Canadian Public Accountability Board
Conseil canadien sur la reddition de comptes

SEPTEMBER 2020

COVID-19 Insights:
Understanding internal control in the audit

Entities have been adapting to the COVID-19 pandemic by reimagining their business models and operations. Many have expanded their digital footprints and implemented virtual work environments to protect the health and safety of staff and customers.

These changes give rise to new business risks that may adversely impact an entity's ability to achieve its financial reporting objectives. The adequacy of management's responses to these risks, including the implementation of well-designed controls, impacts the auditor's assessment of risks of material misstatement and the nature, timing and extent of further audit procedures.

The Canadian Public Accountability Board (CPAB) is focused on audit quality and protecting the investing public during this crisis. In coordination with the audit firms we regulate, the accounting profession, standard setters and other regulators in Canada and abroad, CPAB is actively identifying the challenges auditors are facing and providing our perspectives on key issues related to the performance of high-quality audits. This publication highlights considerations for auditors as they obtain an understanding of internal controls to inform their risk assessments in audits performed during the pandemic.

1 UNDERSTANDING INTERNAL CONTROLS

Obtaining an understanding of relevant controls, including changes to controls made by entities to respond to the pandemic, is required even when auditors adopt a fully substantive audit approach. Auditors obtain that understanding by evaluating the design of those controls and determining whether they have been implemented. This helps auditors assess risks of material misstatement and design audit approaches to address those risks.

Risk assessments will be more challenging because of the scope of changes auditors are likely to encounter in 2020 audits.

Components of internal control

1. Control environment
2. The entity's risk assessment process
3. The information system and communication
4. Control activities
5. Monitoring of controls

Control environment

Auditors may find that the focus on maintaining a satisfactory control environment at some entities has been diverted away by other priorities.

The control environment[1] sets the tone of an organization, influencing the control consciousness of its people. It 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 to the entity.

Considerations for auditors include:

- Have attitudes toward information processing and accounting functions and personnel changed? For example, have staff layoffs led to staff performing functions that were previously regarded as incompatible related to authorizing (initiating) transactions, custody of assets and record-keeping?
- Have attitudes changed related to overrides of internal controls to support operational expediencies during the disruption?
- Has appropriate attention been dedicated to remediating findings and recommendations from internal or external auditors?
- Have those charged with governance challenged strategic decisions taken by management to respond to the crisis and exercised appropriate oversight of internal controls implemented to achieve those strategic objectives?

The existence of a satisfactory control environment can be a positive factor when the auditor assesses risks of material misstatement.

> An unsatisfactory control environment may undermine the effectiveness of the other components of internal control. It may also be indicative of elevated risks of material misstatement, including the risk of fraud, that apply pervasively to the financial statements.

The entity's risk assessment process

Understanding the entity's risk assessment process[2] is perhaps even more relevant for auditors in the current environment because management has the best vantage point to identify, assess and respond to the rapidly emerging business risks affecting their entities.

Auditors may find it useful to review the minutes of crisis management meetings held by management during the period of disruption. This will give auditors an opportunity to understand what business risks management thinks are impacting the achievement of their business objectives and whether management is appropriately responding to those risks, including implementing well-designed controls.

A satisfactory risk assessment process by the entity helps the auditor identify risks of material misstatement.

> Auditors may identify, based on their own knowledge of how the entity has been impacted by the pandemic, risks of material misstatement that have not been identified by management. This may be indicative of a significant deficiency in the entity's risk assessment process.

[1] Refer to the extant Canadian Auditing Standard (CAS) 315, *Identifying and assessing the risks of material misstatement through understanding the entity and its environment*, paragraphs 14 and A76-A86 for the requirements and application guidance related to understanding the **control environment**.

[2] Refer to CAS 315, paragraphs 15-17 and A87-A88 for the requirements and application guidance related to understanding **the entity's risk assessment process**.

The information system and communication

Auditors should expect to see changes to entities' information systems, including the related business processes, relevant to financial reporting, and communication[3]. For example, changes are likely to arise because of entities' digital transformation initiatives that respond to the disruption. They may involve business processes and specifically how business transactions are initiated, recorded, processed, and reported in entities' information systems.

These changes may also impact how the entities communicate financial reporting roles and responsibilities pertaining to internal control over financial reporting including the means of reporting exceptions to an appropriate higher level within the entity.

Because of the pace of change in the current environment, auditors may find it necessary to perform walk-throughs of selected transactions for an entity's main transaction cycles to understand the applicable processes and changes to the information system and communication.

> Walk-throughs may be necessary because alternative ways of obtaining this understanding may not be as reliable. For example, finance personnel may not have current information on changes to business processes and, similarly, policy/procedural manuals may be out-of-date in this fast-paced environment.

Control activities

Auditors should expect to identify changes to control activities[4], including new control activities, implemented by management to respond to new business risks related to financial reporting objectives affecting their entities.

Relevant control activities include those that relate to significant risks[5].

Auditors will likely identify and assess more significant risks in their 2020 audits. Significant risks often relate to non-routine transactions or judgemental matters[6]. For example, auditors may determine that the measurement uncertainty associated with a variety of estimates made by management in the current environment should be assessed as significant risks. Examples include impairment assessments for long-lived assets, intangible assets and goodwill, allowances for credit losses, going concern, etc.

> Auditors may find that some entities have not implemented control activities that respond to new significant risks identified in the audit because of competing demands on management's time and resources. Such gaps should be regarded as indicators of significant deficiencies in internal control.

Monitoring of controls

Auditors obtain an understanding of the major activities that the entity uses to monitor internal controls[7] relevant to financial reporting and how the entity initiates remedial action to deficiencies in its internal controls.

Auditors should anticipate that some entities have scaled back their monitoring of controls, including monitoring performed by internal audit, if applicable, to redirect resources and staff to other operational functions and priorities.

> Insufficient monitoring activities, including delays in remediating deficiencies in internal controls, is an indicator of a significant deficiency in management's monitoring process.

[3] Refer to CAS 315, paragraphs 18, 19 and A89-A95 for the requirements and application guidance related to understanding **the information system, including the related business processes, relevant to financial reporting, and communication**.

[4] Refer to CAS 315, paragraphs 20, 21 and A96-A105 for the requirements and application guidance related to understanding **control activities** relevant to the audit.

[5] CAS 315, paragraphs 29 and A137-139

[6] CAS 315, paragraphs 28 and A132-A135.

[7] Refer to CAS 315, paragraphs 22-24, A106-A117 for the requirements and application guidance related to understanding **monitoring of controls**.

2 RISKS ARISING FROM USE OF INFORMATION TECHNOLOGY

The disruption has led many entities to accelerate digital transformations of their information systems. Drivers that are causing this trend include:

- Enhancing their digital interactions with customers to respond to customer preferences for reduced face-to-face sales and servicing.
- Undergoing end-to-end digitization of their value chains including automation, artificial intelligence and workflow enhancements.
- Transitioning their workforces to a virtual work environment to minimize business interruptions.

These changes give rise to risks from the use of information technology (IT). When such risks are identified, auditors are required to obtain an understanding of relevant internal controls, including IT general controls and application controls, that respond to those risks.

Auditors should look out for the following internal control deficiencies in the current environment:

- Reduced compliance with policy and procedures related to the granting and management of access privileges may lead to unauthorized or inappropriate access privileges for IT applications and databases.
- Reduced compliance with program change controls may lead to unauthorized or untested changes to key IT applications.
- Changes to key IT applications made by IT personnel in the production environment, bypassing policies and procedures, to expedite the implementation of changes to those systems may have unintended consequences.
- Reduced IT monitoring activities may delay or inhibit management's ability to respond to risks in an appropriate and timely manner.
- Fewer IT staff due to staff layoffs may lead to delays in implementation of critical IT projects.

Cybersecurity considerations

An auditor's consideration of risks arising from the use of IT may include the risk of unauthorized access by external parties.

Cybersecurity risks may be relevant to auditors because of the sharp rise in cyber incidents during this period and the vulnerability of extended virtual work networks to cyber attacks. Cyber attacks may impact IT applications, databases and operating systems relevant to financial reporting.

Auditors should obtain an understanding of the risk of unauthorized access by external parties to critical financial reporting infrastructure and, if applicable, how the entity is managing those risks.

[8] CAS 315, paragraphs 21 and A103-105.

3 UNDERSTANDING INTERNAL CONTROLS TO ASSESS FRAUD RISKS

Understanding an entity's internal controls is also meant to inform an auditor's assessment of risks of material misstatement due to fraud. Auditors are required to treat identified fraud risks as significant risks and, accordingly, to obtain an understanding of internal controls that mitigate those risks[9].

Earlier this year, CPAB published the results of a thematic review carried out in our 2019 inspections to evaluate how well auditors were complying with Canadian Auditing Standard 240, *The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements*. Although the thematic review was about audits in a pre-COVID-19 world, the areas described may be even more relevant today.

CPAB recommended that auditors enhance their understanding of the following areas to help them better identify and assess fraud risks:

- Management's fraud risk management program including internal controls designed to prevent or detect fraud.
- The entity's whistleblower program.
- Management's compensation arrangements and analyst expectations.

We also recommended that auditors consider engaging forensic experts for more complex entities, even in the absence of an actual or suspected fraud, to help them perform fraud risk assessments, including obtaining an understanding of relevant internal controls that relate to identified fraud risks.

Auditors should expect that the disruption has increased fraud risks for some entities.

The financial strains faced by entities in the current environment create incentives or pressures to commit fraud. Opportunities to commit fraud may also be present when the components of internal control have become misaligned with an entity's business risks. For example, layoffs of key personnel that perform important control activities may provide opportunities for fraud to occur because controls may be vulnerable to being circumvented.

[9] CAS 240, *The auditor's responsibilities relating to fraud in an audit of financial statements*, paragraph 28.

4 USE OF SERVICE ORGANIZATIONS

The pandemic has been just as disruptive for service organizations as it has been for the entities that use their services (user entities).

In the current environment, the outsourcing by user entities of aspects of their businesses to service organizations poses additional challenges to auditors of user entities. For example, service delays or interruptions in the service organizations' operations can give rise to additional business risks for user entities. Similarly, changes to internal controls or the identification of significant deficiencies at service organizations could delay or limit the scope of work by service auditors which, in turn, may delay or limit the scope of financial statements audits of entities that use the services of those organizations.

Considerations for auditors of user entities include:

- Obtaining an understanding of whether management has considered service gaps, service delays and ineffective controls at service organizations in the entity's risk assessment process.
- Assessing management's responses to such risks, including the design and implementation of compensating controls.
- Evaluating the impact on the financial statement audit of delays in receiving service auditors' reports, truncated periods covered by the reports, and internal control deficiencies or scope limitations disclosed in the service auditors' reports.

> Auditors should obtain an understanding of whether management is appropriately identifying and responding to business risks that are arising from adverse impacts of the disruption on the service organizations used by the entity.

5 REMOTE AUDIT CONSIDERATIONS

We anticipate that many auditors will continue to perform their audits remotely for the remainder of the year. The following will be relevant to auditors that carry out remote audit procedures:

Authenticity of documents

Auditors should exercise an appropriate level of professional skepticism when accepting documents as authentic given that most of the audit evidence they will obtain in a remote audit will be received electronically. When scans of original documents are received, auditors may consider requesting that the entity mail a sample of those original documents so that auditors can compare them to the scanned versions.

Field of view

The field of view of an auditor will be constrained when performing the audit remotely. For example, where auditors have historically observed the operation of a control by sitting with the control owner, auditors may have difficulty during a video conferencing meeting discerning which report parameters are being input by the control owner into an IT system. Auditors should carefully consider whether they are able to obtain sufficient appropriate audit evidence when tests and procedures are performed remotely.

Internal controls that cannot be tested remotely

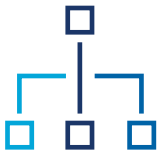
There may be some internal controls that auditors determine cannot be tested remotely. For example, auditors may determine that they will not be able to evaluate the design and implementation of physical access controls in a video conference. Auditors should carefully consider whether compensating controls exist for those controls that can be tested remotely. When it is not practicable to obtain sufficient appropriate audit evidence regarding the entity's internal controls, auditors should consider the implications of those limitations to their audits.

6 PRACTICAL IMPLICATIONS

Timing of an auditor's understanding of internal controls

When performing risk assessments, auditors need to consider whether performing one set of walk-throughs of transactions that occurred during the period of disruption is enough to obtain an understanding of relevant internal controls. Auditors may determine, for example, that there are two distinct periods that are relevant to their risk assessments: a pre-COVID-19 period and a COVID-19 period.

Auditors should consider performing two distinct risk assessments, one for each period to design procedures to address different risks of material misstatement that they may assess for each period.



Revisiting risk assessments throughout the audit

An auditor's risk assessment is an iterative and dynamic process that happens throughout the entire audit process. New challenges for entities are likely to emerge throughout the year and entities will be responding fluidly to emerging risks. We expect that auditors will revisit their risk assessments to ensure that they reflect changes to the entity and its environment, including the entity's internal controls identified during the audit. In some cases, auditors may need to modify previously planned audit procedures or design new procedures to respond to revised risk assessments.

Involving more experienced members of engagement team

Audit engagement leaders should consider involving more experienced staff to test the design and implementation of relevant internal controls or to closely supervise that work. Because of the changes that auditors are likely to encounter in internal controls at many entities, it will not be as straightforward as rolling forward business process narratives or control testing documentation from the prior year audit file.

Learn More

Visit us at www.cpab-ccrc.ca and join our mailing list. Follow us on Twitter — @CPAB-CCRC

www.cpab-ccrc.ca / Email: info@cpab-ccrc.ca

cpab ccrc Canadian Public Accountability Board
Conseil canadien sur la reddition de comptes