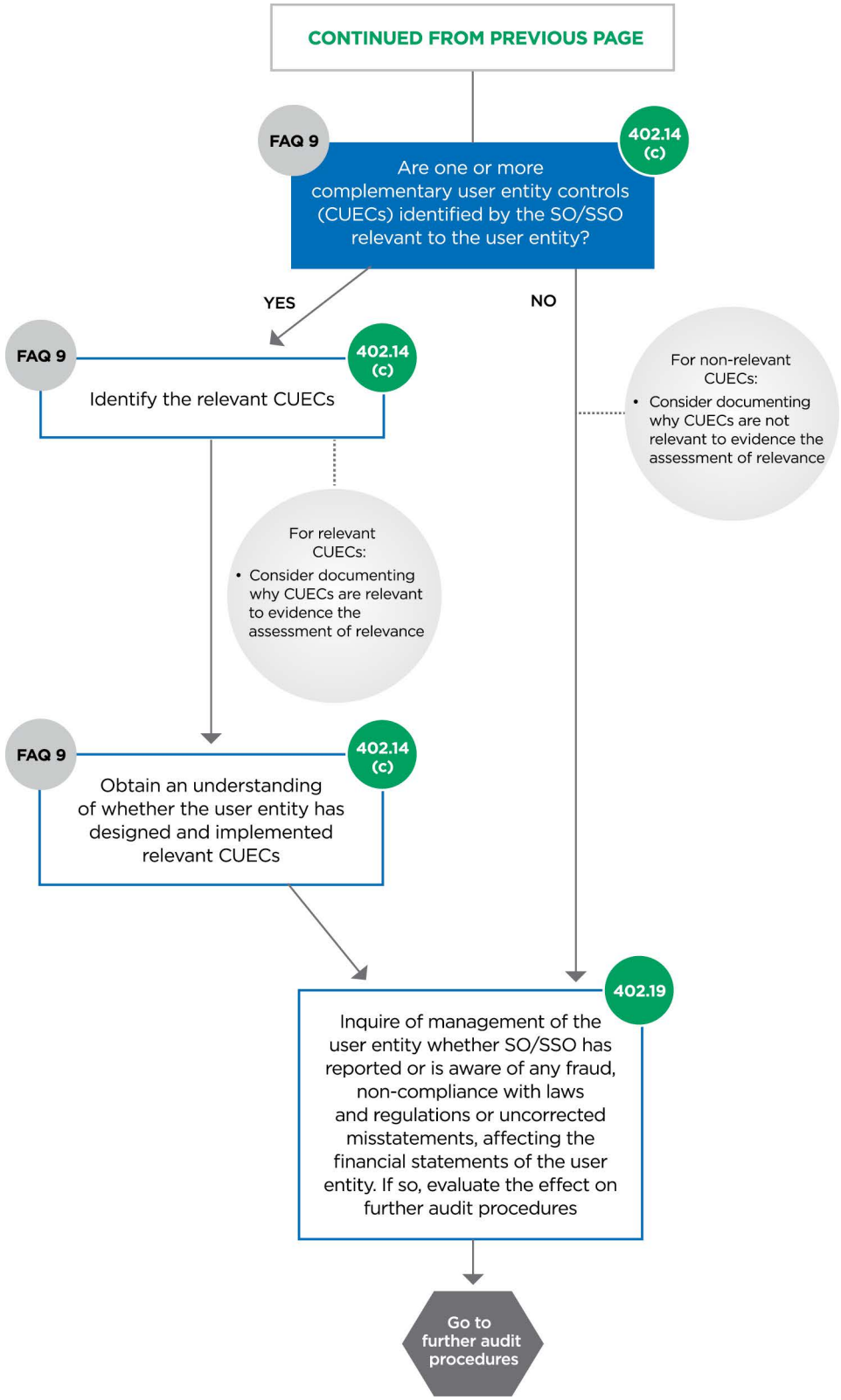
Questions Addressed in this FAQ

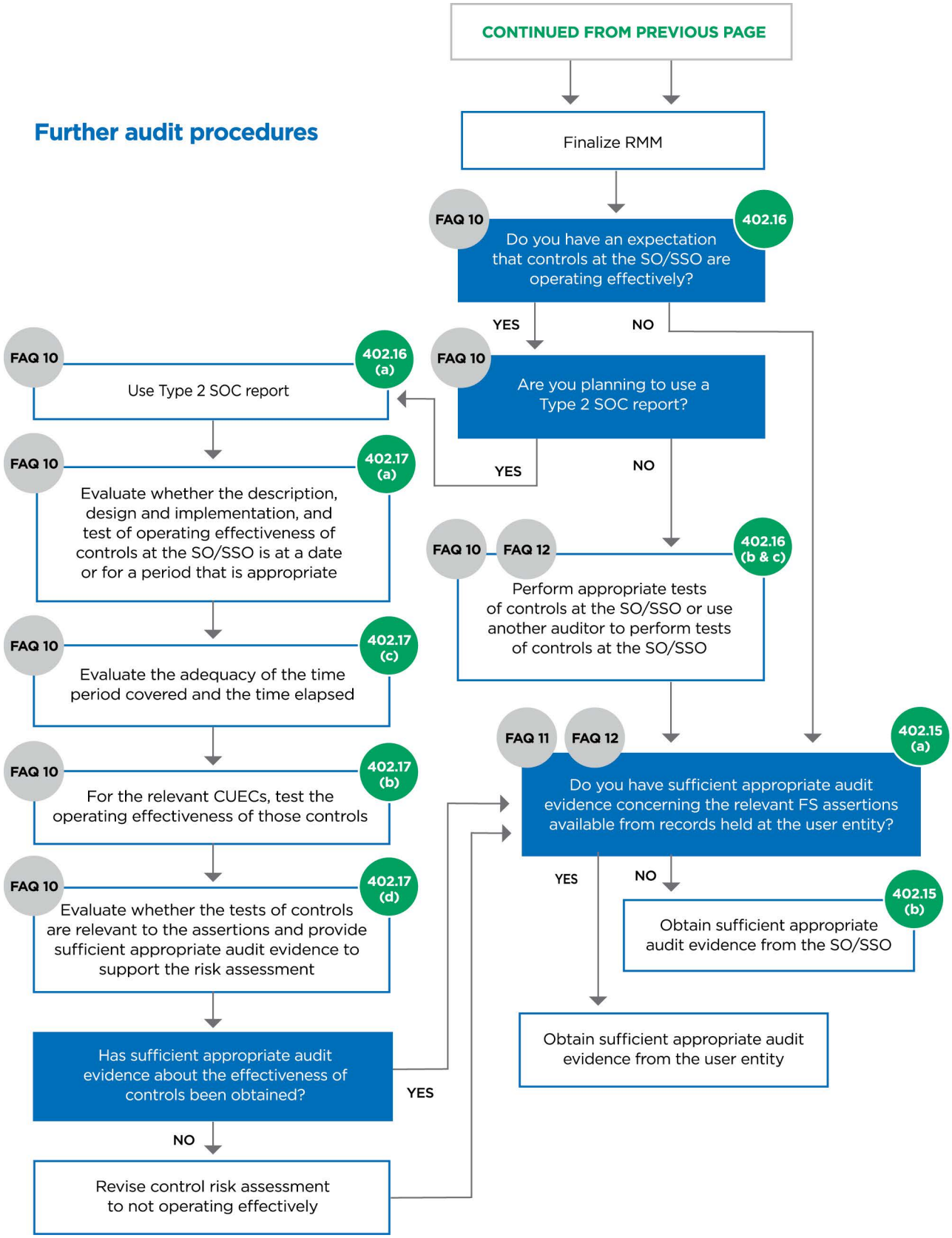
Flowchart: CAS 402 Requirements

The flowchart below can be used as a navigation tool for this FAQ. It can also be used to help auditors walk through an entity's circumstances to determine the applicability of CAS 402, and if so, how best to meet the applicable requirements. Professional judgment needs to be exercised during all aspects of the audit including when identifying and evaluating third-party organizations and whether they meet the definition of a service organization as per CAS 402.


FAQ 1
Does the entity use/interact with a third-party organization?
YES
NO
CAS 402 N/A
FAQ 2
Are the services performed by the third-party organization part of the user entity's information systems relevant to financial reporting?
YES
NO
FAQ 2 (a)
402.3
FAQ 2 (a)
Service organization (SO)
Not a SO
FAQ 3
CAS 402 N/A
FAQ 5
402.9
Obtain an understanding of how a user entity uses the services of an SO in the user entity's operations in accordance with CAS 315.19
FAQ 4
402.8 (g)
Note that the SO may use the services of a subservice organization (SSO) that may be part of the user entity's information systems relevant to financial reporting.
FAQ 2
Obtain an understanding of the user entity's information system relevant to financial reporting in accordance with CAS 315.25
Need to understand how transactions are initiated through to recording in the financial statements, including the documents used by performing risk assessment procedures.
Identify preliminary risks of material misstatement (RMM) at the assertion level in the control activities component (CAS 315.26)
NEXT PAGE


CONTINUED FROM PREVIOUS PAGE
FAQ 6
402.10
Obtain an understanding of the control activities component in accordance with CAS 315.26 by identifying controls that address RMM at the assertion level (CAS 315.26(a)).** Specifically, identify controls at the user entity that relate to the services provided by the SO
402.10
Evaluate the design & implementation of controls identified
402.11
To provide an appropriate basis for the identification and assessment of RMMs, has sufficient understanding been obtained of:
• the nature and significance of theservices provided by the SO, and;
• the effect of the services provided by the SO on the user entity's system of internal control?
YES
NO
Go to further audit procedures
FAQ 7
FAQ 8
402.12
Perform one or more of the following procedures:
• Obtain a Type 1 or Type 2 SOC report for the SO/SSO
• Contact the SO/SSO to obtain specific information
• Visit the SO/SSO and perform procedures
• Use another auditor to perform procedures at the SO/SSO
Did you obtain a Type 1 or Type 2 SOC report for the SO/SSO?
YES
NO
Go to further audit procedures
FAQ 9
402.13
Determine sufficiency & appropriateness of audit evidence to support the user auditor's understanding of the SO/SSO
FAQ 9
402.14 (a)
Evaluate whether the description & design of controls at SO/SSO is at a date or for a period that is appropriate
FAQ 9
402.14 (b)
Evaluate the sufficiency and appropriateness of the evidence provided by the report for the understanding of the controls at the SO/SSO.
NEXT PAGE
Note that if the SO uses a SSO to perform services that are part of the user entity's information system relevant to financial reporting, and you are unable to obtain a sufficient understanding of the nature and significance of the services provided by the SSO and their effect on the user entity's system of internal control from the user entity, then you will likely need to obtain a System and Organization Controls (SOC) report or do the other procedures in paragraph 12 over the SSO. If obtaining a SOC report, the SSO may be included (inclusive) or excluded (carved out) from the SO's SOC report. If the SSO is excluded, you will likely need to obtain an understanding of the SSO independent of the SO.
402.18
402.A14
**RELEVANT CONTROLS
Controls that address a risk that is determined to be a significant risk
Controls over journal entries, including non-standard journal entries used to record non-recurring, unusual transactions or adjustments
Controls for which the auditor plans to test operating effectiveness in determining the nature, timing and extent of substantive testing
Controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence
Other controls that the auditor considers are appropriate to enable the auditor to identify and assess RMMs and to design further audit procedures, based on the auditor's professional judgment


CONTINUED FROM PREVIOUS PAGE
FAQ 9
402.14 (c)
Are one or more complementary user entity controls (CUECs) identified by the SO/SSO relevant to the user entity?
YES
NO
FAQ 9
402.14 (c)
Identify the relevant CUECs
For non-relevant CUECs:
• Consider documenting why CUECs are not relevant to evidence the assessment of relevance
For relevant CUECs:
• Consider documenting why CUECs are relevant to evidence the assessment of relevance
FAQ 9
402.14 (c)
Obtain an understanding of whether the user entity has designed and implemented relevant CUECs
402.19
Inquire of management of the user entity whether SO/SSO has reported or is aware of any fraud, non-compliance with laws and regulations or uncorrected misstatements, affecting the financial statements of the user entity. If so, evaluate the effect on further audit procedures
Go to further audit procedures


CONTINUED FROM PREVIOUS PAGE
Further audit procedures
Finalize RMM
FAQ 10
402.16
Do you have an expectation that controls at the SO/SSO are operating effectively?
YES
NO
FAQ 10
Are you planning to use a Type 2 SOC report?
YES
NO
FAQ 10
402.16 (a)
Use Type 2 SOC report
FAQ 10
402.17 (a)
Evaluate whether the description, design and implementation, and test of operating effectiveness of controls at the SO/SSO is at a date or for a period that is appropriate
FAQ 10
402.17 (c)
Evaluate the adequacy of the time period covered and the time elapsed
FAQ 10
402.17 (b)
For the relevant CUECs, test the operating effectiveness of those controls
FAQ 10
402.17 (d)
Evaluate whether the tests of controls are relevant to the assertions and provide sufficient appropriate audit evidence to support the risk assessment
Has sufficient appropriate audit evidence about the effectiveness of controls been obtained?
YES
NO
Revise control risk assessment to not operating effectively
FAQ 10
FAQ 12
402.16 (b & c)
Perform appropriate tests of controls at the SO/SSO or use another auditor to perform tests of controls at the SO/SSO
FAQ 11
FAQ 12
402.15 (a)
Do you have sufficient appropriate audit evidence concerning the relevant FS assertions available from records held at the user entity?
YES
NO
402.15 (b)
Obtain sufficient appropriate audit evidence from the SO/SSO
Obtain sufficient appropriate audit evidence from the user entity

FAQ 1 – Does the entity use/interact with a third-party organization?

It is important for the auditor to ask sufficient questions and request appropriate documentation (see below for examples) in order to obtain an understanding of the entity and identify any relationships the entity has with third-party organizations.

CAS 315, *Identifying and Assessing the Risks of Material Misstatement*, requires the auditor to perform risk assessment procedures to obtain an understanding of the entity and its environment:

- Paragraph 19(a)(i): includes an understanding of the entity's organizational structure, ownership and governance, and its **business model**, including the extent to which the business model integrates the use of information technology (IT).
- Paragraph 25(a)(iv): requires the auditor to obtain an understanding of the entity's resources, including the IT environment, used in the entity's information processing activities. The information processing activities may use information from and/or send information to third-party organizations.
- Paragraph A23: provides examples of inquiries that auditors may perform including inquiries directed to the risk management function (which may help to identify any additional third-party organization) and inquiries directed towards in-house legal counsel (which may help to identify arrangements with business partners, such as third-party service agreements or contracts).
- Paragraph A34: provides examples of risk assessment procedures which may identify engagement of third-party organizations, such as the observation or inspection of internal documents (e.g., business plans, strategies, records, internal control manuals, meeting minutes, etc.). Auditors can also inquire about any new or updated third-party service agreements or contracts.[1]
- Appendix 1: explains the objectives and scope of the entity's business model and provides examples of matters that the auditor may consider in understanding the activities of the entity that may be included in the business model. Further, obtaining an understanding of the entity's business model/vendor/third-party risk management process may help to identify any additional third-party organizations that the entity interacts with.

Gaining this understanding of the entity and its environment, along with an understanding of how information flows through the entity's information system relevant to the preparation of the financial statements, may help you identify any third-party organization that the entity engages with.

There are many examples of services that entities may outsource to third-party organizations. Some common examples include:

- employee benefits administration and services
- health insurance claims processing
- point-of-sale processing
- data management and repository services

1 CAS 402, paragraph A1

- custodian or investment management services[2]
- application services
- cloud services

Note the above is not an exhaustive list as examples may vary from entity to entity; the examples listed are services from third-party organizations and may or may not be considered service organizations as defined by CAS 402, depending on the facts and circumstances of the relationship. Given their understanding of the entity, auditors may use their professional judgment and the flowchart above to help identify which third-party organizations are service organizations as defined by CAS 402.

FAQ 2 – What is a service organization? What is a user entity?

CAS 402 defines a **service organization as a third-party organization (or segment of a third-party organization) that provides services to a user entity that are part of that user entity's information systems relevant to financial reporting**[3] (see **FAQ 2(a)**). **A user entity is an entity that uses a service organization and whose financial statements are being audited**.

A third-party organization may be considered a service organization to one entity and not to another depending on how the user entity interacts with them and the services they perform. An entity may interact with service organizations, and indirectly with subservice organizations (see **FAQ 4**).

There may be elements of judgment in assessing whether a third-party organization is a service organization based on the specific facts and circumstances of the user entity.

Note that paragraph 5 of CAS 402 specifically excludes 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, CAS 402 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.

NOTE:

All service organizations are third-party organizations, but not all third-party organizations are service organizations! This FAQ uses the term "third-party organization" for any third-party that provides services to a user entity and "service organization" where a third-party organization is also a service organization as defined by CAS 402. Where a reference is made to a third-party organization that is not also considered a service organization as defined by CAS 402, it will be noted as such.

2 See CAS 402, paragraph 5 for services that are not in scope of CAS 402.

3 CAS 315 paragraph 25 uses the terminology "relevant to the preparation of the financial statements" to describe this. This paper uses terminology from CAS 402.

FAQ 2(a) – What does "*the user entity's information system relevant to financial reporting*" refer to?

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 financial reporting.

Paragraph 25 of CAS 315 requires the auditor to obtain an understanding of the entity's information system and communication relevant to the preparation of the financial statements, through performing risk assessment procedures. This understanding will help the auditor identify when services provided by a third-party organization are part of an entity's information system relevant to financial reporting (as outlined by paragraph 3 of CAS 402).

For more information on obtaining an understanding of the IT environment, see CPA Canada's FAQ CAS 315 and the Auditor's Responsibilities for General IT Controls.

The auditor's understanding of the information system includes understanding the policies that define flows of information relating to the entity's significant classes of transactions, account balances and disclosures, and other related aspects of the entity's information processing activities. This information, and the information obtained from the auditor's evaluation of the information system may confirm or further influence the auditor's expectations about the significant classes of transactions, account balances and disclosures initially identified.

Moreover, if the services provided by the third-party organization impact any of the areas discussed in the **table (a-d) below**, then those services are relevant to financial reporting. However, if you conclude that no service organization relationship exists (and therefore CAS 402 is not applicable under the circumstances), the requirements of CAS 315 still apply, as appropriate, to the services provided by the third-party organization, for identifying and assessing risks of material misstatement in the related assertions for the significant class of transactions, account balance or disclosure.

REQ.	CAS 315	CAS 402
Paragraph	Per **CAS 315.25**, the auditor shall obtain an understanding of the entity's information system and communication relevant to the preparation of the financial statements, through performing risk assessment procedures, by:	Per **CAS 402.3**, a service organization's services are part of a user entity's information system(s) relevant to the preparation of the financial statements if the services affect any of the following:
(i)/(a)	understanding the entity's information processing activities (including its data and information), the resources to be used in such activities and the policies that define for **significant classes of transactions, account balances and disclosures**: (i) how information flows through the entity's information system, including how: (a) transactions 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 (b) information about events or conditions, other than transactions, is captured, processed and disclosed by the user entity in the financial statements	how information relating to **significant classes of transactions, account balances and disclosures** flows through the user entity's information system, whether manually or using information technology (IT), and whether it is 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
(ii)/(b)	the accounting records, specific accounts in the financial statements and other supporting records relating to the flows of information in the information system;	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);

REQ.	CAS 315	CAS 402
(iii)/(c)	the financial reporting process used to prepare the entity's financial statements including disclosures; and	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 accounting estimates relating to significant classes of transactions, account balances and disclosures; and
(iv)/(d)	the entity's resources, including IT environment, relevant to (a)(i) to (a)(iii).	the entity's IT environment relevant to a) through c).

Paragraph 15 in Appendix 3 of CAS 315 states that the information system relevant to the preparation of the financial statements consists of activities and policies, and accounting and supporting records, designed and established to:

- initiate, record and process entity transactions (as well as to capture, process and disclose information about events and conditions other than transactions) and to maintain accountability for the related assets, liabilities and equity;
- resolve incorrect processing of transactions, for example, automated suspense files and procedures followed to clear suspense items out on a timely basis;
- process and account for system overrides or bypasses to controls;
- incorporate information from transaction processing in the general ledger (e.g., transferring of accumulated transactions from a subsidiary ledger);
- capture and process information relevant to the preparation of the financial statements for events and conditions other than transactions, such as the depreciation and amortization of assets and changes in the recoverability of assets; and
- ensure information required to be disclosed by the applicable financial reporting framework is accumulated, recorded, processed, summarized and appropriately reported in the financial statements.

An entity's business processes include the activities designed to:

- develop, purchase, produce, sell and distribute an entity's products and services;
- ensure compliance with laws and regulations; and
- record information, including accounting and financial reporting information

Business processes result in the transactions that are recorded, processed and reported by the information system.[4]

4 CAS 315, Appendix 3 paragraph 16

FAQ 3 – What is an example of a difference between the services of a service organization and a third-party organization that is not considered a service organization?

For service organizations, the information and transactions generally flow both ways, like a "two-way street" (i.e., to and from). Service organizations can be used by many user entities; however, the information is likely specific to each individual user entity. Examples of services provided by a service organization include:

- maintenance of the user entity's accounting records
- management of assets
- initiating, recording or processing transactions as agent of the user entity[5]

For third-party organizations that are not considered service organizations, the information is an external information source that generally flows one way, like a "one-way street" (i.e., from). Information provided by third-party organizations can be used by several different entities, and is therefore not entity specific. Some examples of third-party organizations include:

- Bloomberg
- Bank of Canada CPI Index
- real estate prices suitable for a broad range of users

As stated previously, auditors should use professional judgment in assessing whether a third-party organization is a service organization based on the specific facts and circumstances of the user entity.

FAQ 4 – What is a subservice organization?

CAS 402.8(g) defines a **subservice organization as 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**.

Subservice organizations may perform limited to extensive functions on behalf of the service organization. A common scenario may be when a service organization (e.g., Service Org. XYZ) uses another service organization (e.g., Service Org. ABC) for cloud computing infrastructure to store and process the data of the user entity. This other service organization (Service Org. ABC) is therefore a subservice organization to the service organization (Service Org. XYZ).

5 CAS 402 paragraph A4

FAQ 5 – How do you obtain an understanding of how a user entity uses the services of a service organization in the user entity's operations?

When obtaining an understanding of the entity in accordance with CAS 315, paragraph 9 of CAS 402 requires the auditor to obtain an understanding of how a user entity uses the services of a service organization in its operations, including:

- 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;
- the nature and materiality of the transactions processed, or the 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 entity (e.g., directing and monitoring versus autonomy – does the user entity have the ability to understand, assess and potentially influence the controls implemented by the service organization or not?); and
- 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.

FAQ 6 – What controls do you identify and how do you evaluate the design and implementation of those controls?

CAS 315 paragraph 26(a) requires the auditor to identify relevant controls that address risks of material misstatement at the assertion level in the control activities component (see **relevant controls** outlined in flowchart). When the auditor considers that identifying "other controls" are appropriate to enable the auditor to identify and assess risk of material misstatements, paragraph A165 of CAS 315 indicates that these controls may include complementary user entity controls (see **FAQ 9**), if using a service organization. This decision is based on the auditor's professional judgment.

Paragraph 10 of CAS 402 states that when obtaining an understanding of the user entity's system of internal control in accordance with CAS 315, the auditor shall identify controls in the control activities component 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 for the **user entity**, and evaluate their design and determine whether they have been implemented.

The auditor is required to evaluate design and implementation of relevant controls regardless of whether they plan on testing their operating effectiveness.[6] It is important to note that this applies to all relevant controls, whether performed internally at the user entity or by the service organization(s).

6 CAS 315, paragraph A125

Remember that, to determine whether controls have been suitably designed and implemented, you must perform procedures in addition to inquiry of the user entity's personnel. You may consider using a combination of inquiry, observation and inspection, as inquiry alone is not sufficient for such purposes.[7]

To evaluate the design and implementation of controls at the user entity that relate to the services provided by the service organization (or subservice organization), you may first consider whether you're able to obtain sufficient appropriate audit evidence from the user entity alone. If you're unable to, then the auditor may perform further audit procedures to obtain sufficient appropriate audit evidence or use another auditor to perform those procedures at the service organization on their behalf (see **FAQ 12**).

If using another auditor to perform those procedures at the service organization on the auditor's behalf, a common way this can be achieved is through a SOC assurance engagement completed by a service auditor.[8] This type of engagement provides a report on certain controls at a service organization. (see **FAQ 7**)

FAQ 7 – What are System and Organization Controls (SOC) reports?

SOC reports are assurance reports issued by practitioners (service auditors) who are engaged directly by the service organization to conduct a SOC assurance engagement. There are several types of SOC assurance engagements (e.g., SOC 1, SOC 2, etc.) and each is designed for a specific purpose and for different users. Depending on the type of report, it may assist the auditor in obtaining an understanding of:

- 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
- 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
- the control objectives at the service organization that are relevant to the entity's financial statement assertions
- whether controls at the service organization are suitably designed and implemented to prevent or detect processing errors that could result in material misstatements in the user entity's financial statements
- the IT environment used by the service organization in processing significant transactions

7 CAS 315, paragraph A177

8 A service auditor: an auditor who, at the request of the service organization, provides an assurance report on the controls of a service organization. A user auditor: an auditor who audits and reports on the financial statements of a user entity.

SOC 1 engagements are typically more relevant to you as the auditor, as they address the controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting. SOC 1 engagements are performed in accordance with the Canadian Standard on Assurance Engagement (CSAE) 3416, *Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting*.

A **SOC 2** engagement is related to controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy and may also provide additional relevant information related to aspects of the IT environment, depending on the scope of the SOC engagement. However, a SOC 2 report on its own will likely not provide the evidence the auditor needs to meet the requirements of CAS 402. SOC 2 engagements are performed in accordance with CSAE 3000, Attestation Engagements Other Than Audits or Reviews of Historical Financial Information and use the Trust Services Criteria, a set of criteria established by the American Institute of Certified Public Accountants (AICPA) Assurance Services Executive Committee. It is important to highlight that the risks and corresponding controls covered in a SOC 2 report may not be designed, implemented or tested with the specific focus on addressing the user entity's internal controls over financial reporting and therefore may not be relevant for the audit.

In some cases, IT controls related to the applications that support the business process controls in a SOC 1 report may be part of a separate SOC report (e.g., SOC 2 report). Therefore, careful consideration of the nature of the control objectives covered by each SOC report is important. Further, it is management's responsibility to obtain and review the SOC report and provide it to the auditor. A SOC report may or may not be available or appropriate to meet your needs.

FAQ 8 – What types of SOC reports are available?

There are two **types** of reports available for each SOC 1 or SOC 2 report:

- A **type 1** report is a report on the description and design of controls at a service organization and provides evidence of whether controls have been designed effectively and implemented at a **point in time**. This type of report is more commonly used to help determine the significance and understanding of the controls of the service organization.
- A **type 2** report is a report on the description, design and operating effectiveness of controls at a service organization and provides evidence of whether controls have been designed effectively, implemented and are **operating effectively throughout the period covered by the report**. This type of report would more commonly fit your needs when your expectation is that controls are operating effectively (see **FAQ 10**), and this will form the basis of your assessment of control risk.[9]

A type 1 report does not provide any evidence of the operating effectiveness of controls.

9 CAS 315, paragraph A226

In situations where one or more subservice organizations are used by the service organization and are part of the user entity's information systems relevant to financial reporting, 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 organization(s). 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 important factors for the auditor to consider in determining the significance of the services of the service organization and subservice organization to the user entity.[10]

In situations where one or more subservice organizations are used, the 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 part of the information system relevant to the preparation of the financial statements, you are required to apply the requirements of CAS 402 in respect of the subservice organization.[11] This may include obtaining the SOC report for the subservice organization.

FAQ 9 – If a SOC report is available, what are some considerations if you plan to use it as audit evidence?

The auditor needs to determine that the audit evidence provided by a SOC report is sufficient and appropriate to support their understanding of the service organization / subservice organization. In doing this, paragraph 13 of CAS 402 requires the auditor to be satisfied as to:

- the service auditor's professional competence and independence from the service organization; and
- the adequacy of the standards under which the type 1 or type 2 report was issued.

If the auditor plans to use the SOC report as audit evidence to support their understanding about the design and implementation of controls at the service organization, paragraph 14 of CAS 402 requires the auditor to evaluate the following:

10 CAS 402, paragraph A20

11 CAS 402, paragraph A40.

REQUIREMENT (CAS 402 PARAGRAPH 14)	CONSIDERATIONS / EXAMPLES
Is the description and design of controls at the service organization at a date or for a period that is appropriate for the user auditor's purposes?	• The report may cover periods by calendar-year (i.e., January 1, 201X to December 31, 201X), whereas the user entity's financial statements under audit may be for an off calendar-year period (i.e., May 1, 201X to June 30, 202X). See **FAQ 11**.
Is the evidence provided by the report sufficient and appropriate for the understanding of the controls at the service organization?	• Consider whether the control objectives address the identified risks of material misstatement. • Consider if the report addresses the controls at the service organization that are likely to be part of the user entity's information system relevant to financial reporting. If not, then you may need to consider changing your approach. • Consider whether there may be exceptions or deviations noted that, while not impacting the overall SOC report opinion, may impact the assessment you perform as the auditor.
Are **complementary user entity controls** (CUEC) identified by the service organization relevant to the user entity? If yes, did you obtain an understanding of whether the user entity has designed and implemented those controls?	• CUECs are 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. • Consider CUECs that are relevant to the control objectives in relation to the user entity's information system relevant to financial reporting. • If you determine that one or more CUECs are relevant (i.e., as per the control objectives discussed above), obtain an understanding of whether the user entity has designed and implemented such controls. Obtaining an understanding of whether the user entity has designed and implemented such CUECs does not require you, the auditor to evaluate their design or implementation, unless such CUECs meet the requirements in CAS 315.26(a). • If you determine that one or more CUECs are not relevant, you may consider documenting why they are not relevant such that it would enable an experienced auditor, having no previous connection to the audit, to understand why they are not relevant.

By evaluating the above, the auditor may determine that controls (those at the service organization and CUECs) are suitably designed to address the risks of material misstatement at the assertion level.

FAQ 10 – What are the implications when your risk assessment includes an expectation that controls at the service organization / subservice organization are operating effectively?

Paragraph 16 of CAS 402 states that when the auditor's risk assessment includes an expectation that controls at the service organization are operating effectively, the 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.

As stated in FAQ 10, a type 2 report is a report on the description, design and operating effectiveness of controls at a service organization and provides evidence of whether controls have been designed effectively, implemented and are operating effectively throughout the period covered by the report. If you plan to use a type 2 report as audit evidence that controls at the service organization (or subservice organization) are operating effectively, CAS 402 paragraph 17 requires that the user auditor 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.

If a type 2 report is **not** available, CAS 402 paragraph A30 states you 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 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.

A type 2 report is generally the most common and effective way to obtain audit evidence when your risk assessment includes an expectation that controls at the service organization / subservice organization are operating effectively. For this reason, as part of the auditor's client acceptance and continuance procedures, consider obtaining an understanding of the service organizations / subservice organizations the entity uses and whether type 2 reports are available.[12] See **FAQ 12** for more information on when a SOC report is not available or does not meet your needs.

FAQ 11 – What if a type 2 report is available, but does not cover the period under audit?

As type 2 SOC reports need to be available in a timely manner to meet the user auditor's timelines, often the period covered by the SOC report will precede the entity's period-end for which the user auditor is seeking reliance on controls. This timing difference is sometimes referred to as the "gap period." In such cases, the auditor may make inquiries of user entity management to determine whether management has identified any changes in the service organization's[13] controls subsequent to the period covered by the service auditor's report, and the auditor may consider the results of other procedures for indications of changes in controls at the service organization. These changes might include the following:

- changes in personnel, with whom user entity management interacts, at the service organization
- changes in reports or other data received from the service organization
- change in contracts or service level agreements with the service organization
- errors identified in the service organization's processing

Based on an evaluation of the following risk factors:

- the timing and length of the gap period
- the significance of the service organization activities
- whether control deficiencies have been identified in the service organization's processing activities
- the nature and significance of any changes in the service organization's controls identified by the user auditor or management

the auditor considers whether they need additional evidence about the operating effectiveness of controls during the gap period or if changes need to be evaluated as to their effect on the auditor's conclusion on the effectiveness of internal controls. This information is usually obtained in the form of a bridge letter from the service organization to the user auditor. The information provided in a bridge letter is equivalent to making high level inquiries of the management of the service organization. If the bridge letter states that significant changes have occurred since the date of the most recent SOC report, the auditor considers those changes and determines their effect on the

12 Refer to CAS 315, paragraph 7.

13 And where applicable, subservice organization

audit procedures. Auditors review the bridge letter for appropriateness, whether the bridge letter covers the remainder of the audit period, and whether controls have not changed significantly since the date of the Type 2 SOC report. The bridge letter is signed by the service organization's management (not the service auditor) attesting that the internal controls are still operating effectively. See **FAQ 12** if the auditor is unable to obtain an appropriate bridge letter.

NOTE:
It is possible that a user entity auditor is relying on more than one Type 2 SOC reports to obtain sufficient coverage for the audit period (i.e., you could be using part of one Type 2 SOC report and part of another Type 2 SOC report), and you may still also need a bridge letter.

Auditors may consider whether to request that management obtain a more current Type 2 SOC report if:

- there is a significant amount of time in the gap period
- the controls at the service organization are more likely than not to have changed during the gap period.

If a more current report cannot be obtained, then the auditor will typically perform other procedures in order to obtain evidence over the controls at the service organization (see **FAQ 12**).

FAQ 12 – If a SOC report is not available or does not meet your needs, what is the impact to the audit and audit report?

If a SOC report is not available or does not meet your needs as the auditor (e.g., such as not fulfilling the requirements of CAS 402, paragraph 14-17), you still need to obtain evidence to support your understanding about the design and implementation of controls at the service organization,[14] which may include:

- assessing whether there is sufficient appropriate audit evidence concerning the relevant financial statement assertions available from records held by the user entity
- contacting the service or subservice organization, through the user entity, in order to visit the service organization or subservice organization and directly perform procedures to evaluate the design and implementation of controls at the service organization or subservice organization that relate to the services provided to the user entity
- engaging another auditor to perform the appropriate procedures on your behalf[15]

14 Or where applicable, subservice organization

15 CAS 402, paragraph 12

If the outcome of your risk assessment includes an expectation that controls at the service organization or subservice organization are operating effectively, and a Type 2 report is not available or does not meet your needs, you can use the same approaches mentioned above to test the operating effectiveness of relevant controls.

If you are unable to conduct the necessary audit procedures to obtain sufficient appropriate audit evidence to address the assessed risks of material misstatement regarding the service/subservice organization services, you would need to modify your opinion in the auditor's report.

CAS 705, *Modifications to the Opinion in the Independent Auditor's Report*, paragraph 13 states that if the auditor is unable to obtain sufficient appropriate audit evidence, the auditor shall determine the implications as follows:

a. If the auditor concludes that the possible effects on the financial statements of undetected misstatements, if any, could be material but not pervasive, the auditor shall qualify the opinion; or

b. If the auditor concludes that the possible effects on the financial statements of undetected misstatements, if any, could be both material and pervasive so that a qualification of the opinion would be inadequate to communicate the gravity of the situation, the auditor shall:
    i. withdraw from the audit, where practicable and possible under applicable law or regulation; or (Ref: Para. A13)
    ii. if withdrawal from the audit before issuing the auditor's report is not practicable or possible, disclaim an opinion on the financial statements.

About this publication

The Research, Guidance and Support group of the Chartered Professional Accountants of Canada (CPA Canada) undertakes initiatives to support practitioners and their clients in the understanding and implementation of standards. As part of these initiatives, the CPA Canada Advisory Group on the Implementation of Canadian Auditing Standards (Advisory Group) provides advice on the identification of issues related to the implementation of Canadian Auditing Standards (CAS) and on the development of non-authoritative implementation guidance related to these issues. The Advisory Group includes volunteers from the following Canadian firms: BDO, Deloitte, EY, Grant Thornton, KPMG, MNP and PwC.

This paper was developed and reviewed with the support of several volunteers, including CPA Canada's Advisory Group on the Implementation of the CAS and certain Auditing and Assurance Standards Board (AASB) technical staff. CPA Canada expresses its appreciation to all of the volunteers for their support in preparing this publication.

Consultation and feedback

In the interest of continuous improvement and our commitment to the development of high-quality non-authoritative guidance, we would welcome any comments, questions and suggestions regarding this Frequently Asked Questions at the following address:

Yasmine Hakimpour, CPA, CA
Principal, Audit and Assurance
Research, Guidance and Support
Chartered Professional Accountants of Canada
277 Wellington Street West
Toronto, Ontario M5V 3H2
Email: **research@cpacanada.ca**

DISCLAIMER

This FAQ was prepared by the Chartered Professional Accountants of Canada (CPA Canada) as non-authoritative guidance. CPA Canada and the authors do not accept any responsibility or liability that might occur directly or indirectly as a consequence of the use, application or reliance on this material. This FAQ has not been issued under the authority of the Auditing and Assurance Standards Board.

Copyright © 2024 Chartered Professional Accountants of Canada

All rights reserved. This publication is protected by copyright and written permission is required to reproduce, store in a retrieval system or transmit in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise).

For information regarding permission, please contact **permissions@cpacanada.ca**.

Appendix 1: Audit Client Briefing

Considerations for management when using services from a third-party organization

The purpose of this Audit Client Briefing is to make you (management) aware of matters to consider when using the services of a third-party organization, and the auditor's requests pertaining to Canadian Auditing Standard (CAS) 402, *Audit Considerations Relating to an Entity Using a Service Organization*.

Given today's complex business landscape and the number of new and emerging services and industries, there has been an increase in the range of business activities that are being outsourced to third-party organizations. To comply with Canadian auditing standards, your auditor is required to obtain a sufficient understanding of the services provided by third-party organizations you rely on in order to identify, assess and address the risks of material misstatements in the financial statements. In order for your auditor to obtain this understanding, it is your responsibility first and foremost as management to have an understanding of the services that are being outsourced.

What does this mean for your audit?

CAS 402 is not a new audit standard; however, given the changes in how businesses operate and the increased number of businesses engaging with third-party organizations, auditors may ask you additional questions about your business operations to identify any new third-party relationships. Auditors may ask you more specific questions about your interactions with third-party organizations to identify which third-party organizations are relevant to financial reporting and accordingly would be considered service organizations and in scope of CAS 402. The types of questions they may ask you could include the following (note this is not an exhaustive listing):

- What new third-party organizations have you engaged with for services?
- Which contracts with third-party organizations have changed?
- Can you describe the entity's vendor/third-party risk management process?
- Can you provide details on the organizational structure, ownership, governance and business model, including the extent to which the business model integrates the use of information technology (IT)?
- Can you describe the IT environment and if you use any external vendors?
- Can you explain how your financial system handles the initiation, recording, processing, correction and integration of transactions into the general ledger for reporting in financial statements? Additionally, can you provide details on the percentage of transactions or revenues processed by third-party organizations?

NOTE:
Not all third-party organizations are considered service organizations as per CAS 402. Your auditor will ask questions regarding the nature of any relationships and determine if a service organization relationship exits under Canadian auditing standards.

Depending on the answers to the questions above, your auditor may also ask you for documentation such as:

- business plans, strategies, records, internal control manuals, meeting minutes
- latest contracts with third-party organizations
- System and Organization Controls (SOC) report(s) for service organizations
- bridge letters from service organization management
- Service Level Agreements (SLAs)

If your auditor has determined that a service organization relationship exists between you and a third-party organization, they may need you to obtain a SOC report from the service organization (*and a SOC report from a subservice organization if applicable*[16]). A SOC report is generally more effective than other alternative documentation as it is intended to comprehensively report on controls, assertions and risks related to the information systems relevant to financial reporting. The earlier the SOC report is requested from service organization management, the more effectively your auditors will be able to plan their audit procedures for your audit. A SOC report will inform your auditors about the controls at the service organization and, for certain types of SOC reports, whether controls relevant to your audit are operating effectively.

As management, it is your responsibility to review any applicable SOC reports and determine whether there are any control deficiencies identified by the service auditor and how they may impact the services provided to you. As well, it is your responsibility to go through the list of complimentary user entity controls identified by the service organization and implement those controls effectively within your own organization. Your auditor will likely request evidence to support the design and implementation, and, where appropriate, the operating effectiveness of those relevant complimentary user entity controls. It is always good practice to inquire about SOC reports when engaging with any new third-party organization.

Lastly, depending on whether the SOC report is sufficient to meet the auditor's needs (e.g., in terms of the scope, timing, operating effectiveness of the relevant controls), the auditor may be required to complete additional procedures or, if this is not possible, they may need to modify the auditor's opinion in the audit report to appropriately reflect the limitations of the available information.

16 If a subservice organization performs processing activities on behalf of the service organization you rely on, you, as management, may need to also obtain a copy of the subservice organization's SOC report, if the results were not already included in the service organization's SOC report.