CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Implementation Tool for Auditors

CANADIAN AUDITING STANDARDS (CAS)

DECEMBER 2017

STANDARD DISCUSSED

CAS 315, Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment

There are many steps involved in meeting the requirements of CAS 315. This *Implementation Tool for Auditors* discusses only selected requirements of CAS 315 identified through practice inspection as areas where auditors struggle to meet the requirements of CAS 315.

This *Implementation Tool for Auditors* (*Tool*) is being issued to raise awareness of common pitfalls auditors might encounter when applying certain requirements of Canadian Auditing Standard 315, *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment* (CAS 315) **as it relates to obtaining an understanding of internal control**.

This *Tool* provides non-authoritative audit guidance to you, the auditor, when you are implementing the requirements of CAS 315 **as it relates to obtaining an understanding of internal control**.

The focus of this publication is the objective noted in paragraph 3 of CAS 315, which states that the objective of the auditor is to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels, through understanding the entity and its environment, including the entity's internal control, thereby providing a basis for designing and implementing responses to the assessed risks of material misstatement.

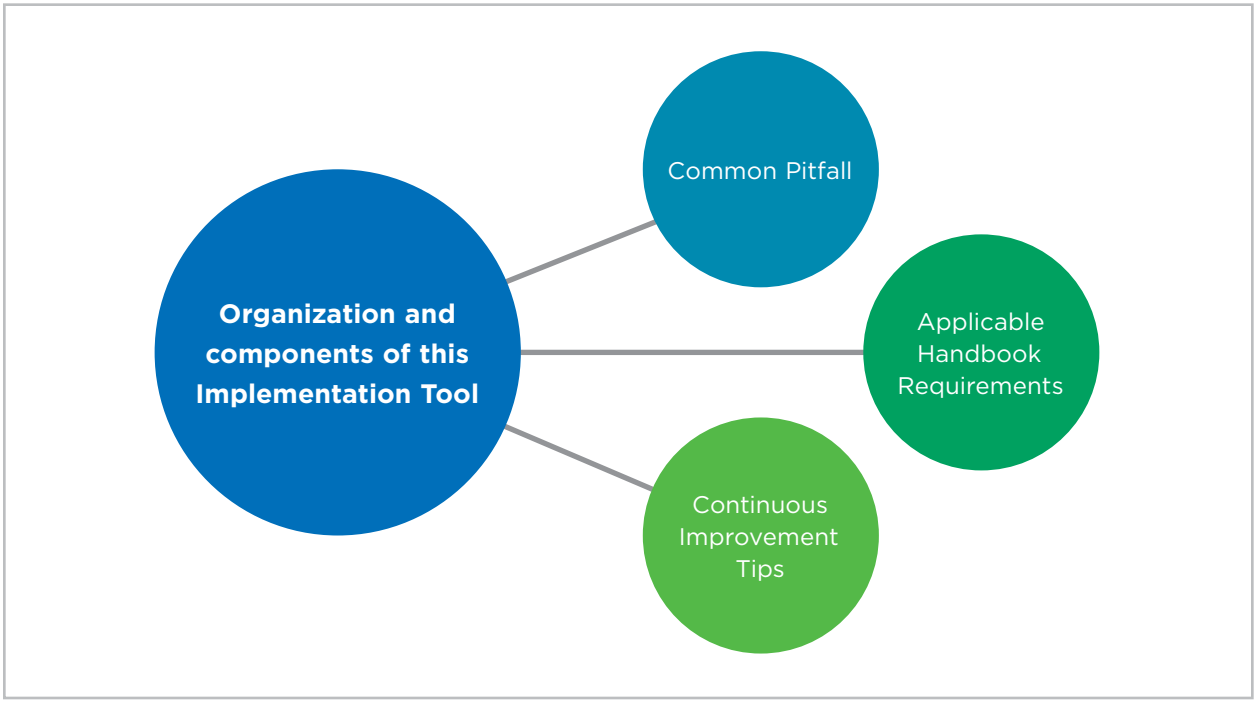
Auditors are encouraged to read this *Tool* as part of their planning and/or preparation for the year-end audit engagement to assist in meeting the requirements of CAS 315 by identifying and assessing the risks of material misstatement in order to understand the entity and its environment.

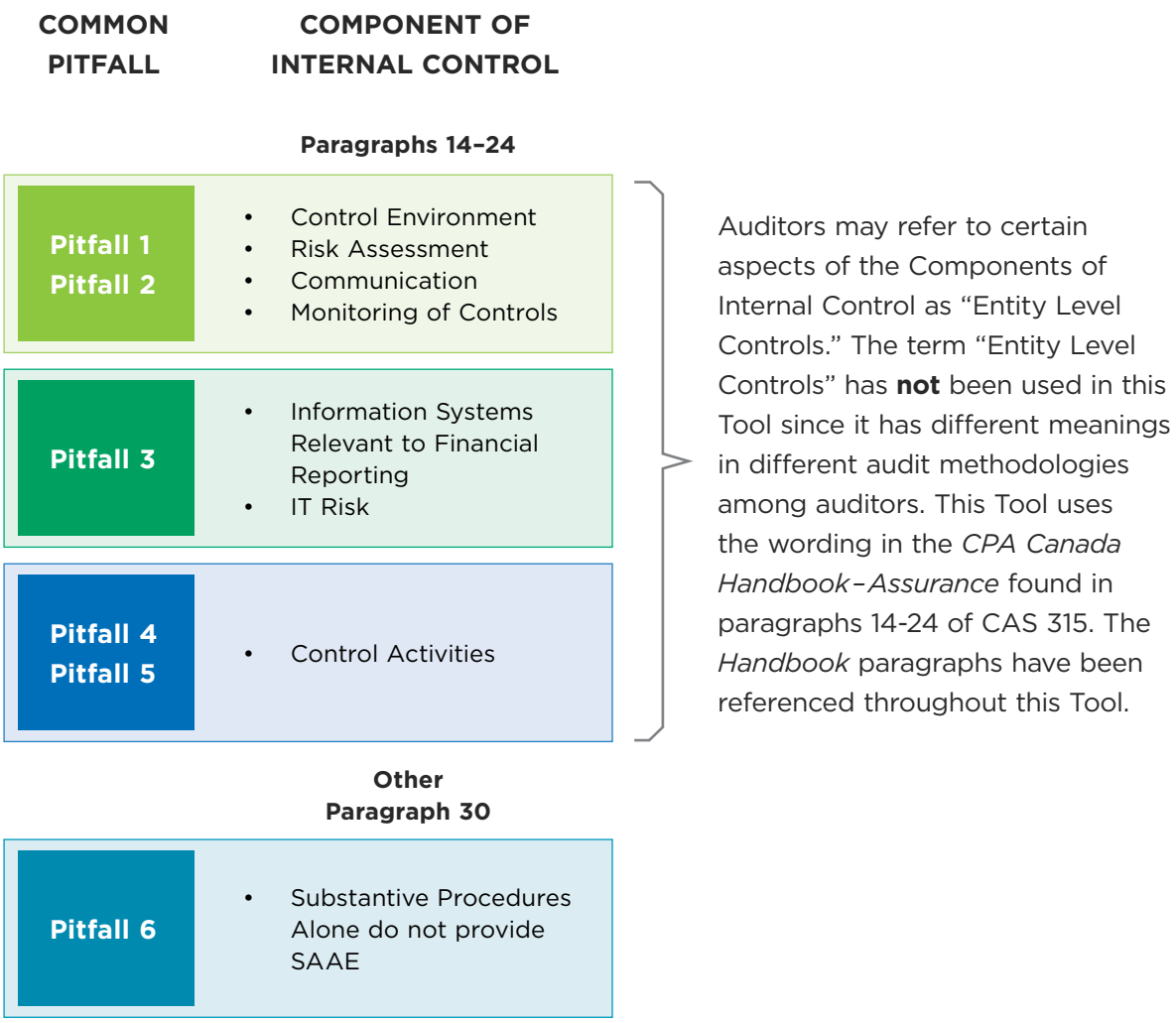
This *Tool* does not replace the need to read CAS 315 in its entirety, including the application and other explanatory material and does not address common pitfalls related to testing the operating effectiveness of internal controls.

Why You Should Read This *Tool*

Even if you are not intending to rely on the operating effectiveness of controls to determine the nature, timing and extent of substantive procedures (i.e., taking a fully substantive approach), you are required to obtain an understanding of relevant controls on every audit. This *Tool* helps auditors identify those relevant controls. You are also required to understand the entity's information system relevant to financial reporting. Both requirements provide a basis for the identification and assessment of risks of material misstatement at the financial statement and assertion levels. [CAS 315. 12, 13, 18, 20, A74-A76]

How This *Implementation Tool* Is Organized





Practitioners are reminded of the documentation requirements in CAS 230, *Audit Documentation* as well as the documentation requirements in paragraph 32(b) of CAS 315. Paragraph 32(b) of CAS 315 requires the audit documentation to include (excerpt only):

- key elements of the understanding obtained regarding each of the internal control components specified in paragraphs 14-24 of CAS 315
- sources of information from which the understanding was obtained
- risk assessment procedures performed.

Pitfall 1—Auditors do not identify relevant controls within the entity's:
- control environment
- risk assessment process
- information system and communication
- monitoring of controls.

What Is the Common Pitfall?

Auditors are:

- not identifying all the controls within the entity's control environment, risk assessment process, communication, and monitoring of controls, relevant to their audits
- concluding that there are no controls within the entity's control environment, risk assessment process, communication, and monitoring of controls, even when relevant controls do exist.

Information systems relevant to financial reporting are presented separately in this *Tool* (see page 13).

CAS Requirement

Paragraphs 12, 14, 15, 16, 17, 19, and 22 of CAS 315

Continuous Improvement Tips

- When there is no entity documentation of the entity's control environment, risk assessment process, communication, and monitoring of controls, the identification of such relevant controls, by the auditor, may be more dependent on inquiry of entity personnel than on inspection of documents. Auditors may consider speaking with more than one person at the entity to corroborate initial inquiries.
- Auditors are required to obtain an understanding of internal controls relevant to the audit.[1] These controls may include controls within the entity's control environment, risk assessment process, communication, and monitoring of controls. It would be rare that "relevant" controls within the entity's control environment, risk assessment process, communication, and monitoring of controls do not exist.
- The identification of the "relevant" controls within the entity's control environment, risk assessment process, communication, and monitoring of controls, will vary depending on the size and complexity of the entity. Auditors should not expect to identify the same type of controls at different entities under audit, even if those entities are in the same industry or of the same size.
- The following provides a useful framework for auditors to consider and presents the requirements related to each component of internal control and considerations for identifying relevant controls:

1 Paragraph 12 of CAS 315

Control component with related CAS 315 Requirements	In identifying relevant controls within the components of internal control	Auditors may consider the following when identifying relevant controls within the components of internal control
Entity's Control Environment (CE) — *CAS 315, paragraph 14*	auditors should identify controls in the entity's CE that: • support a culture of honesty and ethical behaviour that management, with the oversight of those charged with governance, has created and maintained • provide an appropriate foundation for the other components of internal control (e.g., control activities).	• communication and enforcement of integrity and ethical values (e.g., through development and distribution of a code of conduct and implementation of a whistleblower line), [CAS 315.A78] • commitment to competence (e.g., through monitoring that employees are maintaining training or obtaining professional development hours), [CAS 315.A78] • participation by those charged with governance (e.g., through establishing sub-committees such as the audit committee, pension committee, compliance and risk committee), [CAS 315.A78] • philosophy and operating style (e.g., through establishing consequences related to non-compliance with policies and procedures), [CAS 315.A78] • organizational structure (e.g., through maintenance of an organization chart), [CAS 315.A78] • assignment of authority and responsibility (e.g., through delegation of authority such as cheque signing or entering into contracts), and [CAS 315.A78] • human resource policies and practices (e.g., through monitoring performance of individuals) [CAS 315.A78]

Control component with related CAS 315 Requirements	In identifying relevant controls within the components of internal control	Auditors may consider the following when identifying relevant controls within the components of internal control
Entity's Risk Assessment Process (RA) *—CAS 315, paragraphs 15, 16 and 17*	auditors should identify controls in the entity's RA that: • identify business risks relevant to financial reporting objectives • estimate the significance of the risks • assess the likelihood of their occurrence • decide on actions to address those risks.	• The entity's risk assessment process forms the basis for how management determines the risks to be managed. The entity may implement periodic strategy meetings to discuss how management identifies, assesses the significance and likelihood of occurrence and responds to business risks by analyzing comparisons of budgets vs. actuals [CAS 315.A88] • In a smaller entity, there is unlikely to be a formal (documented) risk assessment process. In such cases, it is likely that management will identify risks through direct personal involvement in the business. Irrespective of the circumstances, however, inquiry about how management identifies, assesses the significance and likelihood of occurrence and responds to business risks, is still necessary. [CAS 315.A89]
Entity's Communication (C) *—CAS 315, paragraph 19*	auditors should identify controls in the entity's C that demonstrate: • how the entity communicates internal financial reporting roles and responsibilities and significant matters relating to financial reporting • how the entity communicates between management and those charged with governance • how the entity communicates externally (e.g., to regulatory authorities).	• Communication of the financial reporting roles and responsibilities and significant matters relating to financial reporting may take such forms as: — policy manuals [CAS 315.A97] — financial reporting manuals [CAS 315.A97] — organization charts — job descriptions — important memoranda or minutes of meetings. • Communication channels may exist to report or help ensure that exceptions regarding financial reporting roles and responsibilities are reported to the appropriate higher level within the entity and significant matters relating to financial reporting are reported and acted on. [CAS 315.A97] • Communication may be electronic, oral, written in hard copy, and can be visible through the actions of management.

Control component with related CAS 315 Requirements	In identifying relevant controls within the components of internal control	Auditors may consider the following when identifying relevant controls within the components of internal control
Entity's Monitoring of Controls (M) —*CAS 315, paragraph 22*	auditors should identify controls in the entity's M that demonstrate: • the major activities of the entity to monitor internal control relevant to financial reporting • how the entity initiates remedial actions to correct deficiencies in its controls. Monitoring of controls is not the same as the measurement and review of financial performance (commonly known as monitoring controls). Monitoring of controls is a control component that monitors the effective operations of other control components. [CAS 315.A110]	• The major activities management uses to monitor internal control relevant to financial reporting include ongoing activities, separate evaluations, or a combination of the two. [CAS 315.A110] For example: — periodic review of financial performance based on knowledge of the business that looks for any unexpected relationships that would indicate inaccuracies in financial data and lead to remedies for the underlying control activities and not solely to identifying misstatements in the financial information. — internal auditors or personnel performing similar functions (e.g., compliance functions) contributing to the monitoring of an entity's controls through separate evaluations or testing of control activities. [CAS 315.A113 and A115] — regular management and supervisory activities to monitor internal control. [CAS 315.A110] • Monitoring may come from external parties such as customer complaints and regulators' comments that may indicate problems or highlight areas in need of improvement in internal controls. [CAS 315.A111] • In smaller entities, the owner-manager's close involvement in operations may identify significant variances from expectations and inaccuracies in financial data leading to remedies for the underlying control activities. [CAS 315.A112]

Control Deficiency Considerations

- It would be rare if there were no "relevant" controls within the entity's control environment, risk assessment process, communication, or monitoring of controls. If there are no such "relevant" controls, there is a control deficiency (i.e., the organization has not designed or implemented a control: therefore the controls are inappropriately designed).
- If auditors conclude that the entity has not established an appropriate risk assessment process or has an ad hoc process based on the size and complexity of the entity, auditors are required to discuss with management whether business risks relevant to financial reporting objectives have been identified and how they have been addressed. Auditors are required to evaluate whether the absence of a documented risk assessment process is appropriate in the circumstances or to determine whether it represents a significant deficiency in internal control. [CAS 315.17]
- Auditors are required[2] to determine whether control deficiencies, individually or in combination, constitute significant deficiencies in internal control.
- Deficiencies in the design of controls within the entity's control environment, risk assessment process, communication, and monitoring of controls could have an impact on the auditor's assessment of the risks of material misstatement and in designing the nature, timing and extent of further audit procedures (i.e., tests of control and/or substantive procedures). [CAS 315.A50 and A74]
- Auditors may also need to consider the downstream implications of the control deficiencies in the entity's control environment, risk assessment process, communication, and monitoring of controls, on relevant control activities and consider the upstream implications of the control deficiencies in relevant control activities (see **Appendix 1**—Key Terminology & Concepts).

2 Paragraph 8 of CAS 265, *Communicating Deficiencies in Internal Control to Those Charged with Governance and Management*

Pitfall 2—Auditors do not evaluate the design of relevant controls within the entity's control environment, risk assessment process, communication, and monitoring of controls, and/or do not determine whether or not they have been implemented.

What Is the Common Pitfall?

Auditors are not:

- realizing that obtaining an understanding of relevant controls within the entity's control environment, risk assessment process, communication, and monitoring of controls, means that this understanding requires an evaluation of design and determination of implementation of such relevant controls
- evaluating the design and determining whether or not relevant controls have been implemented within the entity's control environment, risk assessment process, communication, and monitoring of controls
- documenting the key elements of the understanding obtained regarding each of the aspects of the entity and its environment specified in paragraph 11 of CAS 315 of each of the internal control components specified in paragraphs 14–24 of CAS 315.

CAS Requirements

Paragraphs 13, 14, 15, 19 and 22 of CAS 315

Continuous Improvement Tips

In Pitfall 1 above, considerations for identifying the relevant controls within the entity's control environment, risk assessment process, communication, and monitoring of controls, are outlined.

- When obtaining an understanding of relevant controls identified within the entity's control environment, risk assessment process, communication, and monitoring of controls, auditors are required[3] to evaluate the design of those controls and determine whether they have been implemented.

- When evaluating the design and implementation of relevant controls within the entity's control environment, risk assessment process, communication, and monitoring of controls, consider:
  - Inquiry may allow auditors to gather information about the design of a control, but inquiry alone is not sufficient to determine whether a control has been implemented. [CAS 315.A75 and AICPA Audit Guide—Assessing and Responding to Audit Risk in a Financial Statement Audit (September 2014), paragraph 1.13] Therefore, auditors are required[4] to perform procedures in addition to inquiry of the entity's personnel. For example, using professional judgment, the auditor may consider the following:

3 Paragraph 13 of CAS 315

4 Paragraph 13 of CAS 315

  - » CE: inspecting the entity's code of conduct and determining whether its content and elements are appropriate, given the size and complexity of the entity
  - » RA: observing (or inspecting other evidence of) periodic entity strategy meetings to determine whether management identifies, assesses the significance and likelihood of occurrence and responds to business risks
  - » C: inspecting the entity's financial reporting manuals to determine whether they are appropriately updated
  - » M: inspecting internal audit reports to determine how this group monitors internal controls or inspecting lists that monitor the completion of all account reconciliations and account analysis.

- When controls use information produced by the entity, auditors are required to evaluate whether the information is sufficiently reliable for the auditor's purposes.[5]

- Auditors may consider assessing whether the entity's control environment, risk assessment process, communication, and monitoring of controls, are designed appropriately for the entity's size and complexity[6] (e.g., an owner-managed control environment may be smaller and less complex than the control environment of a large public company).

- When entity documentation is lacking to demonstrate that the control has been implemented, auditors may request that the entity provide more observable or documentary evidence to provide support for the implementation of the relevant controls.

Control Deficiency Considerations

- Auditors are required[7] to determine whether control deficiencies, individually or in combination, constitute significant deficiencies in internal control.
- Deficiencies in the design or implementation of relevant controls could impact the auditor's assessment of the risks of material misstatement and the design of the nature, timing, and extent of further audit procedures (i.e., tests of controls and/or substantive procedures). [CAS 315.A50 and A84]
- Auditors may also need to consider the downstream implications of the control deficiencies in the entity's control environment, risk assessment process, communication, and monitoring of controls, on relevant control activities and consider the upstream implications of the control deficiencies in relevant control activities (see **Appendix 1**—Key Terminology and Concepts).

5 Paragraph 9 of CAS 500, *Audit Evidence*

6 Auditors may wish to refer to the Committee of Sponsoring Organizations of the Treadway Commission (COSO)—*Internal Control over Financial Reporting—Guidance for Smaller Public Companies*.

7 Paragraph 8 of CAS 265, *Communicating Deficiencies in Internal Control to Those Charged with Governance and Management*

Pitfall 3—Auditors do not understand the information system relevant to financial reporting, and how the entity has responded to the risks arising from IT.

What Is the Common Pitfall?

Auditors do not:

- obtain an understanding of the information system(s) relevant to financial reporting, therefore, their understanding:
  - does not capture the complexities of the information system(s), is limited or superficial
  - has been rolled forward from a prior-year file and is not up to date
  - is inaccurate
  - is incomplete.

- understand: [CAS 315.21 and A108]
  - the risks arising from IT
  - the controls implemented to address the IT risks
  - the impact that such IT risks have on the audit.

- consider whether a team member with expertise in IT/information system(s) is necessary, based on the complexity of the information system(s).

CAS Requirement

Paragraph 18(a)–(f) of CAS 315
Paragraph 21 of CAS 315

Continuous Improvement Tips

Considerations regarding engagement team competencies:

- Consider whether the engagement team collectively has the appropriate competencies and capabilities to evaluate the design and implementation of controls as the complexity of the information system(s) relevant to financial reporting increases. If not, the engagement partner may take action, such as assigning additional members to the engagement team (e.g., a person who has expertise in auditing IT systems[8]) to satisfy themselves that the engagement team has such competencies and capabilities.

Considerations when obtaining an understanding of information system(s) relevant to financial reporting:

- Identify the information system(s) relevant to financial reporting used by the entity:
  - Consider obtaining a list of the information systems used by the entity and then ask the question: "Is the information produced by the information system used in financial reporting?"

8 CAS 220.14

  - Examples of information systems relevant to financial reporting:
    - a separate point-of-sale system that interfaces with the accounting system
    - a separate system to manage real-property lease agreements, where the monthly revenue is calculated; a journal entry is subsequently prepared and used to record the revenue in the accounting system
    - an Excel spreadsheet used to maintain a fixed asset subledger where monthly depreciation and amortization is calculated; a journal entry is subsequently prepared and used to record the depreciation and amortization in the accounting system
  - Example of an information system not relevant to financial reporting:
    - a distinct information system, such as a scheduling system for the housekeeping staff at a hotel or restaurant, which may address a business risk, but is not relevant to financial reporting.

- Identify the nature and characteristics of the information system(s) relevant to financial reporting; to assist in determining the complexity of such systems:
  - infrastructure (e.g., where the data is stored)
  - type of software (e.g., extent of customization/configuration of information systems, "off-the-shelf software package" with no modification or with modification)
  - operating systems (OS) (e.g., whether the IT security system is integrated with the OS)
  - people (e.g., centralized IT function vs. a third-party service provider)
  - procedures (e.g., automated vs. manual interfaces as might be encountered in an e-commerce environment, batch vs. transactional processing)
  - data (e.g., ability to modify data, structured vs. unstructured, internal vs. external data sources, data sharing)
  - databases (e.g., read only vs. write and read privileges)
  - changes (e.g., the number and type of changes to the Information System (I/S) in the period under audit, use of emerging technologies)
  - implementation (e.g., a new I/S has been implemented in the year)
  - evidence (e.g., the availability of audit evidence, type of audit evidence: electronic vs. manual, whether the entity uses Electronic Data Interchange, and unavailability of reliable external evidence).

Obtaining an understanding of the information system relevant to financial reporting (note—inquiry alone is not sufficient):

- Consider linking the requirements in paragraph 18(a)–(f) of CAS 315 within the audit documentation:

18(a)	Have all relevant classes of transactions in the entity's operations (significant for the financial statements) been included?	Auditors may obtain an understanding of the information system, including the related business processes, relevant to financial reporting by performing risk assessment procedures such as inquiry of entity personnel.
18(b) & (c)	Have the relevant procedures, accounting records and supporting information (including both IT systems and manual systems) by which the entity's transactions are: • initiated • recorded • processed (including system overrides or bypasses to controls) [CAS 315.A90] • corrected as necessary (e.g., resolve incorrect processing of transactions) [CAS 315.A90] • transferred to the general ledger • reported in the financial statements been included? Have end-user computing tools (e.g., spreadsheets) been considered as part of the above?	Auditors may obtain an understanding of the information system, including the related business processes, relevant to financial reporting by performing risk assessment procedures, which may include: [CAS 315.A75] • inquiring of various entity personnel responsible for the procedures and preparing the accounting records to assist in preparing narratives or flowcharts • observing the application of specific controls • inspecting documents and reports such as entity-prepared narratives or flowcharts • tracing transactions through the information system relevant to financial reporting such as performing a walk-through.
18(d)	How does the information system(s) relevant to financial reporting capture events and conditions other than transactions that are significant to the financial statements?	Auditors may obtain an understanding of the information system, including the related business processes, relevant to financial reporting by performing risk assessment procedures such as inquiry of entity personnel regarding matters listed in Appendix 2 of CAS 315 for Conditions and Events That May Indicate Risks of Material Misstatement.

18(e)	How does the entity prepare its financial statements?	Auditors may obtain an understanding of the information system, including the related business processes, relevant to financial reporting by performing risk assessment procedures such as inquiry of entity personnel regarding how management: • makes accruals and other accounting estimates • accumulates information for financial statement preparation (e.g., cash flow statement, consolidation process) • resolves incorrect processing of transactions • determines how information required to be disclosed by the applicable financial reporting framework is accumulated, recorded, processed, summarized and appropriately reported in the financial statements • determines the reasonableness of accounting estimates and the adequacy of disclosures • determines the impact, if any, of subsequent events.
18(f)	What controls surround journal entries, including non-standard journal entries used to record non-recurring or unusual transactions or adjustments?	Auditors are encouraged to read CPA Canada's ***Implementation Tool for Auditors: Testing Journal Entries and Other Adjustments: Responding to the Risk of Management Override of Controls***.

Obtaining an understanding of how the entity has responded to risks arising from IT related to the information system(s) relevant to financial reporting:

- The risks arising from IT that pose specific risks to an entity's internal controls, include, for example: [CAS 315.21]
  - — reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both [CAS 315.A64]
  - — unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or non-existent transactions or inaccurate recording of transactions. Particular risks may arise where multiple users access a common database [CAS 315.A64]
  - — possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties [CAS 315.A64]
  - — unauthorized changes to data in master files [CAS 315.A64]
  - — unauthorized changes to systems or programs [CAS 315.A64]
  - — failure to make necessary changes to systems or programs [CAS 315.A64]
  - — inappropriate manual intervention [CAS 315.A64]
  - — potential loss of data or inability to access data as required. [CAS 315.A64]

- The extent and nature of the risks arising from IT vary depending on the nature and characteristics of the entity's information system(s) relevant to financial reporting. The entity responds to the risks arising from IT by establishing effective controls in light of the nature and characteristics of the entity's information system(s) relevant to financial reporting. [CAS 315.A67]

- Controls over IT systems are effective when they maintain the integrity of information and the security of the data such systems process, and include effective general IT controls and application controls. [CAS 315.A107]

- General IT controls provide assurance that applications are developed and subsequently maintained such that they provide for the functionality required to process transactions and provide automated controls. General IT controls that maintain the integrity of information and security of data commonly include controls over the following: [CAS 315.A108]
  - data center and network operations
  - system software acquisition, change and maintenance
  - program change
  - access security
  - application system acquisition, development, and maintenance.

Obtaining an understanding of how the entity has responded to risks arising from IT:

- Consider determining whether the entity has general IT controls over the items listed in the last bullet above or Paragraph A108 of CAS 315.
- Auditors may obtain an understanding of the above by performing risk assessment procedures such as inquiry of entity personnel, including IT personnel.

Other considerations related to risks arising from IT:

- When auditors plan to rely on effective general IT controls in order to rely on the consistent operation of application controls (see Key Terminology and Concepts Section) to modify the nature, timing and extent of substantive procedures, general IT controls are "relevant" to the audit.
- Auditors are required to evaluate the design of those relevant general IT controls and to determine whether they have been implemented by performing procedures in addition to inquiry of the entity's personnel.[9]

9 Paragraph 13 of CAS 315

Pitfall 4—Auditors do not identify control activities relevant to the audit.

What Is the Common Pitfall?

Auditors do not identify relevant control activities on their audits. For example, auditors possibly focus on:

- taking a substantive approach to their audits and incorrectly presuming there are no relevant control activities in the audit to identify
- identifying control activities that are not relevant to financial reporting
- identification of processes rather than control activities.

CAS Requirements

Paragraph 12, 20, 21, of CAS 315

Continuous Improvement Tips

- Consider that the CASs deem certain control activities to be **relevant to the audit**:
  - Control activities, automated or manual (see below) that relate to significant risks:

    Example: The auditors consider controls surrounding journal entries, including non-standard journal entries used to record non-recurring, unusual transactions or adjustments to address the non-rebuttable risk of management override of controls.

    Example: The auditors consider controls surrounding revenue recognition to address the presumed risks of fraud in revenue recognition when not rebutted.[10]

  - Control activities, automated or manual (see below), that relate to risks for which substantive procedures alone do not provide sufficient appropriate audit evidence (see Pitfall 6)
  - Control activities, automated or manual (see below), considered to be relevant in the judgment of auditors: [CAS 315.A100]

    Example: The auditors' judgment about whether or not a control activity is relevant to the audit considers 1) the identified risk that may give rise to a material misstatement and 2) whether it would be appropriate to test the operating effectiveness of the control when determining the extent of substantive testing. [CAS 315.A101]

10 Paragraphs 26-28 of CAS 240, *The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements*

  - Control activities, automated or manual (see below), regarding related parties and significant transactions and arrangements outside the normal course of business such as controls to[11]: [CAS 550.14]
    - » identify, account for, and disclose related-party relationships in accordance with the applicable financial reporting framework
    - » identify, account for, and disclose related-party transactions in accordance with the applicable financial reporting framework
    - » authorize and approve significant transactions and arrangements with related parties
    - » authorize and approve significant transactions and arrangements outside the normal course of business.

- Consider whether the control activity includes: [CAS 315.A62]
  - an automated control:

    Example: Edit checks of input data. [CAS 315.A109]

  - a manual control using information produced by IT (i.e., system generated report or a spreadsheet):

    Example: A manual review of a system-generated exception report with follow-up or manual review of plant and equipment depreciation calculation prepared in a spreadsheet. [CAS 315.A109]

  - a manual control independent of IT.

- Consider the entity's information systems (and their complexity) to assist in identifying control activities relevant to the audit.

- Consider performing walk-throughs of the information system(s) relevant to financial reporting to assist in identifying control activities relevant to the audit (see **Pitfall 3**).

- Consider "what can go wrong" at the assertion level to assist in identifying control activities relevant to the audit.

- Consider that although most controls relevant to the audit are likely to relate to financial reporting, not all controls that relate to financial reporting are relevant to the audit. It is a matter of the auditor's professional judgment whether a control, individually or in combination with others, is relevant to the audit.[12]

- Consider whether controls at a service organization or user controls related to a service organization may be included as part of control activities relevant to the audit.

- Consider whether some operational or compliance controls may be included as part of control activities relevant to the audit.

11 Paragraph 14 of CAS 550, *Related Parties*

12 Paragraph 12 of CAS 315

- Consider that:
  - controls can appear to be closely tied to financial reporting, but are not, and may not be, control activities relevant to the audit:

> **Example:** An entity may have controls in place over customer credit limits, which address a business risk by limiting the credit exposure of each customer in order to protect against potential future uncollectible amounts. Although an important operational control for an entity, the control may not be relevant to the audit for certain industries. Rather, from a financial reporting perspective, controls designed to ensure customer accounts receivable amounts exist, are complete, accurately recorded, and valued appropriately at period end, would likely be relevant to financial reporting and therefore perhaps control activities relevant to the audit.

In determining whether an activity is a process rather than a control activity, the auditor may:

- Consider the following question:
  - "Does the activity either a) prevent a misstatement in the financial statements, or b) detect, and correct, a misstatement in the financial statements?" If the answer to either question is no, then the activity may be a process activity and not a control activity or may not be able to address the risk of a misstatement on its own:

> **Example:** An entity may process its sales transactions, and the steps in the process may involve preparing an invoice based on the number of units shipped and price per unit. The extension of units sold is a process. When information is processed, the risk of misstatement is introduced. The calculation of the invoice may be based on incorrect prices (and these incorrect prices would represent a risk of "what can go wrong" at the entity for which a control activity would need to exist to mitigate this risk). Therefore, a check of invoices to make sure the correct prices have been used would prevent a misstatement in the financial statements and therefore would represent a control activity.

Control deficiency considerations:

- If there are no control activities identified, where controls are deemed relevant for the audit by the CASs:
  - there is a control deficiency (i.e., the organization has not designed or implemented a control: therefore inappropriately designed):

> **Example:** Management may not have responded appropriately to significant risks of material misstatement by implementing controls over these significant risks. Failure by management to implement such control activities is an indicator of a significant deficiency in internal control. [CAS 315.A148]

- If there are no control activities identified for an identified "what can go wrong" risk, there is a control deficiency (i.e., the organization has not designed or implemented a control: therefore inappropriately designed).
- Auditors are required[13] to determine whether control deficiencies, individually or in combination, constitute significant deficiencies in internal control.
- Deficiencies in the design of control activities could have an impact on the auditors' assessment of the risks of material misstatement and on designing the nature, timing and extent of further audit procedures (i.e., tests of controls and/or substantive procedures). [CAS 315.A50 and A84]
- Auditors may also need to consider the downstream implications of the control deficiencies in the entity's control environment, risk assessment process, communication, and monitoring of controls, on relevant control activities and consider the upstream implications of the control deficiencies in relevant control activities (see **Appendix 1**—Key Terminology and Concepts).

13 Paragraph 8 of CAS 265, *Communicating Deficiencies in Internal Control to Those Charged with Governance and Management*

Pitfall 5—Auditors incorrectly conclude that control activities relevant to the audit are appropriately designed to prevent (or detect and correct) material misstatements.

What Is the Common Pitfall?

In Pitfall 4 above, considerations for identifying the control activities relevant to the audit are outlined.

Auditors are not appropriately evaluating the design of control activities relevant to the audit ("relevant control activities"). For instance:

- Some auditors include in their audit documentation unmodified descriptions of generic control activities found in pre-populated audit tools that are not in any way linked to the risks of the entity or the business processes and thus do not evaluate the control that actually exists at the entity.
- Some auditors do not realize that the relevant control activities, alone or in conjunction with other control activities, do not address the identified risks that relate to financial statement assertions.

CAS Requirement

Paragraph 13 of CAS 315

Continuous Improvement Tips

- Auditors only need to evaluate the design for relevant control activities and determine whether they have been implemented.

- When evaluating the design of a control activity (automated or manual), consider:
  - whether the control activity, on its own or in combination with other control activities, addresses the identified risk of fraud and/or error (the "what can go wrong")
  - whether the control activity addresses the related financial statement assertions:

    Example: If auditors do not document the risks at the assertion level, they may not have connected the identified control activities to those risks at the assertion level.

  - who performs the control activity:

    Example: The person reviewing the allowance for doubtful accounts (AFDA) analysis may not have attended sales meetings or have access to all the relevant information and therefore may not have all the necessary knowledge needed to review the AFDA appropriately.

    Example: The auditor may consider speaking with the control owner, and may extend such discussions to the process owner.

— when the control activity is performed and how often:

> **Example:** Control activities related to property, plant and equipment may be performed annually in an entity with only minimal office equipment transactions whereas a rapidly expanding entity investing in capital equipment may need control activities to operate more frequently for these controls to be designed appropriately.

— precision of the control activity (e.g., for management review controls):

> **Example:** Senior management reviews an analysis of budgets-to-actuals looking for unusual items, whether there is a sufficiently precise set of criteria, such as a threshold, or another defined method, for investigating variances.

— whether a manual control uses information produced by IT (e.g., a system-generated report)

> **Example:** If management is preparing an impairment analysis of multiple cash generating units (CGUs), the auditor is required[14] to evaluate whether the information (i.e., the system-generated report related to the CGUs) is sufficiently reliable for the auditor's purpose.

— whether there are any application control activities being considered in isolation without considering the impact of general IT controls (see **Pitfall 3**).
— obtaining updated descriptions of the control activities for *each* audit period.
— When using prepopulated tools or resources, update the descriptions of the control activities *each* audit period to reflect the actual control description at the entity; the documentation should reflect the facts and circumstances of the entity.

- Consider determining whether a relevant control activity has been implemented only when it is appropriately designed.

Other considerations:

- Consider whether the engagement team collectively has the appropriate competencies and capabilities to evaluate the design and determine implementation of control activities as the complexity of the information system(s) relevant to financial reporting increases. If not, the engagement partner may take action (e.g., assign additional members to the engagement team such as a person with expertise in auditing IT systems[15]) to satisfy themselves that the engagement team has such competencies and capabilities.

14 Paragraph 9 of CAS 500, *Audit Evidence*

15 Paragraph 14 of CAS 220, *Quality Control for an Audit of Financial Statements*

Procedures to obtain audit evidence about the design and implementation of relevant control activities may include:

- inquiring of entity personnel to gather information about the design of a control activity. An inquiry alone is not, however, sufficient to determine whether a control activity has been implemented. [CAS 315.A75 and AICPA Audit Guide—Assessing and Responding to Audit Risk in a Financial Statement Audit (September 2014), paragraph 1.13]
- observing the application of specific relevant control activities
- inspecting documents and reports
- tracing transactions through the information system relevant to financial reporting, such as performing walk-throughs (Practitioners may wish to refer to the AASB Bulletin: ***Understanding Internal Control Relevant to the Audit—The Function of a Walk-through***).

Control deficiency considerations

- If the control activity is inappropriately designed, there is a control deficiency.
- If a control activity is not implemented or not implemented as designed, there is a control deficiency.
- Deficiencies in the design of control activities could have an impact on the auditor's assessment of the risk of material misstatement and on designing the nature, timing and extent of further audit procedures.
- Auditors are required[16] to determine whether control deficiencies, individually or in the aggregate, constitute significant deficiencies in internal control.
- Auditors may also need to consider the downstream implications of the control deficiencies in the entity's control environment, risk assessment process, communication, and monitoring of controls, for relevant control activities and consider the upstream implications of the control deficiencies in relevant control activities (see **Appendix 1**—Key Terminology & Concepts).

16 Paragraph 8 of CAS 265, *Communicating Deficiencies in Internal Control to Those Charged with Governance and Management*

Pitfall 6—Auditors do not determine when substantive procedures alone are not sufficient to provide appropriate audit evidence.

What Is the Common Pitfall?

In highly automated processing environments, with little or no manual intervention, auditors inappropriately judge that substantive procedures alone **can** provide sufficient appropriate audit evidence.

CAS Requirement

Paragraph 30 of CAS 315

Continuous Improvement Tips

- In determining whether routine business transactions are subject to highly automated processing with little or no manual intervention, the following may be indicative of this environment: [CAS 315.A150]
  - Audit evidence is available *only* in electronic form (its sufficiency and appropriateness usually depend on the effectiveness of controls over its accuracy and completeness).
  - A *significant* amount of an entity's information is initiated, recorded, processed, or reported only in electronic form (e.g., in an integrated system).
- Auditors may apply the knowledge obtained from understanding the information system(s) relevant to financial reporting (**Pitfall 3**) when determining whether the environment is highly automated, with little or no manual intervention.
- If auditors are in this situation:
  - certain controls associated with the highly automated processing environments are relevant to the audit (see **Pitfall 5** for Continuous Improvement Tips)
  - the entity's controls over IT risks are relevant to the audit (see **Pitfall 3** for Continuous Improvement Tips).

Appendix 1—Key Terminology and Concepts Referred to in This Tool

Key Terminology and Concepts

The following terminology and concepts are relevant to the reader of this *Tool*:

Internal Control: An internal control is a process 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 term "controls" refers to any aspects of one or more of the components of internal control. A control will prevent a misstatement from occurring or detect and correct it. [CAS 315.4(c)]

Components of Internal Control: The division of internal control into the following five components for purposes of the CASs provides a useful framework for auditors considering how different aspects of an entity's internal control may affect the audit: [CAS 315.A59]

1. control environment
2. entity's risk assessment process
3. information system, including the related business processes, relevant to financial reporting, and communication
4. control activities
5. monitoring of controls.

This division does not necessarily reflect how an entity designs, implements and maintains internal control, or how it may classify any particular component.

Control environment: The control environment includes the governance and management functions and the attitudes, awareness, and actions of those charged with governance and management concerning the entity's internal control and its importance in the entity. The control environment sets the tone of an organization by influencing the control consciousness of its people. [CAS 315.A77]

Elements of the control environment that may be relevant when obtaining an understanding of the control environment include the following: [CAS 315.A78]

- communication and enforcement of integrity and ethical values. These are essential elements that influence the effectiveness of the design, administration and monitoring of controls.
- commitment to competence. Matters such as management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.

- participation by those charged with governance. Attributes of those charged with governance such as:
  - their independence from management
  - their experience and stature
  - extent of their involvement and the information they receive, and the scrutiny of activities
  - appropriateness of their actions, including the degree to which difficult questions are raised and pursued with management and their interaction with internal and external auditors.

- Management's philosophy and operating style: characteristics such as management's:
  - approach to taking and managing business risks
  - attitudes and actions toward financial reporting
  - attitudes toward information processing, accounting functions and personnel.

- Organizational structure: framework within which an entity's activities for achieving its objectives are planned, executed, controlled and reviewed

- Assignment of authority and responsibility: matters such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established.

- Human resource policies and practices: policies and practices that relate to, for example, recruitment, orientation, training, evaluation, counselling, promotion, compensation, and remedial actions.

Entity's risk assessment process: The entity's risk assessment process forms the basis for how management determines the risks to be managed. If that process is appropriate in the circumstances, including the nature, size, and complexity of the entity, it assists the auditor in identifying risks of material misstatement. Whether the entity's risk assessment process is appropriate to the circumstances is a matter of judgment. [CAS 315.A88]

Control activities: Control activities are the policies and procedures that help ensure management directives are carried out. Control activities, whether within automated or manual systems, have various objectives and are applied at various organizational and functional levels. Control activities may be designed to achieve one or more of the following objectives: [CAS 315.A99]

- authorization
- performance reviews
- information processing
- physical controls
- segregation of duties.

Information system(s) relevant to financial reporting: The information system relevant to financial reporting objectives, which includes the accounting system, consists of the procedures and records designed and established to: [CAS 315.A90]

- initiate, record, process, and report entity transactions (as well as events and conditions) and to maintain accountability for the related assets, liabilities, and equity
- resolve incorrect processing of transactions (e.g., 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
- transfer information from transaction processing systems to the general ledger
- capture information relevant to financial reporting for events and conditions other than transactions (e.g., the depreciation and amortization of assets and changes in the recoverability of accounts receivables)
- ensure information required to be disclosed by the applicable financial reporting framework is accumulated, recorded, processed, summarized, and appropriately reported in the financial statements.

Communication: The entity's communication of the financial reporting roles and responsibilities and of significant matters relating to financial reporting involves providing an understanding of individual roles and responsibilities pertaining to internal control over financial reporting. It includes such matters as the extent to which personnel understand how their activities in the financial reporting information system relate to the work of others and the means of reporting exceptions to an appropriate higher level within the entity. Communication may take such forms as policy manuals and financial reporting manuals. Open communication channels help ensure exceptions are reported and acted on. [CAS 315.A97]

Monitoring of controls: Monitoring of controls is a process to assess the effectiveness of internal control performance over time. It involves assessing the effectiveness of controls on a timely basis and taking necessary remedial actions. Management accomplishes monitoring of controls through ongoing activities, separate evaluations, or a combination of the two. Ongoing monitoring activities are often built into the normal recurring activities of an entity and include regular management and supervisory activities. [CAS 315.A110]

Management's monitoring activities may include using information from communications from external parties such as customer complaints and regulators' comments that may indicate problems or highlight areas in need of improvement. Management's monitoring of controls is often accomplished by management's or the owner-manager's close involvement in operations. This involvement will often identify significant variances from expectations as well as inaccuracies in financial data leading to remedial action for the identified control. [CAS 315.A112]

Monitoring of controls is not the same as the measurement and review of financial performance.[17] Monitoring of controls is specifically concerned with the effective operation of internal control. The measurement and review of financial performance is directed at whether business performance is meeting the objectives set by management (or third parties). [CAS 315.A45]

Application Controls: Application controls are manual or automated procedures that typically operate at a business process level and apply to the processing of transactions by individual applications. Application controls can be preventive or detective in nature and are designed to ensure the integrity of the accounting records. Accordingly, application controls relate to procedures used to initiate, record, process and report transactions or other financial data. These controls help ensure that transactions occurred, are authorized, and are completely and accurately recorded and processed. Examples include edit checks of input data, and numerical-sequence checks with manual follow-up of exception reports or correction at the point of data entry. [CAS 315.A109]

Application controls include automated controls and manual controls that use information produced by IT (i.e., system-generated report or a spreadsheet).

"What can go wrong" at the assertion level (as it relates to internal control): The auditor is required to relate the identified risks to "what can go wrong" at the assertion level, taking into account the relevant controls the auditor intends to test. [CAS 315.26(c)] When describing "what can go wrong" at an entity, it is helpful to describe the risk in a way specific to your client's business processes.

Evaluating the design of a control: Evaluating the **design** of a control involves considering whether the control, individually or in combination with other controls, is capable of effectively preventing, or detecting and correcting, material misstatements. [CAS 315.A74] An improperly designed control represents a control deficiency, which may be determined to be a significant deficiency in internal control. A lack of controls related to a risk of "what can go wrong" also represents a control deficiency, which may be determined to be a significant deficiency in internal control.

Determining whether a Control has been Implemented: Determining whether a control has been **implemented** means that the control exists and that the entity is using it as designed. There is little point in determining whether a control has been implemented if the control is inappropriately designed; thus, the design of a control is considered first. [CAS 315.A74]

17 "The auditor shall obtain an understanding of … the measurement and review of the entity's financial performance." [CAS 315.11(e)]

Downstream impact of the controls on the entity's control environment, risk assessment process, communication, and monitoring of controls on the relevant control activities: The results of the auditor's evaluation of the design and implementation of the entity's control environment, risk assessment process, communication, and monitoring of controls may affect the evaluation of the design and implementation of the relevant control activities. For example, if, in the auditor's judgment, the auditor concludes that the tone at the top is not appropriately designed or implemented, the auditor may determine that certain control activities may not be designed or implemented appropriately.

Upstream impact of control activities: The results of the auditor's evaluation of design and implementation of relevant activity-level controls may impact the evaluation of the design and implementation of the entity's control environment, risk assessment process, communication, and monitoring of controls. For example, significant deficiencies in the design or implementation of control activities could be an indication certain controls within the entity's control environment, risk assessment process, communication, and monitoring of controls are not appropriately designed or implemented.

Narrative: A narrative represents a written description of a workflow or process.

Flowchart: A flowchart is a diagram that represents a workflow or process that shows the steps as boxes of various kinds, and their order by connecting them with arrows.

Appendix 2—Overview of the CAS Requirements Referenced in This *Tool*

It is strongly recommended and encouraged that practitioners reading this *Tool* refer to the *CPA Canada Handbook–Assurance* to review the CAS requirements related to internal controls.

The following CAS requirements are referred to in this *Tool*:

Paragraph from the *Handbook*
Paragraph 12 of CAS 315—The auditor shall obtain an understanding of internal control relevant to the audit. Although most controls relevant to the audit are likely to relate to financial reporting, not all controls that relate to financial reporting are relevant to the audit. It is a matter of the auditor's professional judgment whether a control, individually or in combination with others, is relevant to the audit.
Paragraph 13 of CAS 315—When obtaining an understanding of controls that are relevant to the audit, the auditor shall evaluate the design of those controls and determine whether they have been implemented, by performing procedures in addition to inquiry of the entity's personnel.
Paragraph 14 of CAS 315—The auditor shall obtain an understanding of the control environment. As part of obtaining this understanding, the auditor shall evaluate whether: a. management, with the oversight of those charged with governance, has created and maintained a culture of honesty and ethical behavior; and b. the strengths in the control environment elements collectively provide an appropriate foundation for the other components of internal control, and whether those other components are not undermined by deficiencies in the control environment.
Paragraph 15 of CAS 315—If the entity has established a risk assessment process, the auditor shall obtain an understanding of it, and the results thereof.
Paragraph 16 of CAS 315—If the entity has established such a process (referred to hereafter as the "entity's risk assessment process"), the auditor shall obtain an understanding of it, and the results thereof. If the auditor identifies risks of material misstatement that management failed to identify, the auditor shall evaluate whether there was an underlying risk of a kind that the auditor expects would have been identified by the entity's risk assessment process. If there is such a risk, the auditor shall obtain an understanding of why that process failed to identify it, and evaluate whether the process is appropriate to its circumstances or determine if there is a significant deficiency in internal control with regard to the entity's risk assessment process.
Paragraph 17 of CAS 315—If the entity has not established such a process or has an ad hoc process, the auditor shall discuss with management whether business risks relevant to financial reporting objectives have been identified and how they have been addressed. The auditor shall evaluate whether the absence of a documented risk assessment process is appropriate in the circumstances, or determine whether it represents a significant deficiency in internal control.

Paragraph from the *Handbook*

Paragraph 18 of CAS 315—The auditor shall obtain an understanding of the information system, including the related business processes, relevant to financial reporting, including the following areas:

a. The classes of transactions in the entity's operations that are significant to the financial statements;
b. The procedures, within both information technology (IT) and manual systems, by which those transactions are initiated, recorded, processed, corrected as necessary, transferred to the general ledger and reported in the financial statements;
c. The related accounting records, supporting information and specific accounts in the financial statements that are used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information is transferred to the general ledger. The records may be in either manual or electronic form;
d. How the information system captures events and conditions, other than transactions, that are significant to the financial statements;
e. The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures; and
f. Controls surrounding journal entries, including non-standard journal entries used to record non-recurring, unusual transactions or adjustments.

Paragraph 19 of CAS 315—The auditor shall obtain an understanding of how the entity communicates financial reporting roles and responsibilities and significant matters relating to financial reporting, including:

a. Communications between management and those charged with governance; and
b. External communications, such as those with regulatory authorities.

Paragraph 20 of CAS 315—The auditor shall obtain an understanding of control activities relevant to the audit, being those the auditor judges it necessary to understand in order to assess the risks of material misstatement at the assertion level and design further audit procedures responsive to assessed risks. An audit does not require an understanding of all the control activities related to each significant class of transactions, account balance, and disclosure in the financial statements or to every assertion relevant to them.

Paragraph 21 of CAS 315—In understanding the entity's control activities, the auditor shall obtain an understanding of how the entity has responded to risks arising from IT.

Paragraph 22 of CAS 315—The auditor shall obtain an understanding of the major activities that the entity uses to monitor internal control over financial reporting, including those related to those control activities relevant to the audit, and how the entity initiates remedial actions to deficiencies in its controls.

Paragraph 30 of CAS 315—In respect of some risks, the auditor may judge that it is not possible or practicable to obtain sufficient appropriate audit evidence only from substantive procedures. Such risks may relate to the inaccurate or incomplete recording of routine and significant classes of transactions or account balances, the characteristics of which often permit highly automated processing with little or no manual intervention. In such cases, the entity's controls over such risks are relevant to the audit and the auditor shall obtain an understanding of them.

Resources

- Implementation Tool for Auditors—Identifying, Assessing and Responding to the Risk of Material Misstatement Due to Fraud in Revenue Recognition
- Implementation Tool for Auditors—Testing Journal Entries and Other Adjustments: Responding to the Risk of Management Override of Controls
- Implementation Tool for Auditors—Auditing Accounting Estimates
- Audit Client Briefing—Relevant Considerations for Management in the Determination of Accounting Estimates
- Audit & Assurance Alert: Challenges in Meeting the Requirements in CAS 540, Accounting Estimates
- CPA Canada Webinar: CAS 540, Accounting Estimates
- Committee of Sponsoring Organizations of the Treadway Commission (COSO)—Internal Control over Financial Reporting—Guidance for Smaller Public Companies (Guidance for Smaller Public Companies)
- AICPA Audit Guide—Assessing and Responding to Audit Risk in a Financial Statement Audit (September 2014)

Consultation and Feedback

In the interest of continuous improvement and our commitment to the development of quality non-authoritative guidance, we would welcome any comments or questions regarding this non-authoritative guidance by March 31, 2018. Comments on this *Implementation Tool for Auditors*, or suggestions for future publications should be sent to:

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

CPA Canada wishes to express its gratitude to the author of this publication, Juli-ann Gorgi, CPA, CA, MAcc and to CPA Canada's Advisory Group on Audit Guidance and the Advisory Group on the Implementation of the CASs who assisted in the authoring and review of this publication. Both Advisory Groups are comprised of volunteers from the following Canadian firms: BDO, Deloitte, Ernst & Young, Grant Thornton, KPMG, MNP, and PwC.