CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Frequently Asked Questions

CAS 315 and the Auditor's Responsibilities for General IT Controls

NOVEMBER 2023

DISCLAIMER

The foundation of this FAQ is based on the Australian Auditing and Assurance Standards Board (Australian AUASB) Bulletin: ASA 315 and the Auditor's Responsibilities for General IT Controls published in June 2022 by the Australian AUASB and is used with permission of the Australian AUASB.

This *FAQ* is intended to assist practitioners in the implementation of CAS 315, *Identifying and Assessing the Risks of Material Misstatement*, but is not intended to be a substitute for reading the standard itself. It does not address all requirements in CAS 315 and focuses on only selected requirements.

Executive summary

The term General IT Controls (GITCs) and its variations (such as IT General Controls) is an often-misunderstood term given the fast-paced change in technology and related impact on organizations. The term originated when enterprise computing consisted of mainframe computers housed in centralized data centres and managed by IT departments. These IT departments developed common management processes and related controls (such as security administration, program change management and data processing controls, etc.) that were applied across all of the systems and applications under their management. As such the term "general" IT controls applied to all of the enterprise's systems and applications that operated within that processing environment.

In today's processing environment however, the "centralized" management and control of IT systems and applications is often no longer the case. While "IT departments" still manage many of the "enterprise" level systems and applications, very often systems and applications are managed by various departments within the organization and/or end-users themselves, and in some cases may be outsourced to third-party service organizations.

23-3154

Introduction

This FAQ has been prepared to assist auditors in understanding the role of GITCs in the audit of financial statements and the auditor's responsibilities related to GITCs.

This issue is particularly relevant as a result of the modernized and revised CAS 315, *Identifying and Assessing the Risks of Material Misstatement*, which became effective for audits of financial statements for periods beginning on or after December 15, 2021, and has been enhanced to include auditor considerations in relation to technology, including new and updated appendices for understanding IT and GITCs.

The objective of this publication is to address common questions from auditors about GITCs in the audit of financial statements and the auditor's responsibilities related to GITCs throughout the audit, not just as part of risk assessment in CAS 315. The responses to these common questions are presented as FAQs on pages 7-19.

This publication reinforces that the auditor is not responsible for understanding and testing all GITCs within an entity's control environment. The auditor's responsibility is limited to controls which are relevant to the preparation of the financial statements as identified by the auditor in paragraph 26 of CAS 315.

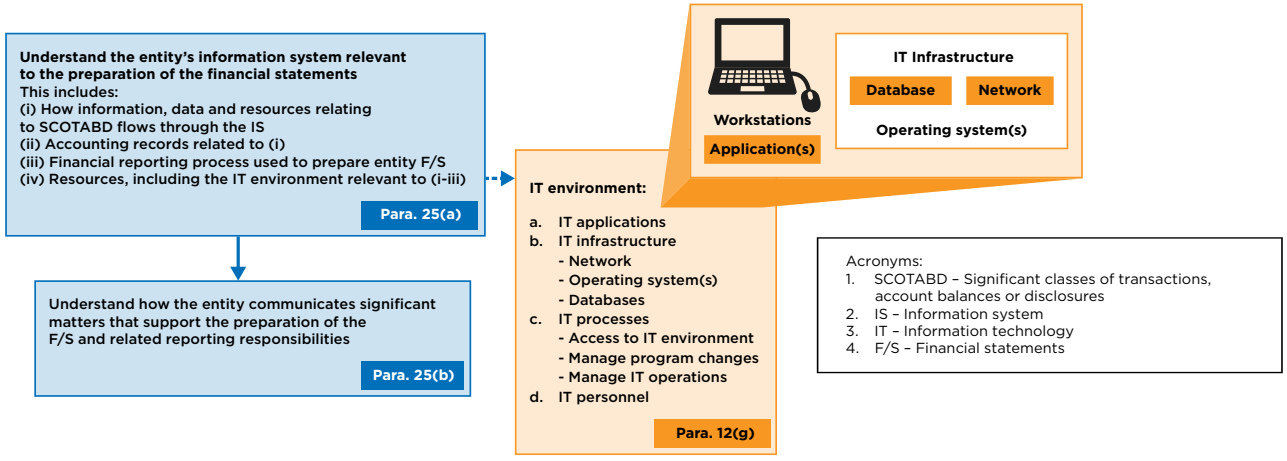
The auditor's understanding of the technology environment and the identification of GITCs

CAS 315 includes significant new material related to technology and the audit of financial statements and has clarified the auditor's responsibilities related to GITCs and the impact they have on how the auditor obtains sufficient appropriate audit evidence.

While GITCs on their own are not sufficiently precise to respond to risks of material misstatement, they are still an important part of the entity's system of internal control and support the operation of automated controls and the integrity of data related to the preparation of the financial statements.

Note: Some of the explanations below use excerpts from the Flowchart, *Understanding the Entity's Use of IT*, in Appendix B of the CAS 315 Implementation tool.

CAS 315, paragraph 25(a) requires the auditor to obtain an understanding of the entity's information system relevant to the preparation of the financial statements as follows:



Obtaining an understanding of the entity's information system is important as this includes the policies that define the flows of transactions and other aspects relevant to the preparation of the financial statements. This information can help inform the auditor in identifying appropriate risks of material misstatement at the financial statement and assertion level. Using the understanding of the IT environment obtained in paragraph 25, the auditor may identify risks arising from the use of IT based on the controls identified in paragraph 26.

Determining whether there are risks arising from the use of IT, and what those risks are, drives whether the auditor needs to identify GITCs that address those risks. Depending on the nature and circumstances of the engagement, the engagement team may consider whether an IT specialist or others are needed to help gain that understanding and identify those risks. Even when the auditor does not plan to test the operating effectiveness of identified controls, the auditor is still required to obtain an understanding of the entity and its environment, the applicable financial reporting framework and the components of the entity's system of internal control, as this understanding may still affect the design of the nature, timing and extent of substantive audit procedures.[1]

The IT environment includes all the various applications, IT infrastructure and related management processes and personnel operating throughout the entity that is relevant to the preparation of the financial statements. There could be many different locations, or "processing environments" where information, data and resources are processed, within the entity's overall IT environment as well as in third-party service organizations. Identifying and differentiating between the various processing environments (and identifying whether they are relevant to the preparation of the financial statements) is important, as while the IT risks (see discussion below) could be similar, the controls to mitigate those risks could be different.

1 See application material A125 of CAS 315.

In CAS 315, paragraph 26(a) the auditor is required to identify controls that address risks of material misstatement at the assertion level as follows:

> CAS 315, paragraph 26(a)
>
> Identifying controls that address risks of material misstatement at the assertion level in the control activities component as follows:
>
> i. controls that address a risk that is determined to be a significant risk;
>
> ii. controls over journal entries, including non-standard journal entries used to record non-recurring, unusual transactions or adjustments;
>
> iii. controls for which the auditor plans to test operating effectiveness in determining the nature, timing and extent of substantive testing, which shall include controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence; and
>
> iv. other controls that the auditor considers are appropriate to enable the auditor to meet the objectives of paragraph 13 with respect to risks at the assertion level, based on the auditor's professional judgment.

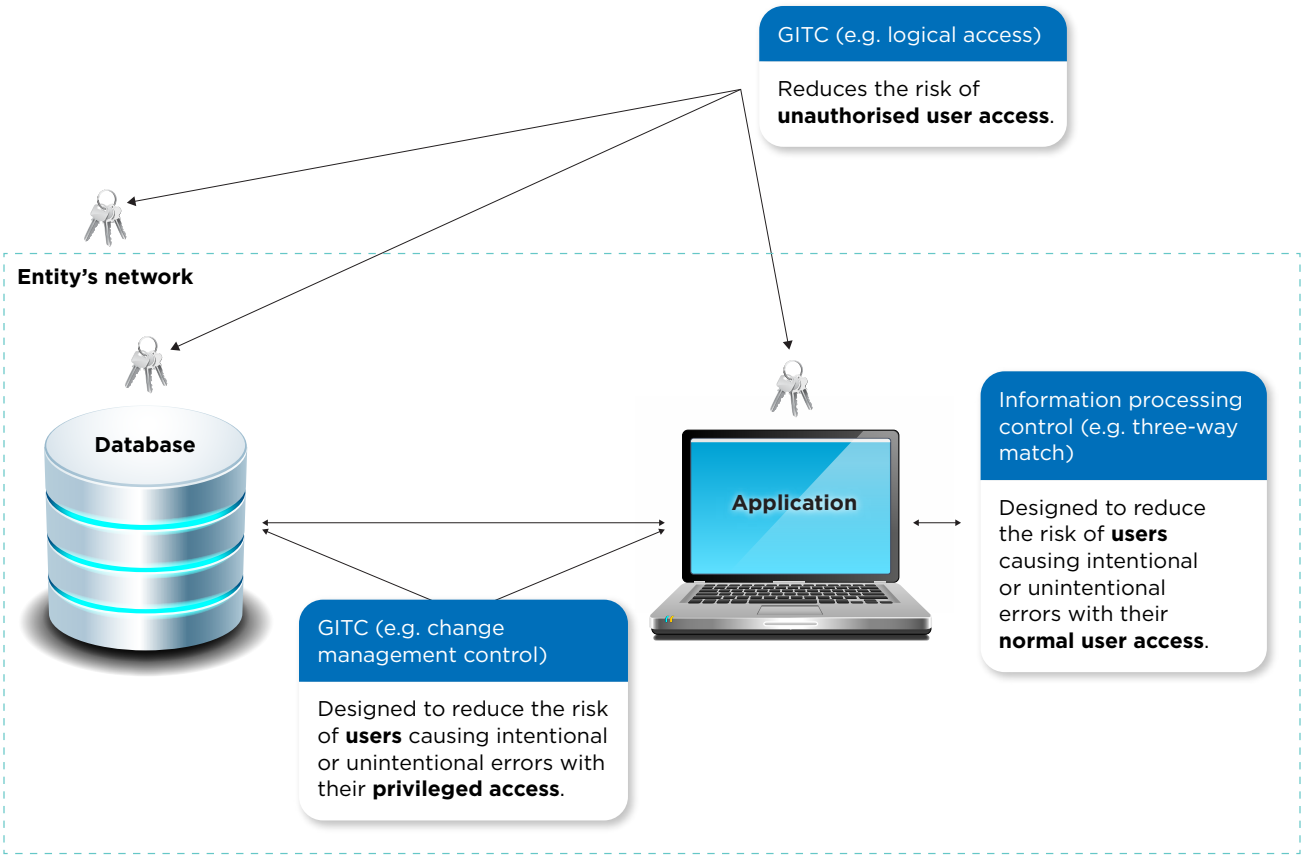
These controls can be information processing controls (see FAQ 2).

Based on the understanding obtained in paragraph 25(a) and the identification of controls activities in paragraph 26(a), the auditor is required to identify the IT applications and other aspects of the entity's IT environment that are subject to risks arising from the use of IT (see FAQ 1).

Where no applications or other elements of the IT environment are subject to risks arising from the use of IT there is no requirement to identify GITCs or evaluate the effectiveness of their design and determine whether they have been implemented.

The auditor determines whether there are risks arising from the use of IT, and if so, responds as follows:

Figure 1 - General IT controls and information processign controls



For example, a three-way match functionality (shown in the diagram above) programmed into an application is an example of an information processing control (in this case an automated control) designed to reduce the risk of errors in the financial data by only processing transactions which have a matching purchase order, vendor shipping document and vendor invoice.

GITCs may be designed to reduce the risk arising from the use of IT related to inappropriate 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. They could also be designed to reduce the risk arising from the use of IT related to the possibility of personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties.

Other GITCs may include:

- Controls within processes that manage logical access privileges to the application are intended to prevent unauthorized users from accessing the application, reducing the risk of erroneous or fraudulent transactions being processed. However, they typically do not prevent authorized users from making errors once they are in the application.

- Controls within processes that manage logical access privileges to the database are intended to limit who can make changes to the entity's data (other than through transactions processed within the application) thereby reducing the risk of erroneous or fraudulent manipulation of the data. They typically do not prevent authorized users from erroneously or fictitiously altering data.
- Controls within database and application change management processes are intended to reduce the risk that changes to the applications or database result in the systems operating in a way that is inconsistent with management's objectives.

Applications are what typical users see (e.g., SAP, People Soft, etc.), they are the systems by which normal users input and view data. Where the data is actually stored is underlying databases which are accessible by privileged users (generally IT personnel). While the auditor's focus may be on the risks within applications, the auditor should also consider risks arising from other elements of the IT environment such as databases as well as from personnel not involved in inputting data through applications but who have privileged access to databases etc.

It is worth noting that the IT processes, and the corresponding GITCs within those processes, may differ between the various processing environments throughout the organization:

- they may be centralized (e.g., within the entity's IT department) and perhaps applicable to multiple application systems
- they may be decentralized (e.g., departmental responsibility for a given application such as the Finance department managing their General Ledger application) and unique to each application
- they may be user-centric (e.g., a spreadsheet application designed and managed by an end-user) and unique to each end-user
- they may be outsourced (e.g., processes that manage the applications that process an entity's payroll at a third-party service organization)

In summary, while information processing controls address the risk related to integrity of the information (i.e. the completeness, accuracy and validity of transactions and other information) within a specific application, GITCs encompass broader controls that support the continued proper operation of the IT environment, including the effective functioning of information processing controls and the integrity of information in the entity's information system. When information processing controls that are subject to risks arising from IT are identified and GITCs address those risks, then both of these controls play a role in the identification and assessment of risks of material misstatement in the financial statements.

FAQ 3 – When do I need to evaluate the design and determine the implementation of GITCs?

In accordance with CAS 315, paragraph 26(d),[6] the auditor is required, for identified GITCs that address the risks arising from the use of IT, to evaluate whether the GITC is designed effectively to support the operation of other controls and determine whether it has been implemented. When

6 See application material in CAS 315, paragraphs A175–A181 for additional guidance.

risks arising from the use of IT are identified, and GITCs are identified to address such risks, the auditor evaluates the design and determines if the GITC is implemented. This is required regardless of whether the auditor plans to test the operating effectiveness of controls as part of the auditor's planned response to address the assessed risks of material misstatement.

Evaluating the design of an identified control involves the auditor's consideration of whether the control, individually or in combination with other controls, is capable of effectively preventing, or detecting and correcting, material misstatements. The implementation of a control is determined by establishing that the control exists and that the entity is using it. This cannot be done through inquiry alone. Additional procedures such as observing the application of the control or inspecting documents and reports may corroborate the inquiry about how the control is designed or implemented, or it may provide the auditor with new information that could impact their risk assessment and related response.

Auditors may need to involve others with specialist skills such as IT auditors (or service organization auditors – see FAQ 9) to assist them to:

- understand IT applications, IT infrastructure, IT processes
- identify risks arising from the use of IT
- identify the GITCs that address the risks arising from the use of IT
- evaluate the design and implementation, and if applicable, test the operating effectiveness of the relevant GITCs

It is the responsibility of the engagement partner under CAS 220, *Quality Management for an Audit of Financial Statements* to determine that members of the engagement team, and any auditor's external experts and internal auditors who provide direct assistance who are not part of the engagement team, collectively have the appropriate competence and capabilities, including sufficient time, to perform the audit engagement.[7]

FAQ 4 – When does the operating effectiveness of GITCs need to be tested?

Where the auditor plans to test the operating effectiveness of identified information processing control(s) as part of the auditor's response to address the assessed risk of material misstatement, and those control(s) are supported by GITCs, the auditor determines whether it is necessary to obtain audit evidence supporting the effective operation of those GITCs within the processing environment(s) in order to rely on the identified control(s).

Where the auditor does not plan to test the operating effectiveness of information processing control(s) as part of their response to address the assessed risks of material misstatement, the auditor does not need to test the operating effectiveness of relevant GITCs.

7 See paragraph 26 of CAS 220.

If the auditor concludes that a GITC is deficient, but still plans to test the operating effectiveness of the identified control, then the auditor considers the nature of the related risk(s) arising from the use of IT to provide a basis for additional procedures that address the assessed risk of material misstatement. Such procedures may address whether:

- the related risk(s) arising from the use of IT occurred
- any alternate, redundant or compensating controls exist and operate effectively, at a level of precision sufficient to address the related risk(s) arising from the use of IT

While the most common reason that the operating effectiveness of a GITC is tested is to support the auditor's assessment of the operating effectiveness of information processing controls, there may be other instances where evidence about the operating effectiveness of GITCs is relevant for other procedures which may include:

- substantive analytical procedures – GITCs may be relevant where the auditor needs evidence over the reliability of data to be used in a substantive analytical procedure and has determined that this is most efficiently done through testing the operating effectiveness of information processing controls. In this situation, the auditor is testing the operating effectiveness of information processing controls to provide evidence about the completeness, accuracy and validity of data which is forming part of the auditor's substantive analytical procedures (e.g., unit rates from a master list which will be used to recalculate the value of a certain class of transactions).
- controls over journal entries[8] – When testing non-standard journal entries as part of journal entry testing, the auditor may choose to test the operating effectiveness of GITCs that manage permissions for posting non-standard journal entries.
- custom built reports or client data – Where the auditor's substantive procedures utilize system-generated reports or client data received in electronic format, the auditor may test the operating effectiveness of GITCs that address the risk of inappropriate or unauthorized changes to the report or data, in addition to controls over the completeness and accuracy of the report or data. (See FAQ 7 for more information about this).
- automated interface - When information flows from one application or system to another system (e.g., sales transactions recorded by point of sale system at retail store level automatically interfaces with the accounting system / general ledger system), the auditor may test the operating effectiveness of GITCs that address the risk of inaccurate, incomplete or unauthorized processing of data between the two interfaces.

8 See CPA Canada CAS 315 Implementation Tool N2 and N3 for questions related to journal entries.

FAQ 5 – How will the nature of GITCs vary based on the complexity of the entity's IT environment?

The nature of GITCs which respond to risks arising from the use of IT may vary depending on the complexity of the IT environment. Appendix 6 of CAS 315 provides examples of common risks arising from the use of IT and GITCs which respond to those risks, as well as differences by complexity of the IT applications.

Example

In a less complex IT environment GITCs may also be less complex (e.g., the entity uses widely used purchased applications and does not have access to source code and vendor provided updates are reviewed, evaluated and tested prior to implementation), compared to a more complex IT environment where processes that manage user access privileges and changes to applications and other IT components are complex, involve multiple people, and may utilize automated tools and IT management applications.

The extent of the auditor's work around GITCs is a matter of professional judgement. The auditor is not responsible for identifying all controls within the entity's control environment including its processing environment(s).

FAQ 6 – Do GITCs have to be tested every year?

There are audit procedures related to GITCs that are required to be completed every year, including:

- understanding the IT processes
- identifying GITCs that address the risks arising from the use of IT (see FAQ 1)
- when risks arising from the use of IT are identified and GITCs are identified to address such risks, evaluating the design and determining the GITC is implemented (see FAQ 3)

Regarding testing the operating effectiveness of GITCs, in certain circumstances, the auditing standards allow auditors to use audit evidence about the operating effectiveness of controls obtained in previous audits. CAS 330, *The Auditor's Responses to Assessed Risks*, paragraph 13 outlines the considerations for the auditor when determining whether it is appropriate to use audit evidence about the operating effectiveness of controls obtained in previous audits. However, the standards are not explicit about whether these considerations also apply to GITCs. As GITCs ensure the consistent operation of information processing controls, the auditor may decide to test them annually.

In other circumstances, audit evidence obtained from previous audits may provide audit evidence where the auditor performs audit procedures to establish its continuing relevance and reliability. For example, in performing a previous audit, the auditor may have determined that a GITC was functioning as intended. The auditor may obtain audit evidence to determine whether changes

to the GITC have been made that affect its continued effective functioning through, for example, inquiries of management and the inspection of logs to indicate what controls have been changed. Consideration of audit evidence about these changes may support either increasing or decreasing the expected audit evidence to be obtained in the current period about the operating effectiveness of the GITC.

FAQ 7 – If I plan to test the operating effectiveness of GITCs, what is the impact of GITCs not being appropriately designed and implemented or not operating effectively?

CAS 315, paragraph 34 requires the auditor to assess control risk as part of their assessment of the risk of material misstatement at the assertion level, if the auditor plans to test the operating effectiveness of GITCs.

Whether the auditor plans to test the operating effectiveness of GITCs is based on the expectation that they are operating effectively and forms the basis of the auditor's assessment of control risk. The auditor develops the expectation that GITCs are operating effectively based on the auditor's evaluation of the design, and the determination of implementation, of the identified controls in paragraph 26.

Where GITCs are not appropriately designed and/or implemented, the auditor considers the impact of this on their assessment of control risk in accordance with paragraph 34 of CAS 315.[9] When a particular GITC is not designed or implemented properly, the auditor's assessment of control risk may take into account whether:

- there are any alternate GITCs, or any other controls, that address the related risk(s) arising from the use of IT
- the auditor can design suitable substantive procedures to address the applicable risks arising from the use of IT

Examples:

- When assessing the design of controls over application changes, the auditor concluded that controls to ensure that all changes were authorized by management were not appropriately designed. However, other application change controls, including controls over completeness and accuracy of the application change log, were appropriately designed and were operating effectively. The auditor determined that they can manually review the application change log, and determine whether any unauthorized changes occurred during the period which would have an impact on the operating effectiveness of the automated information processing control.

9 CAS 315, paragraph A229

- Upon review of processes for the management of a spreadsheet that provides/contains information intended to be used as audit evidence, the auditor concluded that while data input controls, and controls over access to the spreadsheet were designed and operating effectively, there were not sufficient controls over changes to the formulae within the spreadsheet. At appropriate times throughout the audit period, the auditor could independently validate the output generated by the spreadsheet through the use of automated tools and techniques.

Where there are no alternate GITCs or the auditor is unable to design suitable substantive procedures to address the applicable risks arising from the use of IT, the auditor may be unable to rely on:

- the operating effectiveness of automated controls within the affected application, without obtaining sufficient direct evidence that the relevant automated controls operated effectively throughout the audit period (as GITCs may not appropriately prevent or detect unauthorized program changes or access to applications);
- the completeness, accuracy and validity of system-generated reports or client data received in electronic form used for audit purposes, or other reports built in-house by the audit client and IT-dependent manual controls that rely on such reports or data (as the integrity of the information content of such reports or data may not be guaranteed); and
- the operating effectiveness of input controls which provide assurance over data entered into a system (as the application may fail to sufficiently reduce the risk of intentional and unintentional erroneous changes to data after it has been entered into the system). This may also affect any substantive analytical procedures that the auditor may have planned to undertake which relies on point in time data.

In addition to the matters raised above as part of the auditor's consideration of the impact of GITCs not being designed or implemented properly, the auditor may also consider:

- whether the risk of material misstatement is required to be revised to reflect the new information about the operating effectiveness of controls in accordance with CAS 315, paragraph 37
- where there are one or more control deficiencies, whether they represent a significant deficiency and require a report to those charged with governance in accordance with CAS 265, *Communicating Deficiencies in Internal Control to Those Charged with Governance and Management*

In circumstances where the auditor has determined, in accordance with CAS 315, paragraph 33, that substantive procedures alone cannot provide sufficient appropriate audit evidence to address a risk and alternative procedures are unable to be performed, there may be an impact on the auditor's ability to obtain sufficient appropriate audit evidence and the audit opinion.

FAQ 8 – Are GITCs relevant if I am taking a substantive approach?

As outlined above, understanding the IT processes to manage access, to manage program changes and to manage IT operations is required as part of understanding the entity's information system relevant to the preparation of the financial statements. GITCs include controls over the entity's IT processes.

Furthermore, GITCs are important as they address risks arising from the use of IT; that is risks to the completeness, accuracy and validity of information in the information system. (See FAQ 4 for discussion on testing operating effectiveness of GITCs.)

When taking a substantive approach, GITCs are still relevant for the auditor to evaluate the design of the process controls and determine whether these controls have been implemented. Testing the operating effectiveness of GITCs may be relevant even if the auditor is intending to respond to a risk through performing substantive procedures.

For example, when the auditor intends to use information produced by the entity in their substantive test(s) (e.g., system-generated reports or client data received in electronic format) as audit evidence and that information is produced by an application, the auditor may plan to test the information processing controls within that application that ensures the completeness and accuracy of the system-generated reports or client data received in electronic format, including identifying and testing the GITCs that address risks arising from the use of IT (e.g., inappropriate or unauthorized program changes or direct data changes to the reports).

In some instances, the auditor may be able to test the completeness and accuracy of system-generated reports or client data received in electronic format substantively while in other instances, due to the complexity of the system, the auditor may not be able to test the completeness and accuracy of the system generated report or data substantively. In those cases, consideration should be made as to whether it is more efficient to test the information processing controls and related GITCs.

Regardless of whether the auditor plans to test the operating effectiveness of controls, the auditor is required to obtain an understanding of the control activities component in accordance with CAS 315, paragraph 26, which may include evaluating the design and determining the implementation of GITCs. See FAQ 3 for considerations on evaluating the design and determining the implementation of GITCs.

FAQ 9 – What are some considerations when the entity uses third-party services as part of its information system relevant to the preparation of the financial statements?

It is important for the auditor to obtain a sufficient understanding of whether the entity being audited uses third-party services in their operations. These third parties may or may not be considered a service organization to the entity being audited, as this depends on how the entity interacts with them.

When obtaining an understanding of the entity's system of internal control in accordance with CAS 315 the auditor shall identify controls in the control activities component at the entity, from those that relate to the services provided by the service organization, including those that are applied to the transactions processed by the service organization for the entity, and evaluate their design and determine whether they have been implemented.[10] See CPA Canada's new FAQ publication (coming soon) for further considerations regarding CAS 402, *Audit Considerations Relating to an Entity Using a Service Organization*.

About this publication

The Research, Guidance and Support group of the Chartered Professional Accountants of Canada (CPA Canada) undertakes initiatives to support practitioners and their clients in the understanding and implementation of standards. As part of these initiatives, the CPA Canada Advisory Group on the Implementation of Canadian Auditing Standards (Advisory Group) provides advice on the identification of issues related to the implementation of Canadian Auditing Standards (CASs) and on the development of non-authoritative implementation guidance related to these issues. The Advisory Group includes volunteers from the following Canadian firms: BDO, Deloitte, EY, Grant Thornton, KPMG, MNP and PwC.

This paper was developed and reviewed with the support of several volunteers, including CPA Canada's Advisory Group on the Implementation of the CAS and certain AASB technical staff and members. CPA Canada expresses its appreciation to all of the volunteers for their support in preparing this publication.

10 CAS 402, paragraph 10

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, questions and suggestions regarding this *Frequently Asked Questions* at the following address:

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