Canadian Public Accountability Board
Conseil canadien sur la reddition de comptes

Audit considerations relating to an entity using service organizations: strengthening audit quality

The Canadian Public Accountability Board (CPAB) is seeing increased use of service organizations[1] in our inspections of the audits of Canadian reporting issuers. Auditors face new challenges when auditing reporting issuers utilizing the services of service organizations that require a tailored audit response. In our inspections, CPAB is observing an increase in the number of significant findings related to the use of service organizations which requires additional focus for auditors.

This communication is intended to provide examples of observed findings and offer additional insights into the assessment of service organizations, including determining their significance and the identification, assessment and response to the risks of material misstatement. It is important to note that this supplementary information does not replace Canadian auditing standards as it may not encompass all considerations and is not designed to serve as a comprehensive collection of all relevant factors.

We expect firm leadership to distribute this communication to all audit engagement team members and actively encourage open dialogue among engagement teams as they plan and perform their audit engagements.

What our inspections reveal

In today's complex business landscape, organizations increasingly rely on third-party organizations to optimize their business operations. Examples include:

- **Cloud services**: Adoption of cloud services has become widespread in today's business landscape. These services deliver software as a service, eliminating the need for companies to maintain their own software and hardware, and handling increased data volume.

- **Third-party e-commerce platforms**: Businesses are increasingly turning to third-party e-commerce platforms to streamline their operations. These platforms handle various tasks such as warehousing, ordering, fulfillment and shipping services.

- **Managed information technology (IT) services**: Rather than maintaining an in-house IT department, some businesses are turning to third-party IT service providers. These companies can offer a wide range of services, from network management to data backup and recovery.

- **Cryptocurrency custody services**: As the use of cryptocurrencies broadens, businesses are increasingly turning to third-party custody services for the safekeeping and management of their digital assets such as safeguarding offline storage (cold storage) and multi-signature wallets.

[1] CAS 402 paragraph 8(e).

Common inspection findings

Risk identification and assessment	Responding to risks of material misstatement
• Insufficient understanding of the nature and scope of services provided by the service organization.[2] • Understanding of controls at the cryptocurrency exchange (the service organization) holding material digital assets on behalf of the reporting issuer was limited to a discussion with representatives at the third-party exchange. • The System and Organization Controls (SOC) type 2 report[3] obtained did not specify the applications responsible for processing critical financial reporting transactions impacting the auditor's ability to assess the reliability and adequacy of control to address the relevant financial assertion risks. • Insufficient consideration of whether the services provided by subservice organizations were relevant to the audit of the user entity's financial statements.[4]	• Auditors obtained a type 2 report but did not evaluate whether complementary user entity controls (CUECs), which the service organization assumes will be implemented by the user entity, effectively addressed the relevant financial statement assertion risks.[5] • Inappropriate reliance placed on management's reconciliation of monthly reports from external sources to the reporting issuer's database without assessing the service organization's controls or verifying the accuracy and completeness of the reports. • Despite assessing revenue as a significant risk, the auditor's procedures for addressing the risk of errors or fraud in revenue transactions processed by the service organization were insufficient, particularly in assessing discrepancies between accounts receivable balances and amounts subsequently received.

Although we identified deficiencies across a range of service organizations utilized by reporting issuers, we have observed a strong correlation between the quality of management's oversight of the service organization and the quality of audit work. The following are three key areas that are important for auditors to consider:

- Determining the significance of the services provided by the service organization.
- Identifying and assessing the risks of material misstatement.
- Responding to the risks of material misstatement.

[2] CAS 402 paragraph 9.
[3] CAS 402, paragraph 8 (c). A Type 2 report on a service organization's controls includes a description by the service organization's management of the service organization's system, control objectives, and related controls, their design and implementation as at a specified date and their operating effectiveness throughout a specified period.
[4] CAS 402 paragraph 18.
[5] CAS 402 paragraph 17(b).

Determining the significance of the services provided by the service organization

Where a user entity has engaged a service organization to perform services, it is essential that the auditor, at the planning stage of the audit, understands the nature and scope of the services being performed.[6] Our inspections noted auditor challenges in understanding the significance of the services performed in non-traditional third-party arrangements. These servicing arrangements can be highly technical and complex, involving multiple layers of services and interactions. We observed challenges in understanding the intricacies of the technologies involved (i.e., technical architecture, data flows, integration points, security configurations, and automated processes), leading to potential misinterpretations or oversights during the audit process.

As part of their risk assessment and procedures to understand the user entity's control environment, auditors are required to obtain an understanding of how a user entity uses the services of a service organizations, including subservice organizations that are performing information processing activities on behalf of the service organizations.[7] In accordance with Canadian Auditing Standards 402[8], *Audit Considerations Relating to an Entity Using a Service Organization* (CAS 402), when a service organization's activities materially affect the user entity's financial statements, the auditor places increased emphasis on obtaining an understanding of the controls and processes within the service organization. This is especially critical in cases where the service organization's operations significantly impact the user entity's financial statements. To better understand how a user entity uses a service organization, auditors can:

- Review flowcharts or transaction process flows as well as the type of information that flows through the user entity (e.g., financial, operational) to understand how service organizations are involved in the extended enterprise.
- Review the nature and extent of the services provided by subservice organizations that are relevant to the user entities' information systems.
- Review the terms and conditions of agreements with service organizations.
- Identify the dollar amount, frequency, complexity and impact of processed transactions on the user entity's financial statements.
- Understand the impact of IT controls over the integrity of the transactions processed (completeness, accuracy, availability and timeliness).

ASK

- ✓ Who processes the transactions?
- ✓ Who maintains the IT applications?
- ✓ Who maintains other relevant IT environment components?

It may not initially seem apparent to auditors that the transactions handled by both the service organization and its subservice organization have a material impact on the user entity's financial statement. However, in certain instances, the underlying nature of these transactions can carry significant implications. Within such contexts, the auditor may determine the necessity of understanding the nature of these controls. For example, consider scenarios where the service organization or its subservice organization handle critical IT functions for the user entity, such as performing information processing activities or management of

[6] CAS 402 paragraph 9(a).
[7] CAS 315, paragraph 26(a)(iv).
[8] CAS 402, paragraphs 3, 9.

critical financial systems or other services integral to the user entity's financial operations. Weaknesses in the controls governing these functions could result in errors in the processing of financial transactions such as incorrect disbursements, unauthorized transactions processed and/or misallocated payments or interest calculations. These errors, when combined or accumulated over time, could collectively have a material impact on the user entity's financial statements.

> Service organizations can significantly influence the risks of material misstatement in the user entity's financial statements. Auditors must understand the operations and controls of service organizations to effectively assess and address these risks as part of their audit procedures.

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.[9]

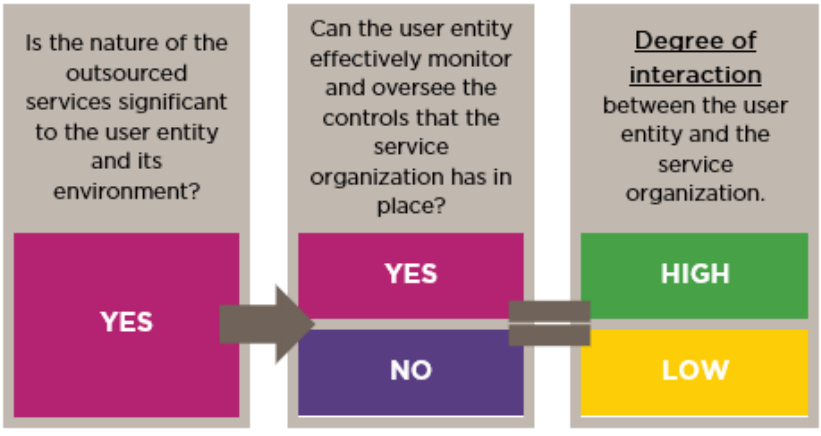
Identifying and assessing the risks of material misstatement

Once the auditor determines the significance of the organization's services and controls, the next step is to identify and assess the risks of material misstatement.[10] To effectively navigate this process, auditors need to obtain a sufficient understanding of how significant classes of transactions flow through the information systems of both the user entity and service organization.[11] This understanding informs the auditor's assessment of assertion-level risks impacted by the outsourced service.

To effectively identify and assess risks of material misstatement, auditors should prioritize the following three critical areas.

1. **Understand the degree of interaction between the service organization and the user entity** in relation to the user entity's ability to monitor and implement effective controls over the service organization's activities. The degree of interaction includes the user entity's ability to understand, assess and potentially influence the controls implemented by the service organization to ensure the reliability and accuracy of the services being provided.

   For example, in the banking sector, when a bank outsources its credit card processing, it often leads to a high degree of interaction because it retains sufficient monitoring controls over authorizing transactions and ensuring the accuracy and security of financial information. Conversely, there may be a lower degree of interaction when a company outsources its IT infrastructure management, including application and database management or cloud services, its ability to implement effective controls over the outsourced services and transaction processing activities may not be practicable or feasible, relying heavily on the controls implemented by the service organization.



[9] CAS 402 paragraph A20.
[10] CAS 402 paragraph 11.
[11] CAS 402 paragraphs 3(a), A22(b).

Recognizing these dynamics helps auditors obtain an understanding of the distinctive risks and control considerations associated with different outsourcing arrangements, allowing for a more effective and targeted audit approach.

2. **Gain a thorough understanding of the flow of information and data through the user entity's process-level activities**. By tracing the movement of information to and from the service organization, identifying interfaces, and evaluating data integrity and security, auditors can assess the potential risks associated with data transmission. For instance, in the case of a manufacturing company outsourcing its inventory management, auditors would be required to understand how inventory data flows through the user entity's information systems between applications, databases or other aspects of the IT environment, internally and externally, as appropriate, through system interfaces. This understanding is necessary to ensure a comprehensive evaluation of controls and data reliability.

> Existing cloud arrangements pose risks concerning data transfer, prompting auditors to assess migration processes for completeness and accuracy. For cloud computing arrangements, auditors may also consider inherent risks like data security vulnerabilities and potential disruptions to business processes, all of which have significant implications for financial reporting and risk management.

3. **Assess how the use of service organizations impacts significant business processes within the user entity**. This involves understanding the interdependencies between the user entity's internal information system and the service organization's information system.[12] For example, when a manufacturing company uses cloud-based enterprise resource planning (ERP) software for inventory and production processes, auditors are required to obtain an understanding of the integration of the user entity's internal ERP system with the cloud-based system to address risks arising from data accuracy, availability and security.

Responding to the risks of material misstatement

CAS 402 expands on the requirements in CAS 330[13], *The Auditor's Response to Assessed Risks* specifically responding to assessed risks of material misstatement arising from the user entity's use of a service organization.

As described in the previous section, the auditor may have based their assessment of assertion-level risks of material misstatement on an expectation that relevant controls at the service organization are operating effectively (i.e., because they intend to rely on those controls). In that case, auditors are required to test the operating effectiveness of those controls at the service organization by obtaining and evaluating a report on the description, design and operating effectiveness of controls at a service organization relevant to the audit of the user entity's financial statements (referred to as a type 2 report) if one is available, performing the tests of operating effectiveness of controls at the service organization themselves or using another auditor to perform tests of controls at the service organization on behalf of the user auditor.[14]

However, there may be situations where substantive procedures alone (or in combination with tests of operating effectiveness of controls at the user entity) will not provide sufficient appropriate audit

[12] CAS 315, *Identifying and Assessing the Risks of Material Misstatement*, paragraph 25 (a), Appendix 5.
[13] CAS 330, *The auditor's responses to assessed risks*.
[14] CAS 402 paragraphs 14, 16, 17.

evidence to mitigate assertion-level risks arising from outsourced services. In these cases, auditors will also need to test the operating effectiveness of relevant controls at the service organization.[15]

CAS 402 underscores the importance of comprehensively evaluating controls at service organizations when addressing risks associated with outsourced services, and auditors should exercise due diligence in assessing the adequacy of controls and evidence provided by reports in the context of the audit of the user entity's financial statements.

Auditors are required to understand the components of the user entity's system of internal controls, which includes the control environment, risk assessment process and the monitoring process. This understanding extends to the user entity's system of internal controls and their relevancy to the preparation of the financial statements.[16] System and Organization Controls (SOC) Reports (SOC 1 and SOC 2)[17] provide valuable insights into a service organization's internal control environment.[18] Here are key considerations:

1. **SOC 1 and SOC 2 reports serve different purposes.**

    - SOC 1 engagements in Canada are performed under the Canadian Standard on Assurance Engagements (CSAE) 3416 standard. This standard is used to evaluate and report on controls at a service organization relevant to a user entity's internal controls over financial reporting (ICFR).

    - SOC 2 engagements in Canada are performed under CSAE 3000 and use the Trust Services Criteria, a set of criteria established by the AICPA Assurance Services Executive Committee (ASEC). These criteria are used to evaluate and report on a user entity's system controls related to security, availability, processing integrity, and confidentiality or privacy of information.[19]

2. **When planning the audit and performing risk assessment procedures, auditors may decide to use a SOC 2 report as a source of information**. This decision considers:

    - Relevancy of controls and trust criteria to the user entity's ICFR and financial reporting risks.

    - Alignment of the report's period with the financial statement audit timeline or the effectiveness of ICFR controls.

    - Significance and uniqueness of the service organization's controls.

While a SOC 2 report covers a broad range of risk areas, including but not limited to organizational structure, IT, human resources and third-party management, it does not primarily focus on ICFR controls. User entities can use a SOC 2 report in their evaluation of certain risks associated with controls stemming from system failures, natural disasters, data breaches, service delivery failures or cyber attacks when engaging with a service organization. However, it is important for the user entity's auditor to carefully consider how the SOC 2 report and the user entity's specific ICFR requirements align.

Auditors should evaluate the suitability and effectiveness of the controls identified in the SOC 2 report. However, they should also conduct their own procedures as necessary to form their opinion on the

[15] CAS 402 paragraphs A29-A30.
[16] CAS / ISA 315, *Identifying and Assessing the Risks of Material Misstatement*, paragraphs 21-26.
[17] CAS 402 paragraph 8(b)(c).
[18] Assurance beyond the financial statements: Reports on system and organization controls, CPA Canada.
[19] Assurance and Advisory (aicpa.org).

effectiveness of the user entity's ICFR.[20] This ensures a comprehensive understanding of the control environment and helps 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.

Key takeaways for auditors

The use of service organizations in today's business landscape has introduced new challenges for auditors. To navigate these challenges and adhere to auditing standards, auditors must adapt their audit plans, focusing on determining the significance of the services provided by the service organizations, identifying and assessing risks of material misstatement, and responding effectively to these risks. Auditors should consider:

Timely collaboration and communication: Timely and clear communication between the auditor, the user entity and the service organization is critical. Gaining an early understanding of the services provided by the service organization and its control environment can assist auditors in identifying the necessary information for developing applicable audit procedures that mitigate the identified risks.

Compliance with professional standards: CAS 402 is not a standalone standard. CAS 402 expands on how the auditor performs risk assessments (CAS 315) and responds to assessed risks (CAS 330) ensuring that they gather sufficient and appropriate audit evidence to support their conclusions. This includes evaluating controls at both the user entity and service organization.

Risk identification and assessment: Understanding the technical intricacies of the services provided, identifying all relevant service organizations and subservice organizations, and evaluating the potential impact of outsourced activities on financial reporting are critical to support risk identification and assessment. This includes reviewing the contract terms, understanding the degree of interaction between the user entity and service organization, tracing data flows and evaluating the impact of outsourced services on significant business processes. Auditors must be diligent in identifying risks, even if certain transactions seem insignificant individually but can collectively impact financial statements.

Develop a response to assessed risks: Responding to risks of material misstatement may involve a combination of approaches, including testing controls at the service organization, obtaining, evaluating system and organization controls (SOC) reports where available and/or performing independent tests as determined necessary. When using a SOC report, the auditor needs to evaluate whether the user entity has designed and implemented controls that address complementary user entity controls[21] (CUECs). The auditor should also consider the need to test the operating effectiveness of relevant CUECs to obtain sufficient appropriate audit evidence.

[20] CAS 402 paragraph A37.
[21] CAS 402 paragraph 17(b).

Technical SOC training and skill sets: Investing in technical tools (e.g., software for data analysis, risk assessment and process mapping, among others) and auditor training is important as the use of service organizations grows. This enhances auditors' risk identification and assessment capabilities. Reviewing and mapping SOC reports requires an understanding of the nature and significance of the services provided by the service organization and their effect on the user entity's internal controls.[22] This ensures effective evaluation of the controls in the SOC reports, enabling auditors to form an accurate opinion on the user entity's ICFR.

Documentation: Documentation is required to be sufficient to enable an experienced auditor, having no previous connection with the audit to understand the nature, timing and extent of procedures to comply with the CAS.[23]

Learn more

Visit us at https://cpab-ccrc.ca/home and join our mailing list. Follow us on LinkedIn.

Canadian Public Accountability Board
Conseil canadien sur la reddition de comptes

[22] CAS 402 paragraphs 7(a), A2.
[23] CAS 230 paragraph 8.