HOW TO GUIDE - SEPTEMBER 2021

ITGC RISK ASSESSMENT QUESTIONNAIRE

BDO

CONTENTS

GO FORWARD
GO BACK
RETURN TO INDEX

INTRODUCTION

This publication provides guidance to engagement teams on completing 2.06.02 - ITGC Risk Assessment Questionnaire in APT Next Gen. The purpose of this questionnaire is to effectively identify risks arising from the entity's use of IT and their IT general controls (ITGCs) that address such risks.

This questionnaire replaces the ITGCs section of the old UIC-CARA & ITGCs questionnaire. Relevant information from the prior year's UIC-CARA & ITGCs, such as our documentation of the design of an ITGC, can be copied into the ITGC Risk Assessment Questionnaire where applicable.

The auditor's understanding of the entity and its environment, the applicable financial reporting framework, and the entity's system of internal control are interdependent with concepts within the requirements to identify and assess the risks of material misstatement. In obtaining the understanding required by Revised ISA 315[1], initial expectations of risks may be developed, which may be further refined as the auditor progresses through the risk identification and assessment process.

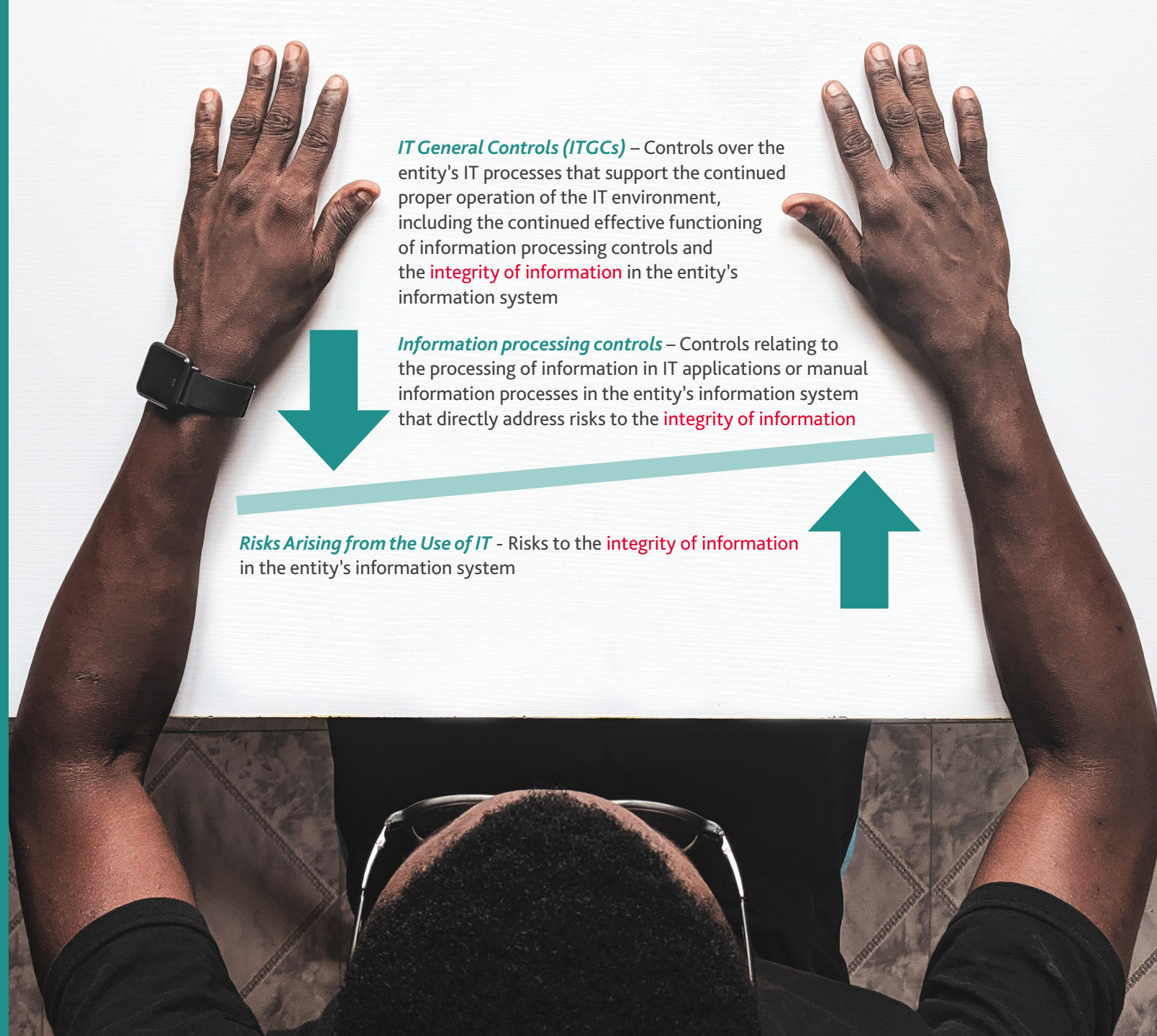
The '*Understanding Your IT Environment*' (UITE) (document 2.06.01 in the international APT library content) is available to assist in gathering the relevant information about the IT environment, which is a necessary first step in the IT risk assessment process.

The publication *How to Guide – Understanding Your IT Environment Template* provides guidance to engagement teams to effectively obtain an understanding of an entity's Information Technology (IT) environment.

[1] International Standard on Auditing 315 (Revised 2019) – Identifying and Assessing the Risks of Material Misstatement.

1.

ISA 315 definitions related to IT and information processing risk and controls



2.

What are the steps within the ITGC Risk Assessment Questionnaire?

STEP 1: IDENTIFYING IT APPLICATIONS RELEVANT TO THE AUDIT AND INCIDENTS THAT OCCURRED DURING THE YEAR

STEP 2:
- CHARACTERISTICS OF IT APPLICATION A * - REVENUE CYCLE
- CHARACTERISTICS OF IT APPLICATION B * - PAYROLL CYCLE
- CHARACTERISTICS OF IT APPLICATION C * - FRCP CYCLE

STEP 3:
- ANALYSIS OF IT RISKS AND RELEVANT ITGCS FOR APPLICATION A
- ANALYSIS OF IT RISKS AND RELEVANT ITGCS FOR APPLICATION B
- ANALYSIS OF IT RISKS AND RELEVANT ITGCS FOR APPLICATION C

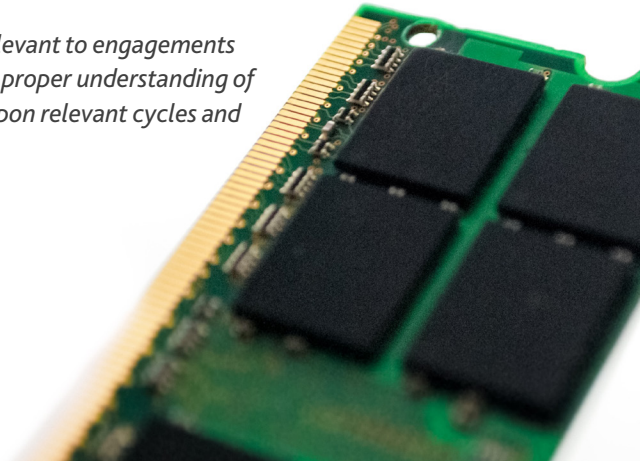
STEP 4: IDENTIFYING CHARACTERISTICS OF THE IT ENVIRONMENT THAT MAY GIVE RISE TO IT RISKS

STEP 5: ANALYSIS OF IT RISKS FOR THE IT ENVIRONMENT, INCLUDING RELEVANT ITGC ASSESSMENT

IS AUDIT SPECIALIST INVOLVE-MENT MAY BE REQUIRED IN ALL OR SOME OF THESE STEPS

(SEE RELEVANT SECTIONS BELOW FOR MORE DETAILS)

** Note that the cycles listed in Step 2 above are merely examples. Applications relevant to engagements will vary by engagement and each engagement team should, in turn, ensure that a proper understanding of the processes performed by each respective client is obtained before concluding upon relevant cycles and relevant applications.*



3.

Guidance on completing the ITGC Risk Assessment Questionnaire

HOW TO COMPLETE STEP 1

How to identify the list of relevant IT applications

As a starting point for identifying potential relevant IT applications:

- Refer to the Understanding Your IT Environment template (UITE) – section 1.6, Applications Used by the Entity. Through our understanding of the IT environment, we may conclude that not all of the IT applications listed within the UITE are relevant to the audit (see below). Engagement teams may document this evaluation process and the considerations that led engagement teams to exclude certain IT applications from the list of relevant IT applications within the UITE or within the Comments field of the ITGC Risk Assessment Questionnaire, Section 1.1, Identifying IT applications relevant to the audit.
- Review our systems descriptions and walkthrough documentation for business cycles with IT applications, as IT applications that are relevant to the audit may extend beyond the accounting or general ledger software package generating the financial statements. For example, inventory systems may feed the general ledger changes in inventory quantities and costing prices; and production or shipping systems may trigger invoicing and revenue recognition.

PRACTICAL GUIDANCE ON COMPLETING THE UITE

Engagement teams may send the UITE template to the entity to complete. In some cases, the entity may fail to list a relevant application or decide that some applications are not relevant; therefore, we recommend direct inquiries with the entity's IT and accounting/finance functions as well and a review of the business cycles narratives or walkthrough working papers to ensure completeness of IT applications identified.

Determining which IT applications are relevant to the audit

When understanding the entity's information systems, we consider all of the IT applications that are relevant to the audit. Audit Manual paragraphs 14.136 – 14.138 state that an IT application is relevant to the audit if:

- Automated or IT-dependent control activities relevant to the audit (CARA) use information from, or depend on processes performed by, the IT application (even if the engagement team is not planning to do TOCs on those CARA); or
- The IT application produces reports or other IPE that will be used in the audit that we do not plan to verify substantively.

CONTROL ACTIVITIES RELEVANT TO THE AUDIT (CARA)

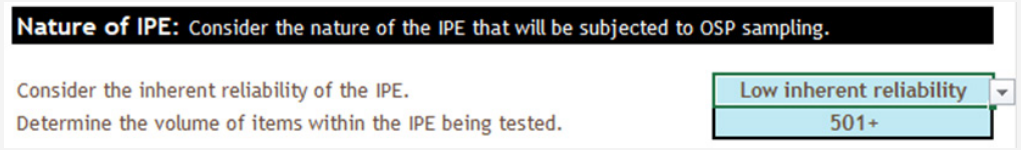
Control activities relevant to the audit include:

- Controls that address significant risks
- Controls over journal entries
- Controls where operating effectiveness testing shall be performed to reduce substantive audit testing
- Controls over related party relationships, related party transactions and arrangements, and significant transactions and arrangements outside the normal course of business
- Other controls that the auditor considers appropriate, based on the auditor's professional judgment.

TESTING IPE SUBSTANTIVELY

CARA identified by engagement teams may depend on system-generated reports, in which case the IT applications are relevant to the audit as they may be subject to risks arising from the use of IT. Even where no CARA have been identified for an IT application, or CARA do not use information from, or depend on processes performed by, the IT application, engagement teams may plan to rely on system-generated reports or other IPE, which may also be subject to risks arising from the use of IT. In such cases, if the engagement team decides to test such IPE substantively by directly testing the inputs and outputs of such reports, they do not need to identify the related IT applications as relevant to the audit.

However, if we are planning to verify these system-generated reports / IPE substantively using the IPE Sample Size Calculator template, because we have not done any controls work on that IPE, we need to select 'low inherent reliability' within the Nature of IPE section.



Depending on the Risk Conclusion and the importance of the IPE to the audit procedures being performed, the IPE sample size could be as high as 60 items. Therefore, it may make sense to include IT applications that produce IPE as IT applications relevant to the audit.

Audit Manual paragraph 14.110 states that based on controls identified, the auditor should identify the IT applications and the other aspects of the entity's IT environment that are subject to risks arising from the use of IT.

Engagement teams obtain the entity's list of IT applications from section 1.6 of the Understanding the IT environment form: 'List of applications / systems / data warehouses relevant for processing and recording of financial information'. Engagement teams must decide which of these IT applications are relevant to the audit and which ones are not. It is expected that most IT applications used in processing and recording financial information that eventually is included in the financial statements will be relevant to the audit. However, in some circumstances, engagement teams may decide that an IT application can be excluded from the list of IT applications relevant to the audit that is recorded in the ITGC Risk Assessment Questionnaire. Below are some considerations that may indicate that an IT application is not relevant to the audit:

- The IT application processes a low volume of transactions and the IPE from that IT application can be easily audited substantively (perhaps 100% of the transactions)
- The IT application processes a low volume of transactions with low values that could not result in an IRMM
- The IT application supports a business cycle/ function that could not result in an IRMM
- The IT application processes financial information but it is not used in financial reporting or in obtaining audit evidence
- The IT application is used only to archive historical financial information.

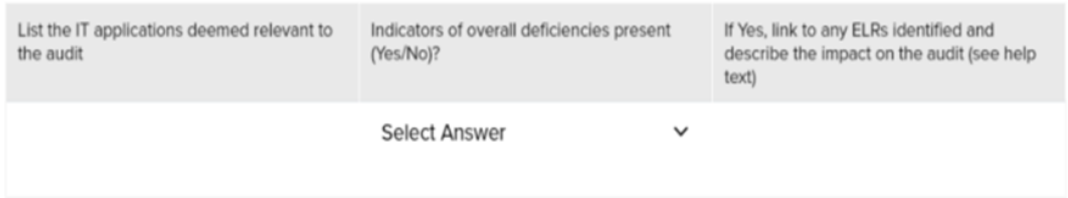
Please note that engagement teams should not just assume that IT applications are not relevant to the audit by saying that the IPE will be tested substantively. It is generally not feasible to audit IPE substantively if there is a high volume of transactions processed by that IT application.

Additionally, engagement teams may decide to consult with an IS Audit Specialist or other engagement team members about the relevance and completeness of the IT applications, and consider how to address various IT applications that are not strictly financial applications, but may transfer data or information to financial applications, such as time recording systems, CRM (customer relationship management) systems and SCADA (Supervisory control and data acquisition) applications.

Engagement teams should document the conclusion for each IT application they decide is not relevant to the audit in the Understanding Your IT Environment template or add the IT application to the list of IT applications relevant to the audit in the ITGC Risk Assessment Questionnaire.

Completing question 1.1 - Identifying IT applications relevant to the audit

- Based on our identification and evaluation of relevant IT applications, add the IT application(s) deemed relevant to the audit to the first column in the table.
- Place a 'Y' in the second column if the application contains overall deficiencies such that it cannot be relied upon. An application may not be suitable for reliance if:
  - You are already aware that the design of ITGCs is ineffective overall in the current year or significant ITGC deficiencies in the prior year have not been remedied
  - IT resources supporting the IT application are not adequate
  - There are competency concerns with respect to the IT function and its performance.



EXAMPLE 1

WHEN SHOULD ENGAGEMENT TEAMS PLACE A 'Y' IN THE SECOND COLUMN?

An entity uses an off-the-shelf-financial application developed by a small software supplier that went bankrupt last year. The entity's IT department does not have access to the database or software code and cannot export the previous year's financial data to a new IT application. Closing and transferring of previous period balances, which is usually performed by the supplier, was not performed this year.

EXAMPLE 2

WHEN SHOULD ENGAGEMENT TEAMS PLACE A 'Y' IN THE SECOND COLUMN?

An entity has developed its in-house revenue recognition application. In the prior year, the engagement team determined via its walkthroughs that there was no segregation of duties enforced such that developers were not segregated from parties that were able to migrate changes to production. Additionally, those developers served as administrators within the application, and any access administration controls were subject to verbal approval. No audit trails with respect to new hire administration or employee terminations were created or maintained. All of the above failures in design and implementation of ITGCs were documented in our audit files.

EXAMPLE 3

WHEN SHOULD ENGAGEMENT TEAMS PLACE A 'Y' IN THE SECOND COLUMN?

A micro entity has outsourced the IT function to a part time consultant who is not available most of the time to perform the IT operations activities. Therefore, unqualified employees have admin roles and can change the ERP parameters and configurations, generate new reports or install software updates.

If the engagement team determines that overall deficiencies in an IT application relevant to the audit have not been remediated, either an Engagement Level Risk (ELR) or an Inherent Risk of Material Misstatement (IRMM) should be recorded in APT and cross-referenced to the 3rd column in question 1.1 of the ITGC Risk Assessment Questionnaire. Engagement team must plan an overall response to address the ELR, or specific procedures to address the IRMM, and describe the impact on the audit on 2.99 Evaluation of Potential Risks screen. For each ELR, engagement teams should determine if it should also be allocated to particular FSAs (Financial Statement Areas) and assertions. For example, overall deficiencies in a payroll application may affect completeness and accuracy of the payroll expenses and payables.

PRACTICAL GUIDANCE RELATED TO OVERALL DEFICIENCIES:

If the overall deficiencies in the IT application relevant to the audit result in IPE with a high risk of being unreliable, engagement team may consider performing the following procedures (these procedures may require the involvement of an IS Audit Specialist):

- Development process - For newly developed reports, or reports derived from newly developed systems, or special purpose reports designed specifically for the audit, assess the report development process, including user requests, parameters and the appropriateness of user acceptance tests.
- Parallel run - Reports that provide simulations and forecasts designed for planning and preparation of financial estimates can be tested by re-running the model that provides the report based on actual data or by a parallel run in a similar system (if available).
- Test data - input test transactions or data for which we can predict the outcome and match this to the actual report (e.g., by creating exceptions that should be captured in an exception report).
- Code review – perform a review of report queries to analyze the report logic and other parameters.

The ITGC Risk Assessment Questionnaire hides steps 2 and 3 for the IT applications that were identified with overall deficiencies and continues to step 4 if no other relevant IT application are listed.

For all IT applications answered No in the second column of the table, a separate section will be automatically created for completing Steps 2 and 3. The name(s) of those IT applications are automatically transferred to those sections in the questionnaire.

If additional lines to record more IT applications relevant to the audit are needed, click on the plus sign (+) to add a new row.

Completing questions 1.2 and 1.3 - Identifying incidents that occurred during the year

Refer to the UITE – section 3.5.2, Cyber attack /incidents which describe any incidents that occurred during the audited period. The potential RMM (IPE integrity and completeness) that could be present relates to loss of data or data restore (in case of new hardware installation) that may affect the financial data integrity or completeness.

When evaluating the completeness and accuracy of the information included within section 3.5.2, engagement teams should consider other information obtained about incidents, system disruptions or other security events from their understanding of the entity and its information systems, public sources, regulators or internal IS Audit reports as applicable.

EXAMPLE

An entity's third-party supplier may have been subject to a cyber attack; the information about the cyber attack and potential hacker was published on a web portal.

EXAMPLES - POSSIBLE IMPACTS OF CYBER ATTACKS OR SECURITY EVENTS ON THE FINANCIAL STATEMENTS

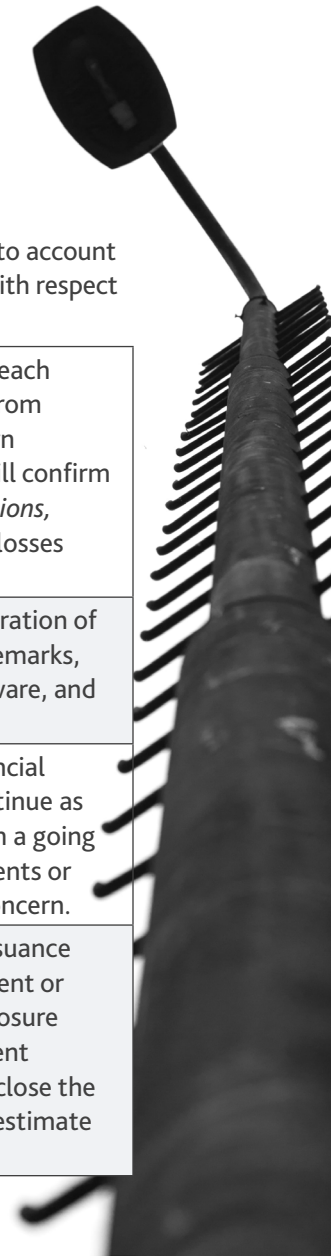
Cyber incidents may have a direct or indirect negative effect on the client's financial statements. An example of a direct effect would be a ransom payment to the threat actor. Examples of indirect impacts could include:

- Temporary interruption to the business cycles
- Hardware replacement and new hardware installation
- Data restore or activation of a secondary data center
- Use of third-party IT companies and/or forensic experts.

Clients may not immediately know the impact of a cyber incident and may be required to develop estimates to account for the various financial implications. Local financial reporting standards may in turn require considerations with respect to either recording or disclosure of contingent liabilities related to the cyber incident.

Liabilities, Provisions and Contingent Liabilities for Losses from Claims	Cyber incidents may result in losses from claims, including those related to warranties, breach of contract, product recall and replacement, and indemnification of counterparty losses from their remediation efforts. Therefore, such cyber incidents may result in liabilities for known obligations, provisions for probable losses or contingent liabilities where a future event will confirm the existence of an obligation. Refer to International Accounting Standard (IAS) 37: *Provisions, Contingent Liabilities* and *Contingent Assets* to determine when to recognize a liability for losses resulting from cyber incidents.
Asset Impairment	Cyber incidents may also result in diminished future cash flows, thereby requiring consideration of impairment of certain assets including goodwill, customer-related intangible assets, trademarks, patents, capitalized software or other long-lived assets associated with hardware or software, and inventory. Therefore, our clients should reassess asset impairment after a cyber incident.
Going Concern	A serious cyber incident with significant implications on the client's business and the financial statements may result in the need for management to consider the entity's ability to continue as a going concern. Even if it is appropriate to continue preparing the financial statements on a going concern basis, disclosure may be required if there are material uncertainties related to events or conditions that may cast significant doubt on the entity's ability to continue as a going concern.
Events After the Reporting Period	To the extent a cyber incident is discovered after the balance sheet date but before the issuance of financial statements, the client should consider whether the incident is an adjusting event or a non-adjusting event after the reporting period. The recognition, measurement and disclosure of subsequent events is addressed in IAS 10: *Events After the Reporting Period*. If the incident constitutes a material non-adjusting subsequent event, the financial statements shall disclose the nature of the incident and an estimate of its financial effect, or a statement that such an estimate cannot be made.

Source: Assurance Matters, Cyber attacks and the audit process (May 2017/ issue 04)



When cyber attacks, system disruptions or other security events have occurred during the year that may have damaged the integrity of the data and/or IT applications that affect financial reporting or may have resulted in the need to recover data affecting financial reporting from backup systems, there is an inherent risk in relation to these events. An IS Audit Specialist should be involved in determining the nature and extent of audit work necessary to address the inherent risk and assist in completing questions 1.2 and 1.3.

HOW TO COMPLETE STEP 2

Question 2.X.1 - Step 2: Characteristics of IT application

A robust understanding of the business cycle and how transactions are initiated, transferred, processed and recorded in the relevant IT application is critical to our understanding and identification of potential risks of material misstatement.

The 4th column in the table below includes references to where the characteristics of the IT application(s) can be found within the UITE. The last column includes further information to support our conclusions as documented within question 2.x.1 in the ITGC Risk Assessment Questionnaire. Question 2.x.1 is replicated for each relevant IT application (i.e., it will be 2.1.1 for the first IT application, 2.2.1 for the second IT application, etc.).

QUESTION NUMBER IN APT	AREA	QUESTION ENGAGEMENT TEAMS NEED TO ANSWER (YES/NO)	UNDERSTANDING YOUR IT ENVIRONMENT - RELEVANT QUESTIONS	EXAMPLES OF CHARACTERISTICS REQUIRING 'YES' RESPONSES
1	Complex user authentication	Does this IT application have any of the following? • Single sign-on? • Central rights management using a dedicated software tool? • Complex multiple level system roles with different rights assignment (e.g., a large number of different roles)?	1.6 and 3.1.2	• The entity's employees use same user account and password to login to the organization's systems, for example the network management application (domain controller), the ERP application and emails • The entity has thousands of users and access rights are granted automatically based on their role, as defined in the employment contract or third-party agreement.
2	Program / configuration changes	Does the entity have the ability (directly or indirectly through the software supplier or a consultant) to do any of the following for this IT application: • Modify the application (make program changes to the system)? • Modify configuration settings with significant financial impact?	3.2	• The entity uses in-house developed billing applications. The IT department employees make changes to the program code based on user requests • The entity uses an ERP application, where a third-party provider modifies the application and/or reports and configuration settings based on users' requests • The entity's IT consultant can modify configuration settings that could pose a risk due to fraud or error, or could significantly impact CARA and/or IPE used in the audit that we do not plan to test substantively (see publication on BDO World called *Understanding and Evaluating Configuration Changes*.).

3	Automated data processing	Does the entity have automated data processing between different systems or applications modules with respect to this IT application, such as: • Custom interfaces between IT applications and the client are not substantively verifying the data transfers using manual controls? • Batch processing (i.e., processing a group (batch) of transactions/ files at one time according to a predefined schedule. This generally does not include items such as accounts payable or payroll batch processing whereby the process is initiated by a user)? • Use of data warehouses to support financial reporting? • Technological complexity to the processing of transactions (e.g., online, real-time, EDI, Blockchain, etc.)?	3.3. and 2.3	• Order details and invoice transferred to the ERP using real time interface developed by the IT department • Batch processing of monthly payroll from the payroll application directly to the general ledger generate summarized accounting entry without supporting reports or batch execution results • Customer aging report is generated from a data warehouse which obtains data from the ERP and the billing system and generates an aggregate/unified report • The entity uses digital wallets to receive payments from customers using PayPal or cryptocurrencies • The entity uses an Electronic Data Interchange (EDI) middleware utility to map customer purchase orders to the sales module in its ERP or revenue recognition system • The entity operates a website and sells products or services through it, such that orders may be placed on the website. Those orders, through an eCommerce middleware tool, are then interfaced to the ERP or revenue recognition system.
4	Data conversion	Was this a new application implemented in the audited period, which would include any of the following situations: • New IT application? • Major system upgrade? • Migration of data to a new system?	1.5 and 3.2.4	• The entity replaced its legacy accounting system with another accounting system supported by a different vendor • The entity upgraded its legacy accounting system from an on-premises version to the same vendor's cloud solution • The entity upgraded its legacy accounting system to a new version supported by the same vendor, but the database must be migrated as well (e.g., SAP ECC to HANA) • The entity recently purchased a new system upon which it will calculate and process its lease expenses.

Definitions and further explanations of the IT terminology being used within this question, along with all other questions within the ITGC Risk Assessment Questionnaire as applicable, can be found in the APT Next Gen help text by selecting the '?' next to the question title as shown below.

Complete the 'Comment' column in question 2.x.1 to document any relevant information supporting our conclusion such as:

- An entity is using different module versions of same ERP application and the single sign-on functionality applies only to some of the modules being used.
- A central rights management system applies only to specific devices accessing the IT application, while other devices are not included in the central rights management system.
- The entity's IT department can modify the application; however, the latest version was not modified since last year's audit, as verified through the application properties screen with Edward Ivy, IT application manager on 3 July 20XX.
- The entity's IT department can modify the configuration settings of reports with financial impact; however, all configuration settings are the same as those identified within the previous year's audit, as verified by the IS Audit Specialist on this audit.
- Custom interfaces between IT applications were changed in the last month of the year so we should focus our testing on data transfers in the last month.

Question 2.X.2 - IS Audit Specialist involvement required

Within Step 2, there is a list of systems characteristics that may suggest the entity is using its system(s) in such a manner that may require IS Audit Specialist involvement. If IS Audit Specialist involvement is necessary, engagement teams record the IS Audit Specialist's name in the ITGC Risk Assessment Questionnaire Comment field.

Consultation with an IS Audit Specialist regarding their involvement in the assessment of relevant ITGCs is mandatory when an event or characteristic of an IT application or the IT environment is true. If the IS Audit Specialist agrees that their involvement is not necessary, document the rationale in the Comments box, and attach the IS Audit Specialist approval.

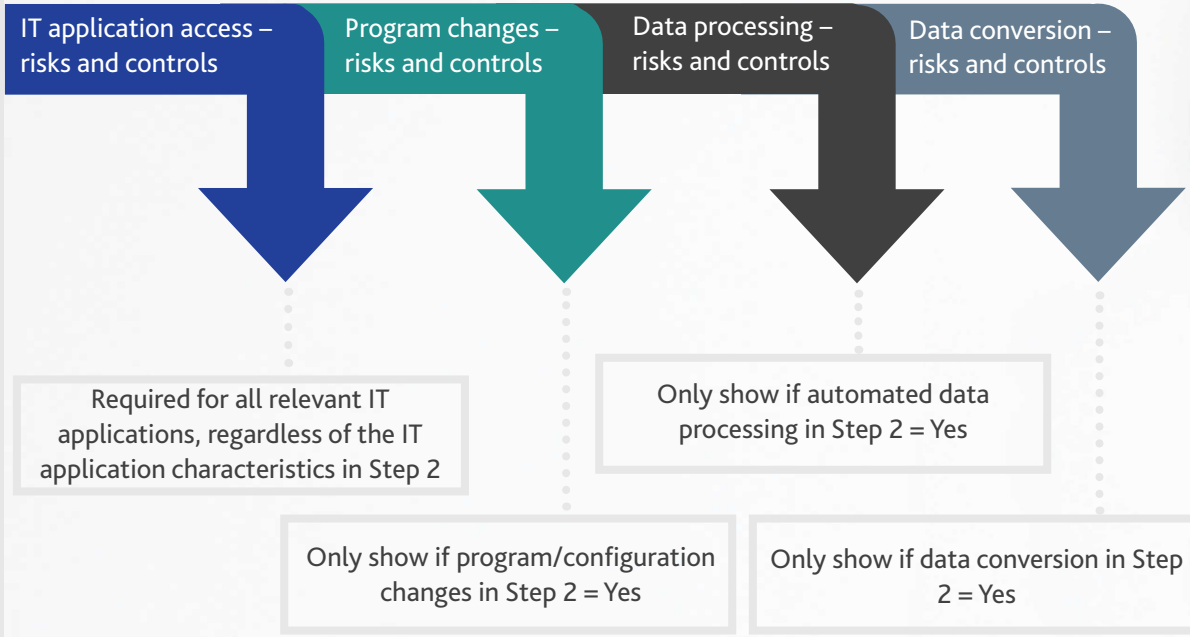
Involvement of an IS Audit Specialist is re-evaluated annually. Approval from the IS Audit Specialist to not be involved must be obtained each year.

The table on the right lists examples of what can go wrong when the IT application characteristics in question 2.x.1 exist and how the IS Audit Specialist can assist the engagement team.

IT APPLICATION CHARACTERISTICS	WHAT CAN GO WRONG?	HOW THE IS AUDIT SPECIALIST CAN ASSIST
Complex user authentication - Single sign-on, central rights management or complex multiple level system roles with different rights assignment (e.g., a large number of different roles)	Misconfiguration or ineffective management of single sign-on, central rights management or complex multiple level system roles may result in unauthorized employees or third-party having access to change financial data.	IS Audit Specialist involvement is necessary to determine whether the design and implementation of those controls relevant to the What Could Go Wrongs are satisfactory or not and correspondingly assist in determining the nature and extent of audit response to address the related IT risks.
Program / configuration changes - IT application or its relevant configuration settings can be modified	Incorrect application code or configuration settings may result in the associated IPE failing to report certain key information (completeness risk) or failing to accurately process transactions, resulting in incorrect presentation of information within the entity's financial statements.	
Automated data processing - Automated data processing between different systems or applications	Incomplete automated data processing may result in financial information failing to be transferred without detection, or partly transferred to the financial application without detection, resulting in incorrect presentation of information within the entity's financial statements.	
Data conversion - New application implemented in the audited period	Incomplete migration of opening balance data or inaccurate mapping of such to the proper chart of accounts could yield inaccurate financial information both during the period and at year end. Incomplete or inaccurate migration of customer, supplier, or other relevant master data files between legacy and new application may result in incomplete or improper accounting for transactions processed within the new system. An entity's failure to design and implement user acceptance testing of key transaction processing events within the new application may result in transactions processed in a manner not in accordance with the entity's expectations and/or not in compliance with accounting standards.	

HOW TO COMPLETE STEP 3 (QUESTIONS 2.X.3.X)

The responses completed within Step 1 and 2 of the questionnaire will automatically populate the relevant ITGC potential risk and control sections as shown below. The purpose of these sections is to understand the IT risks that exist due to characteristics of the IT application and the objectives of Relevant ITGCs that could address those IT risks. The engagement team then identifies the Relevant ITGCs established by the entity to address the IT risks and assesses the design and implementation of those Relevant ITGCs. All tables in this step have the same structure, although the IT risks and objectives columns change in each section.



APPLICATION Q&A

Question: What happens if none of the characteristics in Step 2 are present? Do I still need to perform D&I over ITGCs?

Answer: In the case where all responses to Step 2 are 'No', only the 'Access – risks and controls' section will populate for each relevant IT application. Therefore you will still need to perform D&I over Access ITGCs.

Completing the Risks and Controls tables in Step 3

The following table provides guidance and example documentation on how to complete the Step 3 questions:

COLUMN NUMBER IN THE TABLE	COLUMN CONTENT	ENGAGEMENT TEAM'S EXPECTED ACTION	EXAMPLE DOCUMENTATION
1	IT risks	Understand the pre-populated IT risks at the entity based on our understanding of the IT environment. There are blank rows available to add more IT risks at the end of each question. If any IT risk is believed to be not applicable, document our rationale for that conclusion in the 'Description of the design of the relevant ITGC' column. No further work is required related to that IT risk.	*(All IT risk fields populated with exception of additional 'Other' rows which can be added by the engagement team)* *DPR1 Unauthorized users have access to update the batch jobs (including interface jobs) in the job scheduling software, resulting in inaccurate, incomplete or unauthorized processing of data (Job scheduling).*
2	Objectives of the relevant ITGCs	Consider the pre-populated objective of a relevant ITGC to address the IT risk. This column is meant to provide information to engagement teams to help them identify relevant ITGCs established by the entity that address the listed IT risks. The actual ITGCs established by the entity may not match what is listed in the Objective column.	*(field already populated)* *DPC1 Only authorized users have access to update the batch jobs (including interface jobs) in the job scheduling software.*
3	References	Add cross-references / hyperlinks to relevant systems documentation, design and implementation (D&I) working papers, operating effectiveness (OE) tests / working papers, etc. Consider using the # shortcut in APT.	#2.06 IT Environment - *section 3.3 IT operations (data processing)* #2.05.05 Sales system description #2.05.06 Sales system walkthrough #2.06.02.05 Data processing D&I #2.06.02.06 Data processing operating effectiveness tests
4	Description of the Design of the Relevant ITGC	Record a description of the design of any relevant ITGCs: • The information can be referenced to the UITE or copied in • Once completed, this information can be rolled forward and updated each year, similar to our business cycle understanding.	*The entity has daily batch jobs transferring invoices and orders from the Web shop to the ERP. This procedure is documented in internal accounting and designed as follows:* • *Batch jobs are scheduled in advance to 01:00 hour* • *Only two administrators have access to the scheduling monitor; they can view data but cannot change it* • *Administrators receive an alert in case of batch failure* • *Changes to the batch configuration is performed by programmer and tested by the accounting department* • *Daily reconciliation reports are produced from both systems and reviewed by the sales manager.*

5	ITGC Design Conclusion	For each relevant ITGC, record your design Conclusion (Satisfactory or Unsatisfactory). If unsatisfactory, there is no need to assess implementation of that relevant ITGC.	*Satisfactory*
6	ITGC Implementation Testing	For each relevant ITGC, record your Implementation testing or provide a cross-reference to such testing.	*Engagement team reviewed the following with John Smitt, IT manager on 31 March 2021:* • *Users that can access the batch monitor software and the batch files* • *Sample of alerts or job scheduling notifications* • *Configuration of the batch schedules* • *List of changes to the batch processing interface, including evidence of testing by the accounting department* • *Available reconciliation reports from the application, including evidence of review by the sales manager* *See details of testing performed on #2.06.02.05 Data processing D&I.*[2]
7	ITGC Implementation Conclusion	Record your Implementation Conclusion (Satisfactory or Unsatisfactory) based on implementation testing done.	*Satisfactory*
8	ITGC OE Conclusion	Where you are testing OE of automated or IT-dependent CARA or testing IPE using controls, then you must test OE of the related relevant ITGCs. For each relevant ITGC where you need to test OE, record your OE Conclusion (Satisfactory or Unsatisfactory). If testing of OE of that ITGC is not required, select N/A. If you do plan to test OE, you cannot complete the OE conclusion until after your OE testing is done, so you will have to come back to this question later.	*Satisfactory*

APPLICATION GUIDANCE

If a relevant ITGC covers more than one IT risk, you may record the details for that ITGC once within Step 3 and refer back to that ITGC where relevant to avoid duplicated effort.

Design description documentation of an ITGC within the questionnaire can be used as a base in future years. Engagement teams obtain an understanding of the process each year and can update the design description as applicable.

[2] Rather than recording implementation testing on a separate working paper, engagement teams can choose to record the details of their implementation testing in this column in the questionnaire. The details of the implementation testing need to be sufficient to enable an experienced auditor, having no previous connection to the engagement, to reperform the steps – i.e., which documents were examined, which screens were observed, what the results were, etc. Engagement teams may choose to include screen shots of what was observed when deemed appropriate.

Testing the operating effectiveness of relevant ITGCs

When engagement teams plan to test the operating effectiveness of an automated control, engagement teams also plan to test the operating effectiveness of the relevant ITGCs that support the continued functioning of that automated control to address the risks arising from the use of IT, and to provide a basis for the auditor's expectation that the automated control operated effectively throughout the period.

For example:

- When relevant ITGCs are not designed effectively or appropriately implemented to address risks arising from the use of IT (e.g., controls do not appropriately prevent or detect unauthorized program changes or unauthorized access to IT applications), this may affect the auditor's decision to rely on automated controls within the affected IT applications.
- The ongoing operating effectiveness of an information processing control may depend on certain relevant ITGCs that prevent or detect unauthorized program changes to the IT information processing control. In such circumstances, the expected operating effectiveness (or lack thereof) of the relevant ITGCs may affect the auditor's assessment of control risk (e.g., control risk may be maximum when such relevant ITGCs are expected to be ineffective or if the auditor does not plan to test the operating effectiveness of the relevant ITGCs).
- When information produced by the entity to be used as audit evidence is produced by the IT application, the auditor may decide to test controls over the system-generated reports, including identification and testing of the relevant ITGCs that address risks of inappropriate or unauthorized program changes or direct data changes to the reports. Similar considerations would apply to IT-dependent controls where the person performing the manual part of the control relies on system-generated reports from the IT application (unless we test those reports substantively).

Unsatisfactory conclusion to D&I or OE of one or more controls

The diagram on the right presents the actions required if the engagement team's conclusion for design, implementation and/or operating effectiveness of an ITGC is 'Unsatisfactory':

If design, implementation or operating effectiveness is Unsatisfactory, a question will appear at the end of the section for this IT application called 'Impact of ITGC deficiencies related to this IT Application'.

Record the impact of the unsatisfactory ITGCs on your testing of CARA and/or IPE in this question. For example, one impact may be that you cannot rely on the automated controls and you must test the IPE substantively since relevant ITGCs have deficiencies.

Evaluate whether the ITGC deficiency is already considered as a part or element of a documented RMM. Where it is not, consider adding an RMM in APT to ensure any impacts are integrated into the audit work. Also report the control deficiency to management / those charged with governance (TCWG).

Other implications for the audit when ITGC deficiencies are found include:

- The impact on your assessment of control risk of the related CARA (if applicable)
- The impact on plans to test the operating effectiveness of automated or IT-dependent CARA (if applicable)
- The impact on the testing of IPE (i.e., it will need to be tested substantively) and/or
- The impact on any other audit procedures (e.g., the data from the system may not be sufficiently reliable for use in SAPs or DATs).

To see examples of how engagement teams should document ITGC deficiencies and the impact on the audit, refer to the Assurance Approach and Software Tools publication on BDO World called *ITGC Deficiencies and Possible Audit Responses*.

HOW TO COMPLETE STEP 4 (QUESTION 3.1)

The table below includes references to where the characteristics of the IT environment can be found within the UITE, as well as further information to support our conclusions as documented in Step 4. Should any characteristics be present, IT risks and controls relevant to that area are populated within Step 5 and IS Audit Specialist involvement in evaluating the IT environment is required.

QUESTION NUMBER IN APT	AREA	QUESTION ENGAGEMENT TEAMS NEED TO ANSWER (YES/NO)	UNDERSTANDING YOUR IT ENVIRONMENT - RELEVANT QUESTIONS	EXAMPLES OF CHARACTERISTICS REQUIRING 'YES' RESPONSES
1	Operating system complexity	Does the operating system have one or more of the following characteristics: • Single sign-on? • Any direct linkages to 3rd parties through web-based applications, electronic commerce, electronic data interchange (EDI) related to relevant IT systems identified? • Operating system is complex (anything besides Windows, such as AS400, Unix, etc.)?	1.6, 3.1.1, 3.1.3 and 3.2	• The servers operating system is Unix and is managed by the entity's IT department administrators. • The entity is using a web based electronic commerce solution installed on the local servers to process a material transaction stream. • Third party suppliers have direct link VPN to the entity's servers operating systems with privileged users' roles. • The entity's employees access applications and data warehouse from a remote location using private computers. • The entity manages single sign-on access Microsoft Azure cloud solutions. • Centralized device management using cloud solution, such as the 'Intune' tool.
2	Network security risk	Does the entity have a higher likelihood of network security issues resulting in a risk of material misstatement? For example: • External servers (serverless environment)? • Direct access to third parties – web-based applications, sophisticated electronic commerce, EDI? • Complex network structure with multiple locations?	1.4, 3.1.1, 3.4.2 and 3.5.1	• Third party suppliers and clients have access to the entity's network where they can upload or download documents. • Entity is a financial institution which allows customers to view balances and perform transactions recorded in front office applications. • Virtualized data center, multiple number of servers with different operating systems. • Global company operating in Europe, US and Asia using same IT application and network resources for a central data center.
3	Data backups	Based on your understanding of the IT Environment, are there potential IT risks with data backup that suggest you should evaluate the data backup ITGCs?	3.4.1	• The entity has a serverless environment and does not perform data backup but relies on the cloud data availability. • During the audit period, financial data was lost and was restored from a backup copy.

Question 2.X.2 - IS Audit Specialist involvement required

Consultation with an IS Audit Specialist regarding their involvement in the assessment of relevant ITGCs is mandatory when a characteristic of the IT environment as documented in Step 4 is true. If the IS Audit Specialist agrees that their involvement is not necessary, document the rationale in the Comment box, and attach the IS Audit Specialist approval.

Involvement of an IS Audit Specialist is re-evaluated annually. Approval from the IS Audit Specialist to not be involved must be obtained each year.

Below is a list of characteristics that may suggest the entity's IT environment may require IS Audit Specialist involvement. If IS Audit Specialist involvement is necessary, engagement teams record the IS Audit Specialist's name in the Comment field for question 3.2.

IT APPLICATION CHARACTERISTICS	WHAT CAN GO WRONG?	HOW THE IS AUDIT SPECIALIST CAN ASSIST
Operating system complexity - Single sign-on, direct linkages to 3rd parties or complex operating systems supporting relevant IT application(s)	Ineffective single sign-on management may allow for greater accessibility to relevant financial applications that is beyond the intent of management and beyond the authorized use of employees and third parties, i.e., access in excess of approved job functions may be obtained. Improperly secured interfaces to and from third party systems may allow for theft and/or manipulation of data by unintended parties. Operation of complex operating systems by inexperienced IT personnel may result in unauthorized access to the entity IT environment, loss of data, or fraud.	IS Audit Specialist involvement is necessary to determine the design and implementation of those relevant ITGCs, or if the relevant ITGCs are unsatisfactory, to assist in determining the nature and extent of audit response to address the related IT risks.
Network security risk - External servers (serverless environment), direct access to third parties, web-based applications, sophisticated electronic commerce, EDI or complex network structure with multiple locations	Improperly secured interfaces to and from third party systems may allow for theft and/or manipulation of data by unintended parties. Loss of financial data in transmission may also result. Improperly configured EDI applications, or EDI applications not accurately mapped to the entity's general ledger, revenue, or other relevant system may result in incomplete transmissions of sales or purchase data, or inaccurate transmissions of such data to vendors or customers. Real time transactions processed without appropriately designed and monitored audit trails may result in loss of data, inaccurate processing of such data, and/or incomplete IPE.	
Data backups - Potential IT risks with data backup	In case of a disaster recovery event or other necessary system restoration event, if the data backup is not available or incomplete, financial statements may not be accurate or complete.	

HOW TO COMPLETE STEP 5

The responses completed within Step 4 of the questionnaire will automatically populate the relevant ITGC potential risk and control sections related to the IT environment as shown below. The purpose of these sections is to understand the IT risks that exist due to characteristics of the IT environment, and the objectives of relevant ITGCs that could address those IT risks. All risks and controls tables in Step 5 have the same structure, although the IT risks and objectives columns change in each section.

OPERATING SYSTEM SOFTWARE RISKS & CONTROLS	Only show if operating system complexity in Step 4 = Yes
NETWORK SECURITY RISKS & CONTROLS	Only show if network security risk in Step 4 = Yes
DATA BACKUP RISKS & CONTROLS	Only show if data backups in Step 4 = Yes

The structure of the tables in Step 5 (questions 4.X) are identical to the structure of the tables in Step 3, so follow the guidance provided earlier on how to complete those tables: If design, implementation or operating effectiveness is unsatisfactory, complete the question that appears on 'Impact of ITGC Deficiencies related to IT environment' using the guidance provided in Step 3.

4.

Conclusion

The new ITGC Risk Assessment Questionnaire is designed to help us identify IT applications relevant to the audit, IT risks and corresponding ITGCs in those IT applications, as well as IT risks and ITGCs in the IT environment. It also helps us assess when an IS Audit Specialist needs to be consulted about their involvement in assessing IT applications and the IT environment. Where relevant ITGCs are Unsatisfactory, the questionnaire reminds us to ensure that we modify our audit work appropriately.

For more guidance on completing the ITGC Risk Assessment Questionnaire, see the training video called *2021 Phase 2 Changes to the BDO Audit Approach and APT Next Gen Library.*

CONTACT US:

AUDIT@BDO.GLOBAL

How to Guide is issued by the Global Assurance Department and distributed to the International A&A Coordinators. Please share this publication with relevant partners and staff in your firms.

BDO internal use only.

BDO', 'we', 'us', and 'our' refer to one or more of BDO International Limited, its network of independent member firms ('the BDO network'), and their related entities.

Service provision within the BDO network is coordinated by Brussels Worldwide Services BV, a limited liability company incorporated in Belgium.

Each of BDO International Limited (the governing entity of the BDO network), Brussels Worldwide Services BV and the member firms is a separate legal entity and has no liability for another such entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BV and/or the member firms of the BDO network. Neither BDO International Limited nor any other central entities of the BDO network provide services to clients.

BDO is the brand name for the BDO network and for each of the BDO member firms.