CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Briefing For Management and Those Charged With Governance

Canadian Auditing Standards (CAS)

MARCH 2022

What you need to know about changes to the auditor's risk identification and assessment process in your financial statement audit

Purpose of This Briefing

This *Briefing* informs you, as management or those charged with governance (TCWG), of matters to consider pertaining to Canadian Auditing Standard (CAS) 315, *Identifying and Assessing the Risks of Material Misstatement* (the Standard). You will learn what is involved in preparing for and responding to its significant revisions and to requests from the auditor as a result of these revisions. In particular, this *Briefing*:

- highlights the potential impact on the audited entity (entity), which may result in management preparing more robust support for systems, processes and controls that will be needed to provide audit evidence to auditors for their risk assessment. These highlights will be relevant to TCWG in understanding the onus on management in preparing such support.
- informs TCWG on this key area of the audit to assist in their evaluation of the auditor.

When Is the Standard Effective and to Whom Does it Apply?

The changes to CAS 315 are effective for audits of financial statements for periods beginning on or after December 15, 2021. The Standard applies to the audit of **all** entities, regardless of their nature, size or complexity.

Why Did the Standard Change?

The Standard has been significantly enhanced to evolve with the increasingly complex nature of the economic, technological, and regulatory aspects of the markets and environments in which entities and auditors operate. The key changes require a more robust risk assessment to properly identify risks and promote more focused responses to the identified risks in a manner that is appropriate for the nature, size and complexity of the entity.

Key Changes to the Standard and the Potential Impact on the Entity

Key change	Potential impact on the entity
Overall, a more robust risk identification and assessment process, in turn promoting more focused auditor responses to identified risks	You may receive more up-front questions from the auditor as they plan the audit and identify and assess risks of material misstatement.[1] To facilitate a more robust risk-assessment process, the auditor may request additional information to enhance their understanding of systems, processes and controls. For example, the auditor may request: • a better understanding of the entity's business model and how it integrates the use of information technology (IT) • more information about the entity's own risk assessment process and process for monitoring the system of internal control[2] • more detailed narratives about how transactions are initiated, recorded, processed and reported • support such as policies and procedure manuals, flowcharts and other supporting documentation to validate their understanding of the information systems relevant to the preparation of financial statements • more information (or ask more questions) to support their inherent risk assessment, given there are new factors to consider in completing the assessment This information not only informs the auditor's risk assessment but also assists the auditor in determining an appropriate response to risks identified including, where warranted, new significant risks which would require a different response.

1 Risk of material misstatement: The risk that the financial statements are materially misstated prior to audit. This consists of two components, described as follows at the assertion level:
(a) Inherent risk – The susceptibility of an assertion about a class of transaction, account balance or disclosure to a misstatement that could be material, either individually or when aggregated with other misstatements, before consideration of any related controls.
(b) Control risk – The risk that a misstatement that could occur in an assertion about a class of transactions, account balance or disclosure and that could be material, either individually or when aggregated with other misstatements, will not be prevented, or detected and corrected, on a timely basis by the entity's controls.

2 System of internal control: The system designed, implemented, and maintained by those charged with governance, management, and other personnel, to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. The system of internal control consists of five interrelated components: (i) Control environment, (ii) The entity's risk assessment process, (iii) The entity's process to monitor the system of internal control, (iv) The information system and communication, and (v) Control activities.

Key change	Potential impact on the entity
Modernized to recognize the evolving environment, including in relation to IT	You may receive more focused questions and additional requests to better understand the IT environment of your entity, including: • IT applications, including data warehouses and report writers • supporting IT infrastructure (i.e., network, operating systems, databases and their related hardware and software) • IT processes (i.e., managing program changes, IT environment changes, and IT operations) • IT personnel involved in the IT processes Combined with the identified controls that may be needed to address the identified and assessed risks of material misstatement, this understanding may also identify risks (and potentially new risks) arising from the use of IT.[3] Therefore, you may receive more focused questions and additional requests to understand the general IT controls[4] that address such risks. For example, the auditor may have additional inquiries to understand general IT controls over journal entries (e.g., segregation of duties related to parking and posting entries) to address risks arising from the use of IT. Given the modernization related to IT, the auditor may also involve additional team members, such as IT specialists, who may need to engage with members from your IT team who were not previously involved in the audit process.
Enhanced requirements relating to exercising professional skepticism	You may receive additional inquiries if the auditors find information that appears to contradict what they have already learned in the audit.
Emphasizes how the auditor's risk assessment can be scaled up or down based on the nature and complexity of the entity being audited	The auditor's expectations regarding the formality of your entity's policies and procedures, and processes and systems, will depend on the complexity of your entity.
Recognizes the use of technology by the auditor, in the audit	The auditor may be using automated tools and techniques more frequently or extensively in their audit. This may mean that they will request different information or information in a different format, so that they can execute their audit procedures.

3 Risks arising from the use of IT: susceptibility of information processing controls to ineffective design or operation, or risks to the integrity of information in the entity's information system, due to ineffective design or operation of controls in the entity's IT process.

4 General IT controls: controls over the entity's IT processes that support the continued proper operation of the IT environment, including the continued effective functioning of information processing controls and the integrity of information in the entity's information system.

Questions TCWG May Want to Ask the Auditor in Light of the New Standard

The following sample questions for the auditor may further support you, as TCWG, in understanding the impact of the changes to the Standard and in your evaluation of the auditor. This list of questions is non-exhaustive and can be tailored depending on the stage of the audit in which you make your inquiries.

- How has revised CAS 315 influenced the risk assessment for the current year audit? Have you identified new risks, including those arising from the use of IT, from the prior year? Have you assessed previous risks (that continue to exist) differently? Has the change in assessment changed your response to such risks?
- Did you broaden the scope of your discussions with entity management during the risk assessment process? If so, in what areas? Did this result in the identification of any new risks?
- What additional documentation is needed from management to provide you with the evidence you need to make proper risk assessments?
- How do the changes to revised CAS 315 impact your time and resources to execute the audit?
- To what extent did you involve IT (or other) specialists in the audit to assist in meeting the new CAS 315 requirements? If so, how were the specialists used, and did the use of specialists change in the current year?
- Are there any new concerns with the entity's system of internal control?
- Were there any new areas where you challenged management in relation to conflicting information?
- Have there been or are there anticipated challenges in applying the new CAS 315 requirements to the audit?
- Did your use of technology to execute the audit change in the current year? If so, in what way and what impact did this have on the audit?

Other Resources

- CAS 315 *Implementation Tool for Auditors*
- CAS 315 *Audit and Assurance Alert*
- CAS 315, *Identifying and Assessing the Risks of Material Misstatement* (FRAS Canada)

Comments

If you have any comments on this *Briefing*, or suggestions for future publications, please send them to:

Grace Gilewicz, CPA
Principal, Audit & Assurance
Research, Guidance and Support
Chartered Professional Accountants of Canada
277 Wellington Street West
Toronto ON M5V 3H2
Email: ggilewicz@cpacanada.ca