Canadian Public Accountability Board
Conseil canadien sur la reddition de comptes

MARCH 2024

Identifying and assessing the risks of material misstatement: Strengthening audit quality

The evolving nature of risks

Identifying and assessing the risks of material misstatement is foundational to the audit. Canadian Auditing Standard 315, *Identifying and Assessing the Risks of Material Misstatement* (CAS 315) was revised effective for 2022 calendar year-ends to better align with the increasing complexity of business models and use of technology, while emphasizing an iterative and dynamic approach to risk assessment.

While we have seen improvements to the risk assessment procedures performed by auditors, more remains to be done. The Canadian Public Accountability Board (CPAB) has identified findings related to the implementation of the revised standard across a range of audit areas including revenue, business combinations, financial instruments and inventory.

This communication is intended to highlight the importance of understanding the entity. We also provide insights into the significant findings identified, through illustrative scenarios, and share good practices observed in files with

Why is risk assessment so important?

Because it drives the design of audit responses.

no findings. We expect audit firm leadership to develop targeted actions to improve the quality of auditor's identification and assessment of risks. We emphasize the importance of holding management accountable for fulfilling their responsibilities, effective two-way communication with the audit committee and the importance of robust risk identification and assessment to audit quality.

We expect audit 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.

Auditor's responsibility in evaluating management's risk assessment

CAS 315 requires the auditor to obtain an understanding of management's risk assessment process as well as the oversight of that process by those charged with governance. As business models evolve and become more complex and technology becomes more integral to the reporting issuer's operations, we expect the nature and extent of oversight and governance to increase and management's risk assessment process to consider additional associated business risks. Where the auditor identifies risks of material misstatement that management failed to identify, the auditor needs to consider if these indicate a deficiency in the overall control environment and accordingly, assess the impact on determining inherent and control risk, and the overall audit approach.

Effective communication among the engagement team, management and those charged with governance is important to an engagement team's risk identification and assessment activities. This is also an opportunity for the engagement team to provide timely feedback to management and those charged with governance on the appropriateness of management's risk assessment process.

Importance of understanding the entity

The overall objective of a financial statement audit is for the auditor to obtain reasonable assurance over whether the financial statements as a whole are free from material misstatement, whether due to fraud or error. Auditors work to reduce detection risk, that is, the risk that the procedures performed by the auditor will not detect a misstatement that exists and that could be material, either individually or when aggregated with other misstatements, to an acceptably low level. One of the key factors contributing to common inspection findings stems from engagement teams not obtaining a sufficient understanding of the entity and its environment and the entity's system of internal control. When auditors lack a comprehensive understanding, risks at both the financial statement and assertion levels, including risks arising from the use of information technology (IT) may go unidentified and unassessed.

We have observed a correlation between the depth of the auditor's understanding of the entity and its system of internal controls and the perception of the level of financial reporting and IT complexity. When the auditor does not identify or properly assess all relevant risks, they are more likely to not adequately design and perform appropriate audit procedures to reduce the risk to an acceptably low level.

Common inspection findings

CPAB has observed inspection findings where risks are not identified or sufficiently assessed by the auditor, resulting in an audit response that does not address the risk of material misstatement. Below, we have organized our findings into several key themes that are closely related in audit files where we have identified significant inspection findings:

Expectation that the reporting issuer's internal controls are operating effectively

We have noted multiple instances where the auditor designed substantive audit procedures that implicitly relied on the operating effectiveness of certain internal controls without substantiating their conclusion.

Examples encountered in our inspections include:

- The auditor designed a substantive approach where audit support was based on the expectation that information from the entity's IT system was reliable, however, there was no control or substantive audit procedures performed over the accuracy and completeness of such information. [Scenario one, scenario three]

- The auditor concluded that a substantive approach was appropriate for an entity with highly automated and paperless processing of transactions, involving multiple integrated IT applications, without obtaining an understanding of the relevant processes and controls, IT applications and general IT controls. There was no evidence the auditor evaluated whether substantive procedures alone could provide sufficient appropriate audit evidence for the risks of material misstatement at the assertion level. [Scenario two]

- The auditor did not obtain a sufficient understanding of how an entity uses service organizations in its operations or determine the significance of the service organization to the reporting issuers internal control over financial reporting. [Scenario two, scenario four]. In November 2023, we published Audit Considerations Relating to an Entity Using Service Organizations: Strengthening Audit Quality which provides additional insights in this area.

We also observed that some auditors did not sufficiently consider factors that may increase inherent and control risk at the assertion level and the risks of material misstatement at the financial statement level. Factors that can have a pervasive impact on the risk of material misstatement may include a lack of personnel with appropriate accounting and financial reporting skills, control deficiencies previously identified that have not been remediated by management, and the history of uncorrected and corrected misstatements.

No re-evaluation of the initial risk assessment as the audit progresses

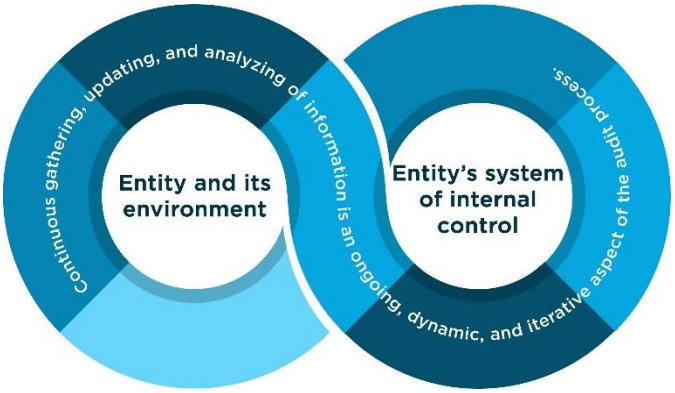
We have noted instances where the auditor did not adequately consider the iterative nature of risk assessment and perform a stand back assessment. This includes re-visiting the initial risk assessment and evaluating the impact of new information, the results of audit procedures performed, and audit evidence obtained to

determine whether the risk of material misstatement at both the financial statement and assertion level remain appropriate.

Examples encountered in our inspections include:

- The auditor identified numerous misstatements when performing audit procedures but did not evaluate whether the misstatements arose from internal control deficiencies and accordingly revise the control risk assessment.

- The auditor did not sufficiently consider all audit evidence obtained during the audit, such as control deficiencies or contradictory information[1] and assess whether the initial risk assessment should be refined. [Scenarios one, two, three, and four] When noted in our inspections, such information was often included in the audit file and/or in public filings but not considered by the engagement team.



No risk of material misstatement at the assertion level for a material class of transactions or account balance

In some instances, we noted the auditor's risk assessment concluded there was no assertion level risk of material misstatement for a material class of transactions or account balance without obtaining an understanding of the relevant processes and IT applications. The stand-back requirement was introduced to prompt the auditor to evaluate the completeness of the identified risks of material misstatement.[2] Irrespective of the assessed risks of material misstatement, the auditor is required to design and perform substantive procedures for each material class of transactions and account balance [3][Scenario three].

Appendix A includes scenarios that are based on actual significant findings, but facts have been modified or excluded to safeguard the identities of the reporting issuers.

We also highlighted key aspects of CAS 315 and practices we observed in our inspections to assist auditors perform more effective risk identification and assessment procedures, which in turn, will result in the auditor designing more effective audit procedures that are responsive to those risks.

[1] Contradictory information may include allegations from a whistleblower, management's discussion and analysis, press releases and management's cash flow forecasts.
[2] CAS 315, para. 36.
[3] CAS 330, para. 18.

Good practices observed at the firm and engagement level

Firm level

A dynamic and robust system of quality management can help prevent the underlying root causes of some of our findings. Examples of firm controls observed that have a positive impact on the risk assessment procedures performed at the engagement-level include:

Common root causes for underestimating the complexity of the entity's structure:

- Insufficient time budgeted to refine the risk assessment and perform a stand-back analysis to confirm the appropriateness of initial risk assessments.
- Engagement team members lacked relevant expertise and industry experience.
- Insufficient involvement of relevant subject matter experts (e.g., IT, tax, climate and fraud), in understanding the entity, including its system of internal controls.

- Establishing a thorough review process for engagement budgets and team composition to ensure the engagement team members have adequate capacity, skills, and industry or other specialized knowledge as required for the engagement.
- Monitoring engagements that may require the support of subject matter experts, such as fraud, valuation, tax or IT.
- Developing and communicating appropriate guidance to support engagement teams as they perform risk assessment and design and perform adequate procedures, including examples and situations where consultations may be beneficial or required.
- Developing appropriate resources such as standardized forms and templates that enable and require teams to consider various aspects of risk at certain stages in the audit process.

Refer to our October 2022 communication System of quality management call to action: Strengthening audit quality for further insights in this area.

Engagement level

CAS 315 has introduced a new concept of the spectrum of inherent risk, which takes into account the assessed likelihood and magnitude of the misstatement and inherent risk factors and varies based on the nature, size and complexity of the entity. For a risk to be assessed as higher on the spectrum of inherent risk, it does not mean both the likelihood and magnitude need to be assessed as high, but auditors need to consider these aspects in combination to conclude whether there is a lower or higher risk of material misstatement.

Below are examples of practices observed in inspections where engagement teams revised their initial risk identification and assessment and designed further audit procedures to respond to the increased level of risk:

Iterative assessment of risks during the audit

- The risk of inventory obsolescence for a manufacturer was initially determined to have a low risk of material misstatement. During the audit of management's estimate of the inventory provision, the engagement team identified that management did not include sufficient consideration for excessive inventory. As a result, the auditor revised their initial risk assessment and elevated the inventory valuation risk of material misstatement to high.

- The valuation of deferred tax assets was initially determined to have a low risk of material misstatement. During the audit, the auditor identified concerns over management's cash flow forecasts including an inappropriate forecasting period and unsupportable assumptions. As a result, the engagement team, along with their tax specialists, re-evaluated their initial risk assessment over deferred tax assets and concluded that there was a high risk of material misstatement relating to the recognition of the deferred tax asset.

- The valuation of goodwill was initially determined to have a moderate risk of material misstatement. The engagement team reviewed the reporting issuer's public disclosures and identified climate commitments made by the company that were inconsistent with assumptions made in management's cashflow forecasts prepared for goodwill impairment analyses. As a result, the engagement team re-evaluated the initial risk assessment based on the evidence obtained and increased the risk of material misstatement to significant. [4]

Identification of new risks during the audit

- The valuation of material spare parts inventory was initially determined to have no risk of material misstatement. During the audit, the engagement team identified new information, specifically that the entity no longer uses certain parts due to engineering changes. As a result, the engagement team re-evaluated their initial risk assessment and concluded that the spare inventory balance had a moderate risk of material misstatement relating to the valuation assertion.

- The engagement team identified a significant risk associated with the existence of events and conditions that cast significant doubt about the reporting issuer's ability to continue as a going concern. Management's going concern assessment is dependent upon the company's ability to remain in compliance with debt covenants. During the audit, several misstatements were identified for which management did not adjust. The engagement team considered the impact of these unadjusted misstatements on the debt covenant as at year-end as well as on the going concern cash flow. The engagement team also considered the related control deficiencies that resulted in the misstatements to determine existence of any previously unidentified risks. Based on procedures performed, the engagement team identified further risks on the going concern disclosure as well as opening balances. As a result of the additional procedures performed, a debt covenant breach was identified resulting in a material uncertainty about the reporting issuer's ability to continue as a going concern.

[4] A communication was issued in March 2024 to all firms registered with CPAB on the impact of climate-related risks on financial statement audits. Auditors should refer to that alert for further considerations on climate-related risks.

Use of flowcharts and Automated Tools and Techniques (ATT)

Capturing the flow of transactions through flowcharts that are supported by detailed walkthroughs, may result in better risk assessments procedures. Engagement teams that use flowcharts generally have a more in-depth understanding of the end-to-end processes and are more likely to identify risks that are more focused, resulting in audit procedures that are responsive to those risks.

Similarly, the use of ATTs can significantly enhance the quality of the auditors' risk assessment by providing auditors with a more detailed and robust understanding of how transactions are processed at an entity. By using process mining ATTs (also referred to as process or transaction mapping), teams can confirm their understanding of how transactions for various cycles flow through the entity's information system, including how they are initiated in the system and recorded in the general ledger. The auditor can then investigate any deviations from the path approved by management through the information system to determine the impact of the deviations on the risk assessment (e.g. identify new risks or increase significance of an already identified risk).

Refer to CPAB Exchange: Technology in the audit for further discussion on how ATT can be used to enhance the quality of audits.

Key takeaways for auditors

As described throughout this communication, the risk of auditors not designing and performing appropriate audit procedures is significantly increased when the auditor does not identify or properly assess all relevant risks. Even if the auditor does not plan to test the operating effectiveness of identified controls, the auditor's understanding of the control activities may still affect the design of substantive audit procedures to ensure the nature, timing and extent are based on and are responsive to the assessed risks of material misstatement. The increasing complexity of business models and use of technology by reporting issuers further increases the need for auditors to identify relevant risks and adequately adjust their audit approach.

The key takeaways for auditors include:	
Importance of understanding the business:	Obtaining an understanding of the reporting issuer's system of internal control and end-to-end processes in sufficient depth is required to identify and assess risks of material misstatement, due to fraud or error. Involving specialists, utilizing ATTs and flow charts to identify risks, processes and controls can improve the auditor's understanding of the entity and the relevant risks.
Iterative audit approach:	Applying an iterative audit approach by continuously refining audit risks based on new information, including misstatements, control deficiencies and other evidence obtained during the audit, is required to ensure that risks are identified and/or revised when new circumstances arise.
Internal control expectations:	Considering whether the planned audit responses are based on the expectation that internal controls are operating effectively is required to ensure that the team applies the appropriate audit approach. For example, when utilizing key reports as part of audit evidence, the auditor either needs to test the operating effectiveness of the controls or perform substantive procedures over the completeness and accuracy of such reports.
Comprehensive IT integration:	Identifying and assessing the increasing integration of IT in an entity's control environment is required to achieve a thorough understanding of the entity's business. This involves collaborating with internal or external IT specialists to gain insights into complex systems, evaluating their impact on financial reporting, and continually developing IT expertise to ensure an effective audit process. Staying up to date with relevant IT advancements is integral to an effective and forward-looking audit process.
Robust system of quality management:	Having robust processes and controls as part of an audit firm's system of quality management is key to support engagement teams in performing a quality risk assessment. Firms can do this by designing and implementing a variety of responses at the firm and engagement level based on the firm's size and complexity.

Appendix A – Illustrative scenarios

These scenarios are based on actual significant findings, but facts have been modified or excluded to safeguard the identities of the reporting issuers.

Scenario one

Background:

The reporting issuer has a diverse portfolio of many business units organized into three operating segments, and the parent company acquires at least 20 new business units each year. The reporting issuer has decentralized operations and not all business units use the same accounting software or use different versions of the same software. The reporting issuer utilizes a combination of spreadsheet programs and a standard consolidation software to prepare their consolidated financial statements.

Audit approach:

The audit engagement was determined to be a group audit and the group engagement team performed all audit procedures directly (no reliance on component auditors). The engagement team obtained a detailed understanding of the nature and types of revenue earned by the reporting issuer within its operating segments and various business units. The engagement team identified a fraud risk and a significant risk relating to the occurrence and accuracy of revenue transactions with multiple performance obligations. No increased risk of material misstatement was identified for other revenue transactions. The engagement team applied a combined audit approach for revenue streams identified as having significant risks, which included testing the design, implementation, and operating effectiveness of certain controls and performing other substantive procedures. For other revenue streams, substantive procedures at the transaction level were only performed for in-scope components.

Revenue from out-of-scope components amounted to 30 per cent of total consolidation revenue which was more than 50 times group materiality. The engagement team concluded there was no risk of material misstatement related to the out-of-scope components because none of them individually had revenue above group materiality. The engagement team also concluded the likelihood of errors occurring in the same direction and aggregating to a material error at the consolidated level was remote due to the large number of components and the decentralized structure.

The engagement team also concluded that the entity's use of IT systems was less complex and did not test general IT controls or identify any risks arising from the use of IT in the entity's information systems. The engagement team performed testing over the consolidation by tracing in-scope components to underlying accounting records for the business unit and by agreeing a sample of elimination entries for in-scope components to supporting documentation.

Findings:

The engagement team did not obtain a sufficient understanding of the reporting issuer's IT environment to support their risk assessment that IT systems were less complex. The engagement team's approach was to only perform substantive audit procedures for the consolidation and revenue streams at in-scope components that did not have a significant risk. This approach placed implicit reliance on the effectiveness of IT and group-wide controls as it was based on an expectation that those controls were operating effectively. These controls were not identified as relevant during planning and were not evaluated for design and implementation or tested for operating effectiveness. Therefore, the understanding of group-wide controls and the consolidation process did not sufficiently identify and assess the risks of material misstatement at the assertion level arising from the complexity of the reporting issuer's structure. The assessment of the IT systems was not sufficient to conclude there were no information technology risks, given the number of components, separate systems, and the continual onboarding of newly acquired entities on a regular basis. Overall, the engagement team had employed a substantive audit approach over the consolidation on the presumption that controls were effective without substantiating their conclusion with an appropriate assessment of the control risk.

Examples of risks not identified and assessed by the engagement team, resulting in insufficient audit evidence obtained include:

Financial statement level risks that also result in assertion level risks related to revenue	Risks arising from the use of IT
• Transactions for newly acquired entities are not processed completely and accurately. • Business units are not included in the consolidated financial statements completely and accurately. • Related party transactions are not identified and eliminated in the consolidated financial statements.	• Transactions are not recorded completely due to system limitations, data integration issues, or manual errors. • Access to transactional data is not authorized, which can result in manipulation or errors, including undetected unauthorized or fraudulent transactions. • System changes or updates are not adequately tested and validated, leading to errors in transaction processing. • Errors in transaction processing, data entry, calculations, and the consolidation process, caused by data integration issues or software errors, are not identified leading to financial reporting inaccuracies. • Newly implemented systems from acquired entities are processing data incompletely and inaccurately.

Scenario two

Background:

The reporting issuer earns revenue from providing online services. Customers deposit funds into their accounts using online payment processing services and purchase services using funds within their accounts. Customers can withdraw funds available in their accounts at any time. Until such funds are withdrawn by the customer, they are held in accounts owned by the reporting issuer but are reported as customer cash deposit liabilities within the financial statements. The reporting issuer developed an in-house IT system that tracks all customer activity, including deposits, purchased services, fees and withdrawals. The reporting issuer relies on the IT system to determine revenue, cost of revenue and customer cash deposit liabilities. The processing of revenue transactions is highly automated and paperless, involving multiple integrated IT applications.

Audit approach:

The engagement team identified a fraud risk, and a significant risk relating to the occurrence and accuracy of revenue. The engagement team concluded that conducting substantive audit procedures would provide sufficient and appropriate audit evidence to address the risks of material misstatement. The engagement team concluded that observable audit evidence could be obtained for each transaction.

The observable audit evidence took the form of reports generated by the in-house IT system for every transaction, along with cross-referencing to cash records whenever feasible, specifically for customer deposits and withdrawals.

Findings:

The engagement team's identification and assessment of the risks of material misstatement was not precise and was based on an incomplete understanding of the reporting issuer's system of internal controls including its IT environment. The specific details of these risks were not explicitly outlined, and the design and implementation of relevant controls was not evaluated. The sufficiency and appropriateness of agreeing transactions to the reporting issuer's in-house IT system relied on the effectiveness of controls over its completeness and accuracy. There was no consideration of whether substantive procedures alone were sufficient to address the risks identified, specifically, whether evidence obtained from the in-house developed IT system was reliable and whether there was a potential for improper initiation or alteration of information to occur and not be detected.

Examples of risks not identified and assessed by the engagement team, resulting in insufficient audit evidence obtained include:

Assertion level risks related to revenue, cost of revenue and customer cash deposit liabilities	Risks arising from the use of IT
• Customer cash deposit liabilities are inaccurate due to incorrect transaction information obtained from other systems, such as the cash deposit and cash withdrawal systems administered by third party services. • Revenue is incorrectly recorded when cash is deposited into a customer account instead of when a performance obligation has been satisfied. • Fictitious customers are set up in the system with fraudulent revenue transactions recorded.	• Customer cash deposit liabilities are incorrect due to errors in IT system calculations or due to the IT system missing transactions or having duplicate transactions. • User authentication and authorization are inadequate, leading to unauthorized access and potential manipulation of customer accounts or financial transactions within the IT system. • IT system change management is inadequate due to a lack of effective monitoring and exception handling controls, introducing errors, vulnerabilities, or increase the risk of undetected irregular transactions.

Scenario three

Background:

A manufacturing entity provides specialty services and products. Inventory cost includes raw materials and supplies with some labour and general overhead allocated to finished goods. The reporting issuer consistently and historically experienced strong gross margins. While they experienced various increases in costs during the year, they have historically been able to pass these onto the customer. This was a first-year audit for the engagement team as the financial statements were previously audited by another auditor.

Audit approach:

The engagement team's approach to inventory and cost of sales was substantive with no planned reliance on internal controls. To understand the labour and general overhead cost allocation process, the engagement team performed a walkthrough of a sample of one. From this walkthrough and from estimating the allocation based upon the inventory balance, the engagement team concluded there was no risk of material misstatement due to unreasonable allocations of labour and general overhead. The engagement team also determined that the valuation of inventory was not a risk of material misstatement on the basis the reporting issuer had historically achieved high margins from the sale of inventory.

Based on the engagement team's risk assessment, no audit procedures were performed to assess the completeness and accuracy of allocations of labour and general overhead or to assess the appropriateness of net realizable value of inventory. The engagement team did identify risks relating to cost of sales, and as a response to the risks identified, performed analytical procedures over gross margin by comparing the current year and prior year results on an aggregate basis. The engagement team concluded no procedures were required to be performed over material manual adjustments to overall overhead allocations included in cost of sales on the basis they were reclassifications within the income statement that did not impact net income.

Findings:

The engagement team's conclusion that there was no risk of material misstatement related to the overhead allocation impacting cost of sales and valuation of inventory were not supported by the risk assessment procedures performed. The engagement team's walkthrough of a sample of one for the overhead allocation did not demonstrate a complete understanding of the cost allocation process including how labour and overhead rates were determined and applied in the IT system and the variances that were identified were not investigated. As a result of the risk assessment conclusion: (i) no lookback assessment of prior year cost allocations was performed to consider the reasonability of management's estimates and (ii) no testing was performed over material manual adjustments to overall overhead allocations that impacted gross margin.

The engagement team performed a gross margin analytic that was not sufficiently precise to support the conclusion that there was no risk of material misstatement over valuation of inventory or to address the risks identified related to cost of sales. Specifically, the analytical procedure was based on total sales at the component level (no disaggregation by product type or month), and before considering material manual adjustments and other information, such as the impact from increasing costs on margin that was observed while performing other substantive procedures.

Examples of risks not identified and assessed by the engagement team, resulting in insufficient audit evidence obtained include:

Assertion level risks related to cost of sales and inventory	Risks arising from the use of IT
• Overhead allocations recognized in cost of sales are not complete or accurate. • Significant differences between budgeted and actual overhead allocations are not investigated resulting in inaccurate costing. • Overhead allocations are not appropriately allocated to the correct product categories resulting in inaccurate gross margins. • Inventory is not recorded at the lower of cost and net realizable value.	• The IT system used to determine overhead allocations, process transactions and calculate purchase price variances is not reliable resulting in overhead allocations that are not complete or accurate.

Scenario four

Background:

The reporting issuer earns revenue primarily through the provision of services. Most contracts are long-term and include multiple deliverables with payment schedules that do not generally align with the delivery of services. The company uses a third-party to facilitate sales to its customers.

Audit approach:

The engagement team performed a walkthrough to assess the design and implementation of controls over the revenue cycle and based on a sample of one, concluded there was a single performance obligation that was satisfied at a point in time. The audit approach for testing revenue was purely substantive and the testing relied on reports from the third-party as the primary source of audit evidence, which was reported based on monthly totals. No audit procedures were performed on individual sales transactions or related contracts.

Findings:

The engagement team did not have a complete understanding of the end-to-end processes in the revenue cycle for how transactions are initiated, recorded, and processed to identify and assess the risk of material misstatement over revenue at the assertion level. There were no procedures performed to support the conclusion that all contracts are uniform and revenue recognition policies are appropriate. As part of the audit response to address identified risks, the engagement team relied on information from the third-party but did not assess if they were a service organization[5] or understand the risks associated with the use of this information.

Risks not identified and assessed by the engagement team, resulting in insufficient audit evidence obtained include:

Assertion level risks related to revenue

- Revenue contracts are not standardized and have terms that may result in different revenue recognition, impacting accuracy and occurrence of revenue.
- Revenue is recorded before the performance obligation has been satisfied.
- The reports obtained from a third-party and used as a basis to record revenue (and related accounts) are not complete or accurate.
- Inadequate monitoring of controls by the reporting issuer over the service organization's activities may lead to a failure to detect and correct errors in a timely manner.

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

[5] As defined by CAS 402, *Audit Considerations Related to an Entity Using a Service Organization*.