OAG Risk Assessment Process
IT Risks Quick Reference

Office of the
Auditor General
of Canada

Bureau du
vérificateur général
du Canada

Dec–2022
Template Owner: IT Audit

IT Risks Quick Reference Guide

Table of contents

Introduction

This Quick Reference Guide provides an overview of the key concepts and requirements related to understanding an entity's IT environment, identifying IT risks and ITGCs that are responsive to these risks. These topics are covered in more detail in OAG Audit 5035.2 as part of the Understand and Identify phases of the OAG Risk Assessment Process.

It is through the identification of IT applications and other aspects of the IT environment (e.g., databases, operating system, network) relevant to the preparation of the financial statements that engagement teams are able to identify the risks arising from the use of IT and related information technology general controls (ITGCs) that address these risks. This provides the basis for the engagement team to understand the entity, identify and assess risks of material misstatement, assess the control risk as documented by our determination of expected controls reliance (i.e., none, partial or high), and develop effective and efficient audit responses to address the risks of material misstatement.

A summary of key reminders is provided on the next page. This is followed by details of considerations relevant to our understanding of the entity’s IT environment, and identifying IT risks and related ITGCs.

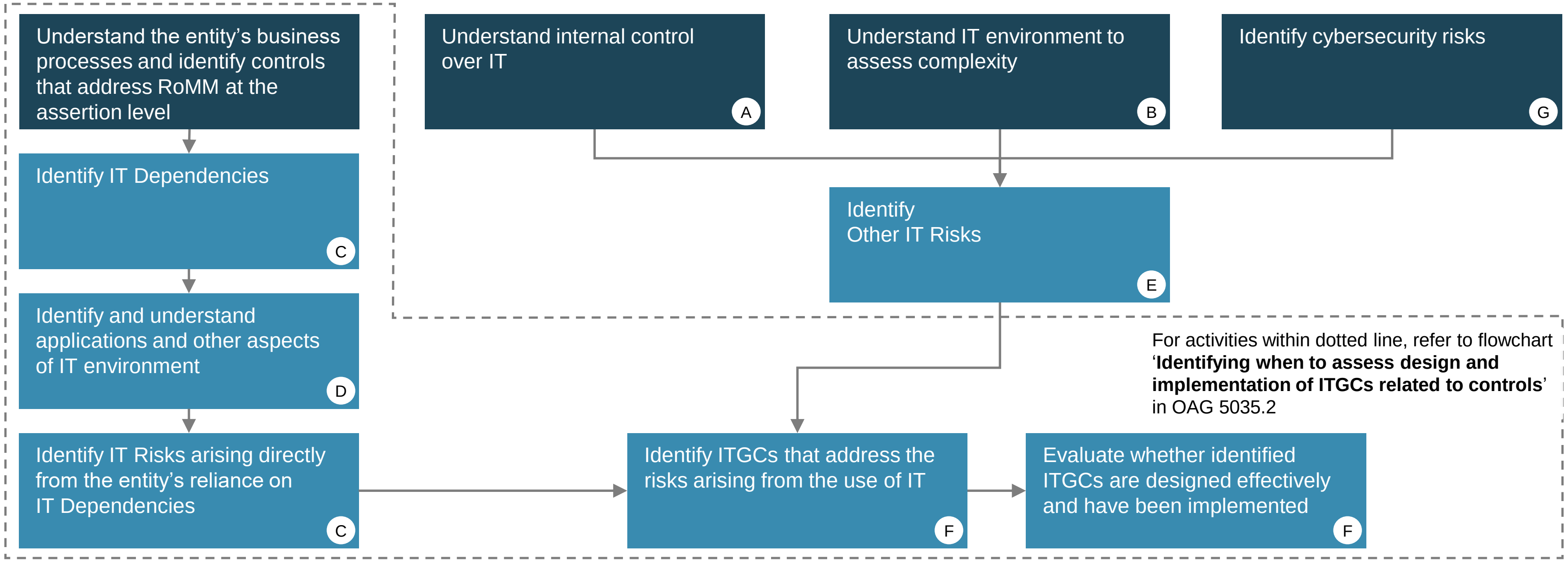
This Quick Reference Guide, which includes references to the relevant sections of OAG Audit, is not a substitute for reviewing the detailed requirements and guidance included in OAG Audit. For detailed guidance refer to OAG Audit 5034 and 5035**,** or contact IT Audit and/or Controls Assurance to assist you with any questions.

Key Reminders

- A granular understanding of the entity’s IT environment is needed to determine the level of complexity and therefore the extent of specialized skills needed for the engagement. This might result in increased involvement of IT Audit specialists in the audit. Consider this when planning resource needs for your engagements.
- The OAG Audit 3102 on IT Audit involvement has been updated to align to the levels of IT environment complexity introduced by the revised risk assessment standard (non-complex, moderately complex and complex).
- Identifying the risks arising from the use of IT and related ITGCs that address such risks starts with obtaining a robust understanding of the business processes and identification of **controls in the control activities component** of entity’s system of internal control.
- Identifying IT risks and related ITGCs is required regardless of whether you plan to test an entity’s controls or instead plan to adopt a fully substantive approach, as these risks are expected to be relevant to any entity using IT.
- Evaluation of design and implementation is required for all ITGCs identified to address the risks arising from the use of IT.
    - If designed and implemented appropriately, consideration is given to whether testing of the operating effectiveness of these ITGCs is an effective and efficient strategy;
    - If not designed or implemented effectively, we consider the impact of the deficiency and IT risk on the nature, timing and extent of substantive or controls testing responsive to the assessed risks of material misstatement at the financial statement and assertion levels
- The new risk assessment procedures are available to support the effective and efficient documentation of our understanding of the IT environment, identified IT risks (including automation to identify commonly applicable IT risks) and ITGCs.

Identifying risks arising from the entity's use of IT and the entity's ITGCs that address such risks

(click on individual tile for details)



Understand the entity's business processes and identify controls that address RoMM at the assertion level

Identify IT Dependencies C

Identify and understand applications and other aspects of IT environment D

Identify IT Risks arising directly from the entity's reliance on IT Dependencies C

Understand internal control over IT A

Understand IT environment to assess complexity B

Identify cybersecurity risks G

Identify Other IT Risks E

Identify ITGCs that address the risks arising from the use of IT F

Evaluate whether identified ITGCs are designed effectively and have been implemented F

For activities within dotted line, refer to flowchart '**Identifying when to assess design and implementation of ITGCs related to controls**' in OAG 5035.2

P_01710 - Understand and assess complexity of the entity's IT environment

- Ⓐ **Tab - Internal control over IT**
- Ⓑ **Tab - Complexity of IT environment**

P_01715 - Identify IT risks and understand and evaluate related ITGCs

- Ⓒ **Tab - IT Dependencies**
- Ⓓ **Tab – Application Complexity**
- Ⓓ **Tab – Application Inventory**
- Ⓔ **Tab - Other IT Risks**
- Ⓕ **Tab - Risks & ITGCs**

P_01696 - Understand and identify cybersecurity risks related to the audit

- Ⓖ

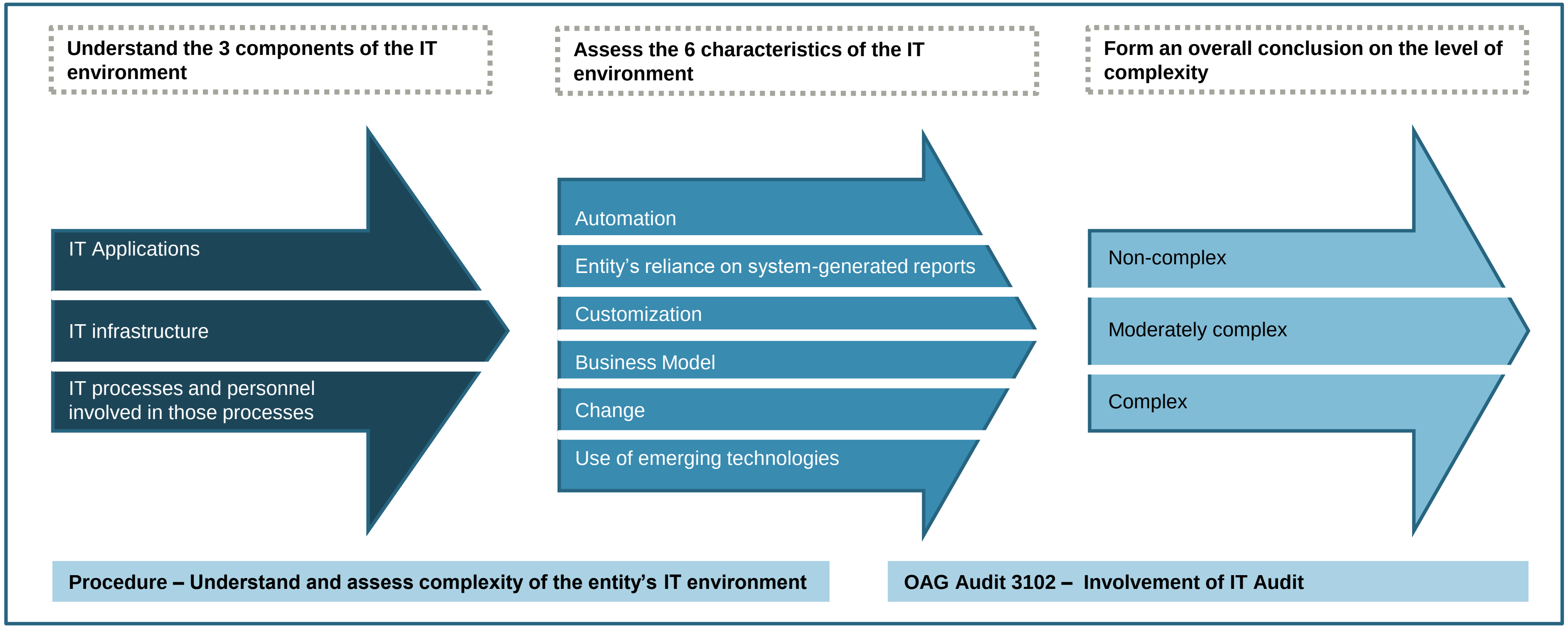
Understanding the IT environment and assessing complexity

Understand the entity's business processes and identify controls that address RoMM at the assertion level

Understand internal control over IT A

Understand IT environment to assess complexity B

Identify cybersecurity risks G



Understand the 3 components of the IT environment

Assess the 6 characteristics of the IT environment

Form an overall conclusion on the level of complexity

IT Applications
IT infrastructure
IT processes and personnel involved in those processes
Automation
Entity's reliance on system-generated reports
Customization
Business Model
Change
Use of emerging technologies
Non-complex
Moderately complex
Complex

Procedure – Understand and assess complexity of the entity's IT environment

OAG Audit 3102 – Involvement of IT Audit

IT risks arising directly from the entity’s reliance on IT dependencies

Understand the entity’s business processes and identify controls that address RoMM at the assertion level

↓

Identify IT Dependencies C

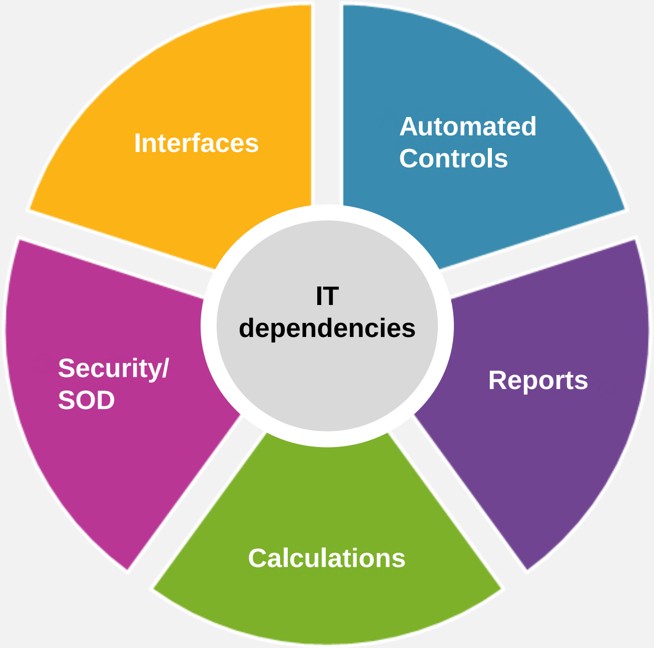
↓

Identify and understand applications and other aspects of IT environment D

↓

Identify IT Risks arising directly from the entity’s reliance on IT Dependencies C

Click hotspots to see more information.



Procedure – Identify IT risks and understand and evaluate related ITGCs

IT Risks Practice Aid

Office of the Auditor General of Canada

Bureau du vérificateur général du Canada

IT risks arising directly from the entity’s reliance on IT dependencies

Understand the entity’s business processes and identify controls that address RoMM at the assertion level

↓

Identify IT Dependencies C

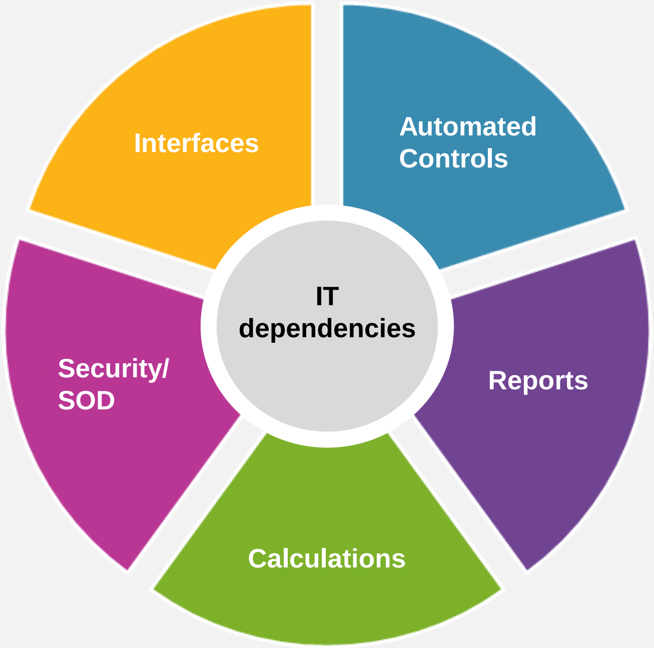
↓

Identify and understand applications and other aspects of IT environment D

↓

Identify IT Risks arising directly from the entity’s reliance on IT Dependencies C

Click hotspots to see more information.



Automated Controls

Automated controls are designed into the IT environment to enforce business rules. For example, many IT applications include format checks (e.g., only a particular date format is accepted), existence checks (e.g., customer number exists on customer masterfile), and/or reasonableness checks (e.g., maximum payment amount) when a transaction is entered.

Procedure – Identify IT risks and understand and evaluate related ITGCs

IT Risks Practice Aid

IT risks arising directly from the entity’s reliance on IT dependencies

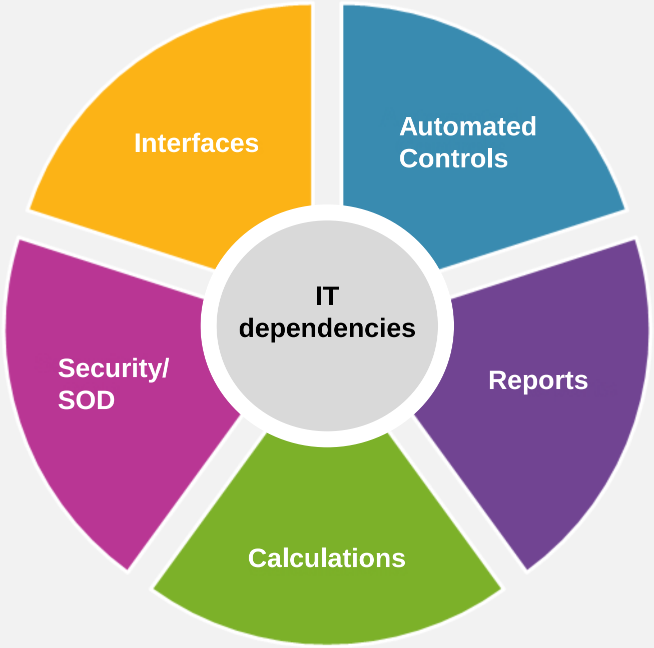
Understand the entity’s business processes and identify controls that address RoMM at the assertion level

Identify IT Dependencies C

Identify and understand applications and other aspects of IT environment D

Identify IT Risks arising directly from the entity’s reliance on IT Dependencies C

Click hotspots to see more information.



Reports

System generated reports are information generated by IT systems (e.g., aged accounts receivable listing used to calculate the allowance for expected credit losses). These reports are often used in an entity’s execution of a manual control, including business performance reviews, or may be the source of entity information used by us when selecting items to perform substantive tests of details or performing a substantive analytical procedure.

Procedure – Identify IT risks and understand and evaluate related ITGCs

IT Risks Practice Aid

IT risks arising directly from the entity’s reliance on IT dependencies

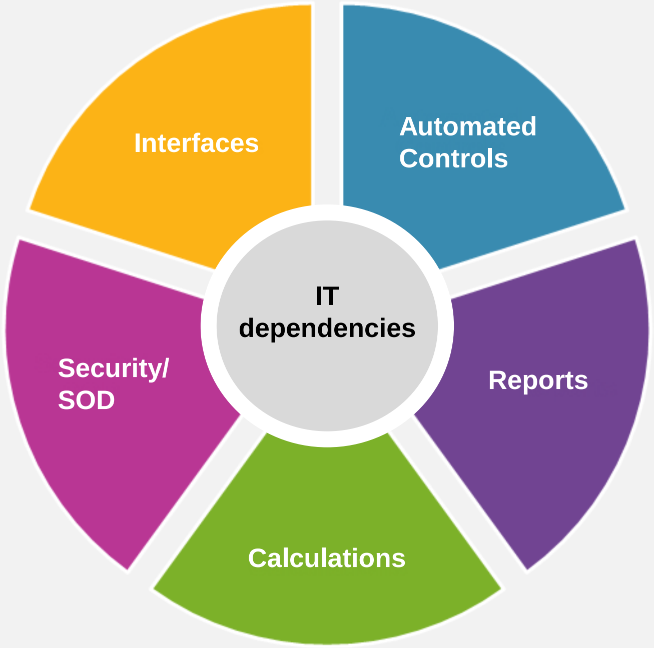
Understand the entity’s business processes and identify controls that address RoMM at the assertion level

Identify IT Dependencies C

Identify and understand applications and other aspects of IT environment D

Identify IT Risks arising directly from the entity’s reliance on IT Dependencies C

Click hotspots to see more information.



Calculations

Calculations are accounting procedures that are performed by an IT system instead of a person. For example, the system will apply the ‘straight-line’ depreciation formula to calculate depreciation of an asset (i.e., cost of the asset, less the residual value of the asset at the end of its useful life divided by the useful life of the asset) or the system will calculate the value of the amount invoiced to a customer by multiplying the item price times the quantity shipped.

Procedure – Identify IT risks and understand and evaluate related ITGCs

IT Risks Practice Aid

IT risks arising directly from the entity's reliance on IT dependencies

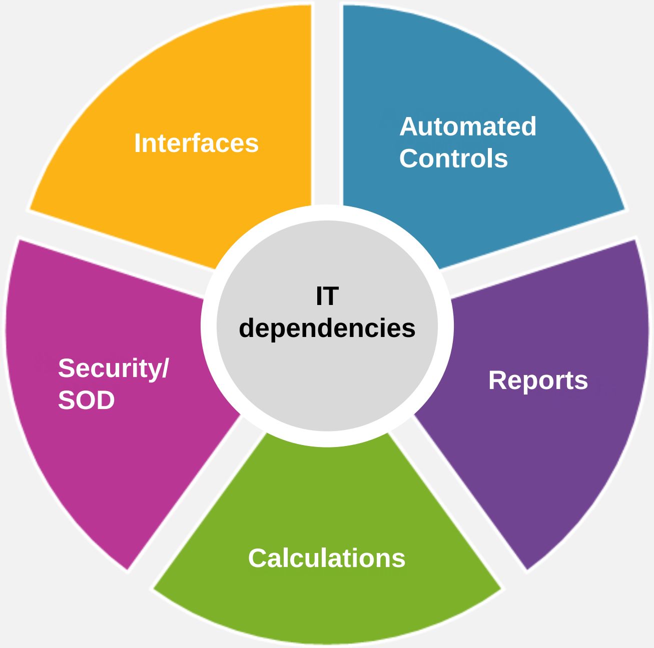
Understand the entity's business processes and identify controls that address RoMM at the assertion level

Identify IT Dependencies C

Identify and understand applications and other aspects of IT environment D

Identify IT Risks arising directly from the entity's reliance on IT Dependencies C

Click hotspots to see more information.



Security/SoD

Security, including segregation of duties, is enabled by the IT environment to restrict access to information and to determine the separation of roles and responsibilities that could allow an employee to perpetrate and conceal errors or fraud, or to process errors that go undetected (e.g., segregation of roles for preparation and approval of payments to vendors).

Procedure – Identify IT risks and understand and evaluate related ITGCs

IT Risks Practice Aid

IT risks arising directly from the entity’s reliance on IT dependencies

Understand the entity’s business processes and identify controls that address RoMM at the assertion level

↓

Identify IT Dependencies C

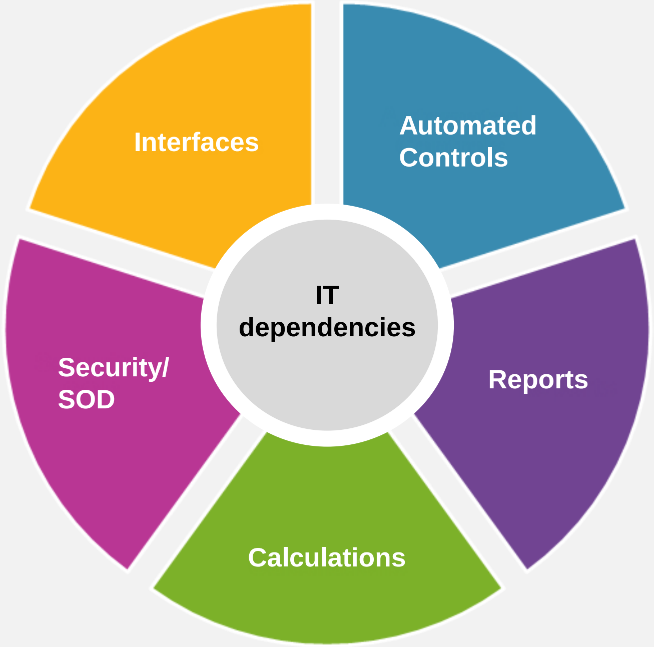
↓

Identify and understand applications and other aspects of IT environment D

↓

Identify IT Risks arising directly from the entity’s reliance on IT Dependencies C

Click hotspots to see more information.



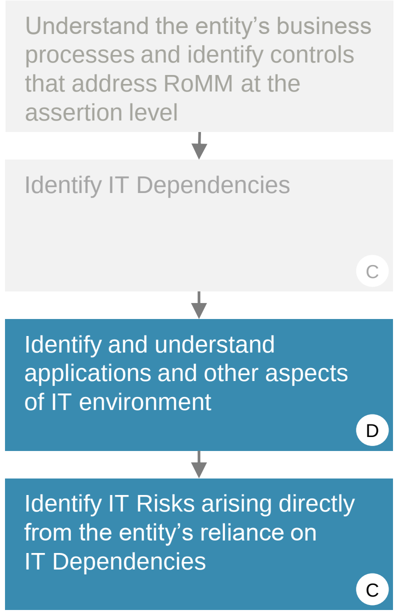
Interfaces

Interfaces are programmed logic that transfer data from one IT system to another. For example, an interface may be programmed to transfer data from a payroll sub-ledger in one IT system to the general ledger in another IT system.

Procedure – Identify IT risks and understand and evaluate related ITGCs

IT Risks Practice Aid

IT risks arising directly from the entity’s reliance on IT dependencies



Understand the entity’s business processes and identify controls that address RoMM at the assertion level

Identify IT Dependencies

C

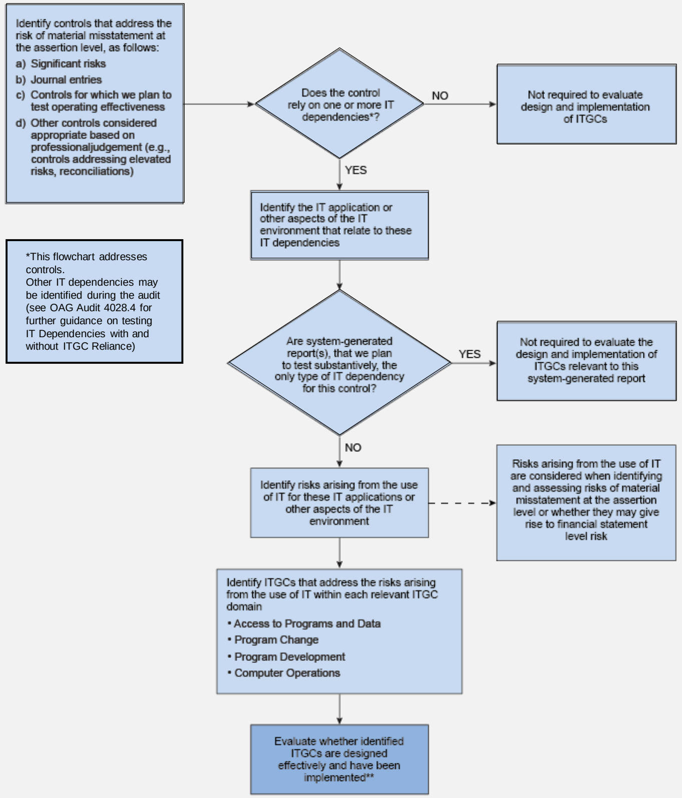
Identify and understand applications and other aspects of IT environment

D

Identify IT Risks arising directly from the entity’s reliance on IT Dependencies

C

Identifying when to assess design and implementation of ITGCs related to controls.



Identify controls that address the risk of material misstatement at the assertion level, as follows:

a) Significant risks

b) Journal entries

c) Controls for which we plan to test operating effectiveness

d) Other controls considered appropriate based on professionaljudgement (e.g., controls addressing elevated risks, reconciliations)

Does the control rely on one or more IT dependencies*?

NO

Not required to evaluate design and implementation of ITGCs

YES

Identify the IT application or other aspects of the IT environment that relate to these IT dependencies

*This flowchart addresses controls.
Other IT dependencies may be identified during the audit (see OAG Audit 4028.4 for further guidance on testing IT Dependencies with and without ITGC Reliance)

Are system-generated report(s), that we plan to test substantively, the only type of IT dependency for this control?

YES

Not required to evaluate the design and implementation of ITGCs relevant to this system-generated report

NO

Identify risks arising from the use of IT for these IT applications or other aspects of the IT environment

Risks arising from the use of IT are considered when identifying and assessing risks of material misstatement at the assertion level or whether they may give rise to financial statement level risk

Identify ITGCs that address the risks arising from the use of IT within each relevant ITGC domain

- Access to Programs and Data
- Program Change
- Program Development
- Computer Operations

Evaluate whether identified ITGCs are designed effectively and have been implemented**

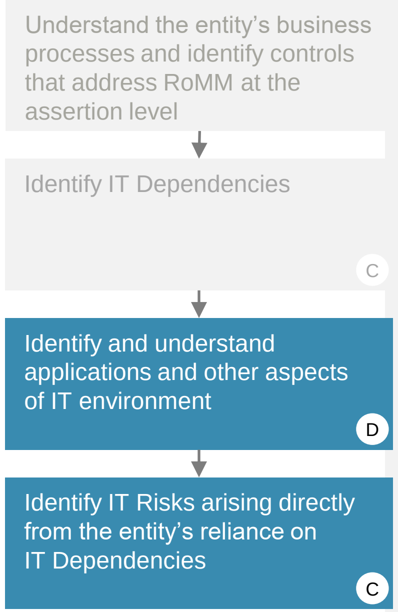
Click hotspots to see more information.

Procedure – Identify IT risks and understand and evaluate related ITGCs

IT Risks Practice Aid

IT risks arising directly from the entity’s reliance on IT dependencies

Back


Understand the entity’s business processes and identify controls that address RoMM at the assertion level

Identify IT Dependencies

C

Identify and understand applications and other aspects of IT environment

D

Identify IT Risks arising directly from the entity’s reliance on IT Dependencies

C

Identifying when to assess design and implementation of ITGCs related to controls.

Identify controls that address the risks of material misstatement at the assertion level, as follows:

a. Significant risks
b. Journal entries
c. Controls for which we plan to test operating effectiveness
d. Other controls considered appropriate based on professional judgement (e.g. controls addressing elevated risks, reconciliations)

The first step is to identify controls within the control activities component of the entity’s system of internal controls and determine whether they rely on IT dependencies.

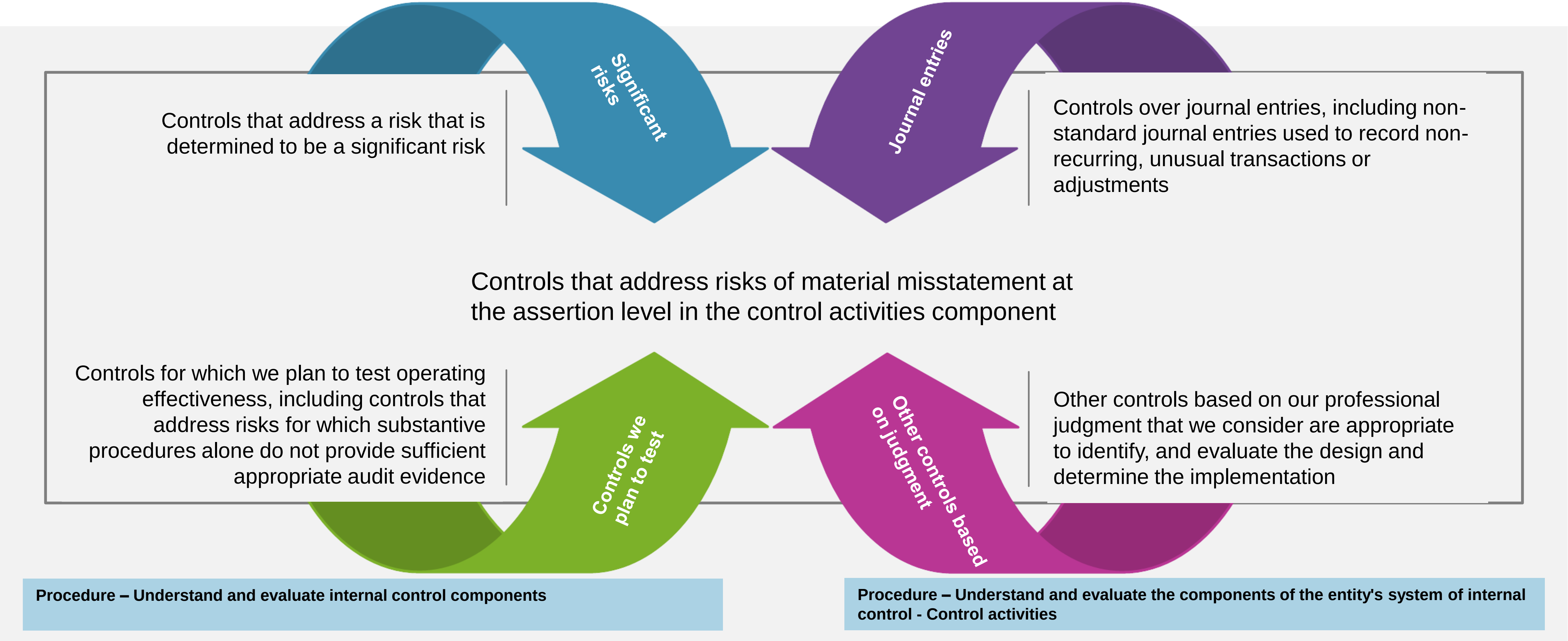
See OAG Audit 5035.1 for additional guidance on the types of controls that fall within this component.

See OAG Audit 5034 for guidance regarding IT dependencies.

Procedure – Identify IT risks and understand and evaluate related ITGCs

IT Risks Practice Aid

What is a control in the control activities component?



Controls that address a risk that is determined to be a significant risk

Controls over journal entries, including non-standard journal entries used to record non-recurring, unusual transactions or adjustments

Controls that address risks of material misstatement at the assertion level in the control activities component

Controls for which we plan to test operating effectiveness, including controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence

Other controls based on our professional judgment that we consider are appropriate to identify, and evaluate the design and determine the implementation

Procedure – Understand and evaluate internal control components

Procedure – Understand and evaluate the components of the entity's system of internal control - Control activities

IT risks arising directly from the entity's reliance on IT dependencies

Back

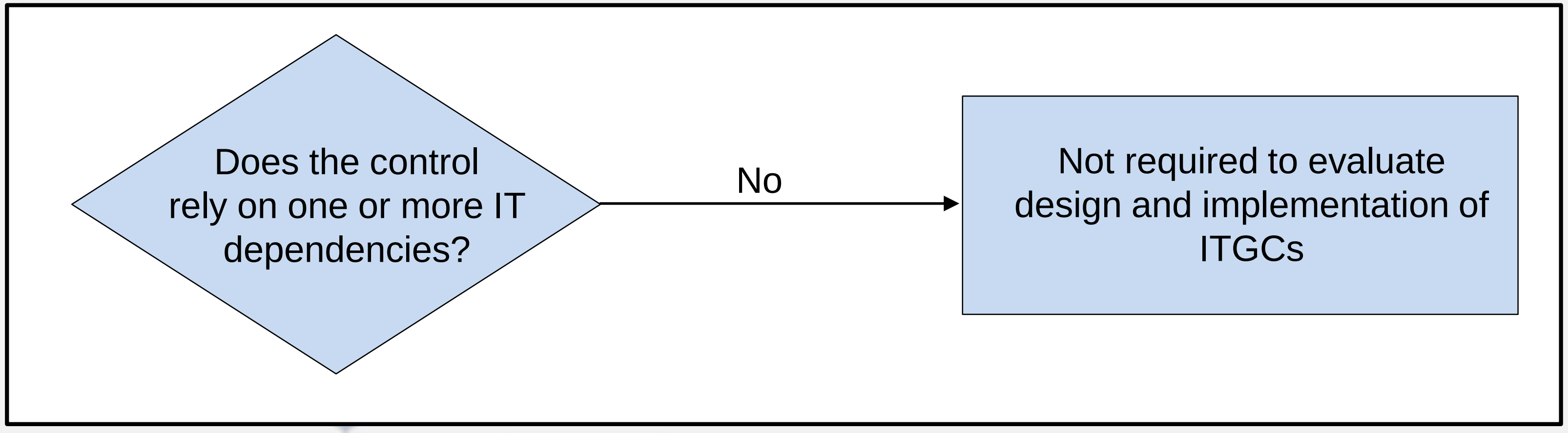
Understand the entity's business processes and identify controls that address RoMM at the assertion level

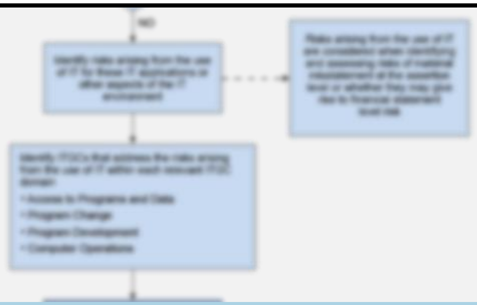
Identify IT Dependencies C

Identify and understand applications and other aspects of IT environment D

Identify IT Risks arising directly from the entity's reliance on IT Dependencies C

Identifying when to assess design and implementation of ITGCs related to controls.


Does the control rely on one or more IT dependencies?
No
Not required to evaluate design and implementation of ITGCs



When we identify a manual control in the control activities component and that control does not rely on any IT dependencies, there is no use of IT and therefore there is no IT risk to be identified. Accordingly, there is no ITGC for which to evaluate design or implementation.

Procedure – Identify IT risks and understand and evaluate related ITGCs

IT Risks Practice Aid

IT risks arising directly from the entity’s reliance on IT dependencies

Back

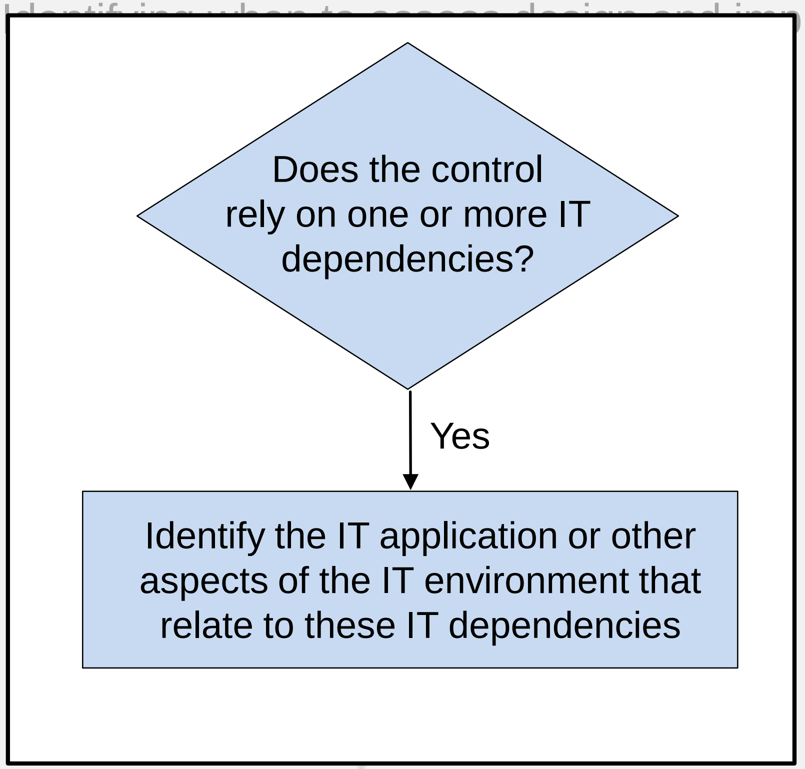
Understand the entity’s business processes and identify controls that address RoMM at the assertion level

Identify IT Dependencies C

Identify and understand applications and other aspects of IT environment D

Identify IT Risks arising directly from the entity’s reliance on IT Dependencies C

Identifying when to assess design and implementation of ITGCs related to controls.


Does the control rely on one or more IT dependencies?
Yes
Identify the IT application or other aspects of the IT environment that relate to these IT dependencies

When we identify a control in the control activities component and that control does rely on one or more IT dependencies (i.e., an automated or IT dependent manual control), for each IT dependency, we identify the related IT application and other aspects of the IT environment (including application type, database, data center, operating system, server name) and consider if they are subject to risks arising from the use of IT.

Procedure – Identify IT risks and understand and evaluate related ITGCs

IT Risks Practice Aid

IT risks arising directly from the entity’s reliance on IT dependencies

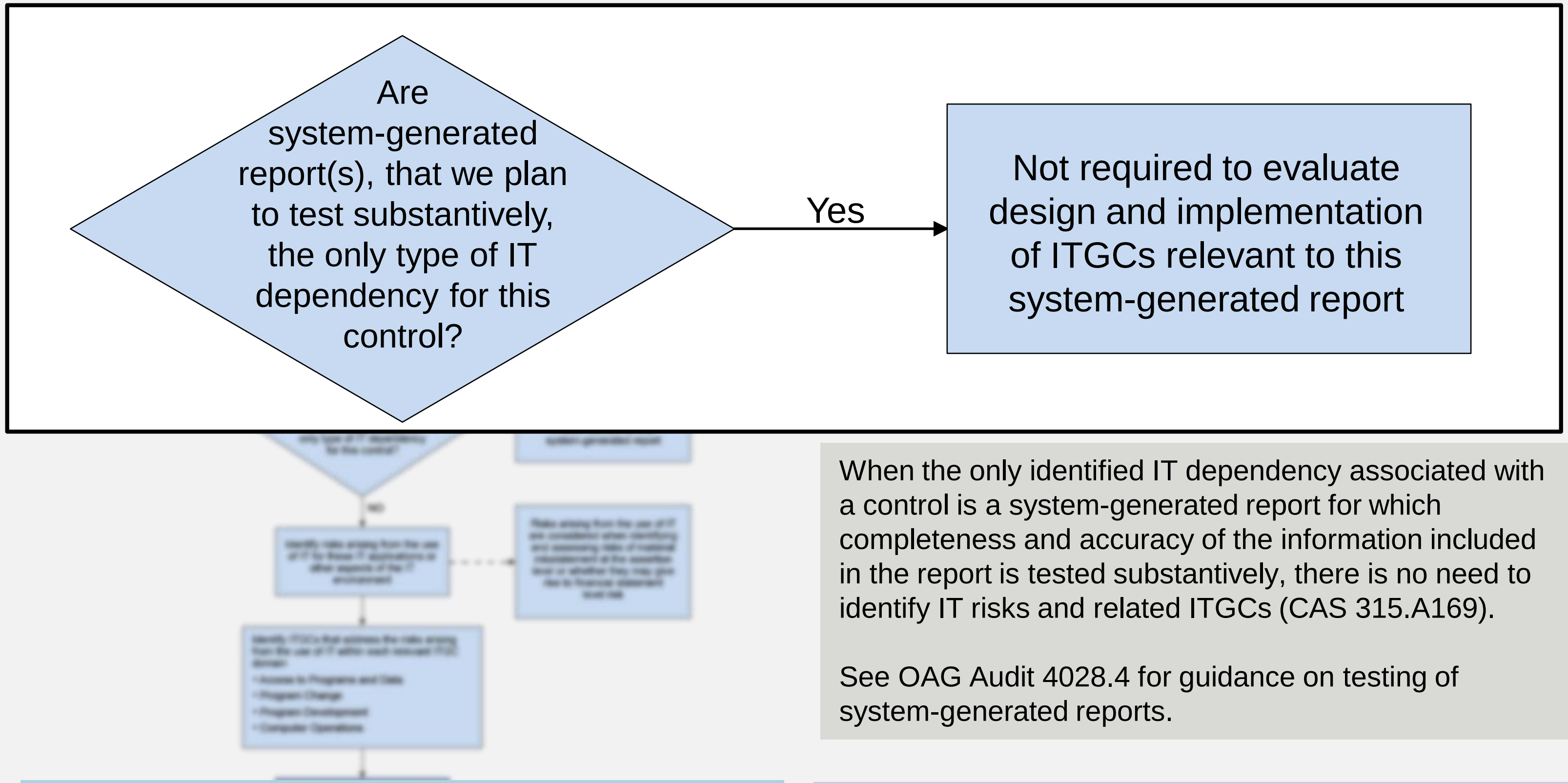
Back

Understand the entity’s business processes and identify controls that address RoMM at the assertion level

Identify IT Dependencies C

Identify and understand applications and other aspects of IT environment D

Identify IT Risks arising directly from the entity’s reliance on IT Dependencies C


Are system-generated report(s), that we plan to test substantively, the only type of IT dependency for this control?
Yes
Not required to evaluate design and implementation of ITGCs relevant to this system-generated report

When the only identified IT dependency associated with a control is a system-generated report for which completeness and accuracy of the information included in the report is tested substantively, there is no need to identify IT risks and related ITGCs (CAS 315.A169).

See OAG Audit 4028.4 for guidance on testing of system-generated reports.

Procedure – Identify IT risks and understand and evaluate related ITGCs

IT Risks Practice Aid

IT risks arising directly from the entity’s reliance on IT dependencies

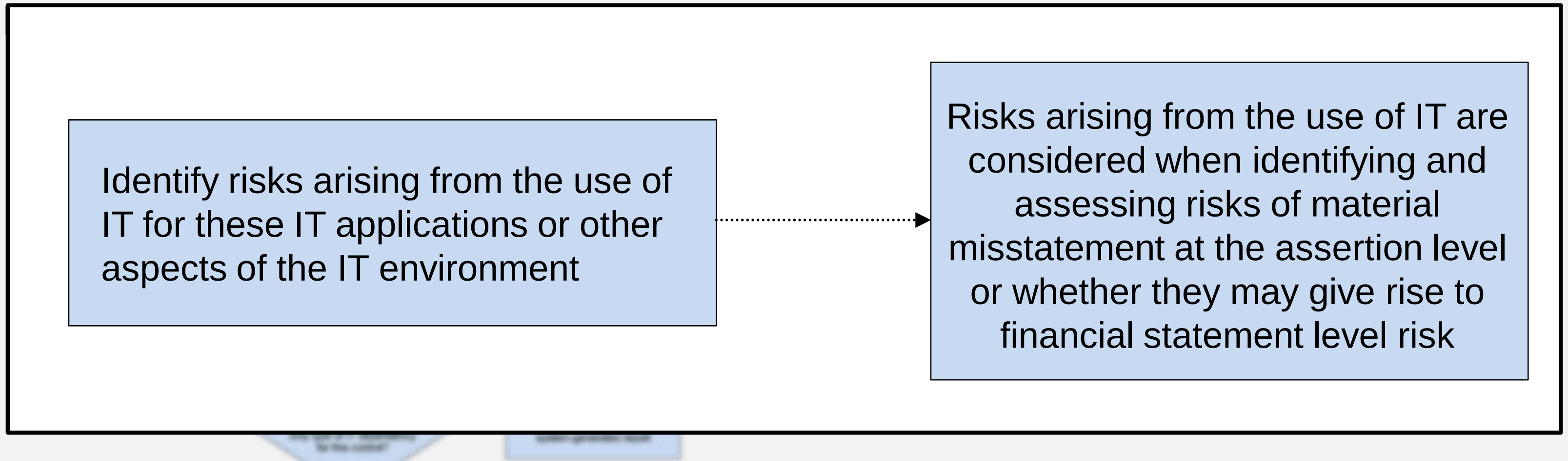
Back

Understand the entity’s business processes and identify controls that address RoMM at the assertion level

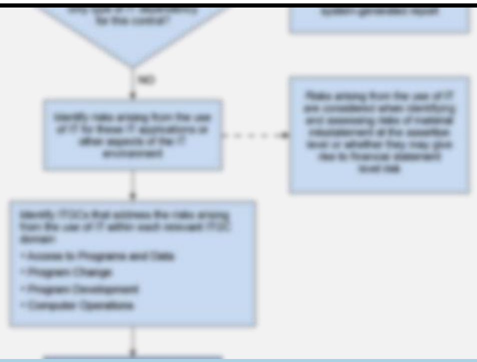
Identify IT Dependencies C

Identify and understand applications and other aspects of IT environment D

Identify IT Risks arising directly from the entity’s reliance on IT Dependencies C


Identify risks arising from the use of IT for these IT applications or other aspects of the IT environment

Risks arising from the use of IT are considered when identifying and assessing risks of material misstatement at the assertion level or whether they may give rise to financial statement level risk



For system-generated reports for which the inputs and outputs will not be substantively tested or any other type of IT dependency, identify the relevant risks arising from the use of IT.

Procedure – Identify IT risks and understand and evaluate related ITGCs

IT Risks Practice Aid

IT risks arising directly from the entity’s reliance on IT dependencies

Back

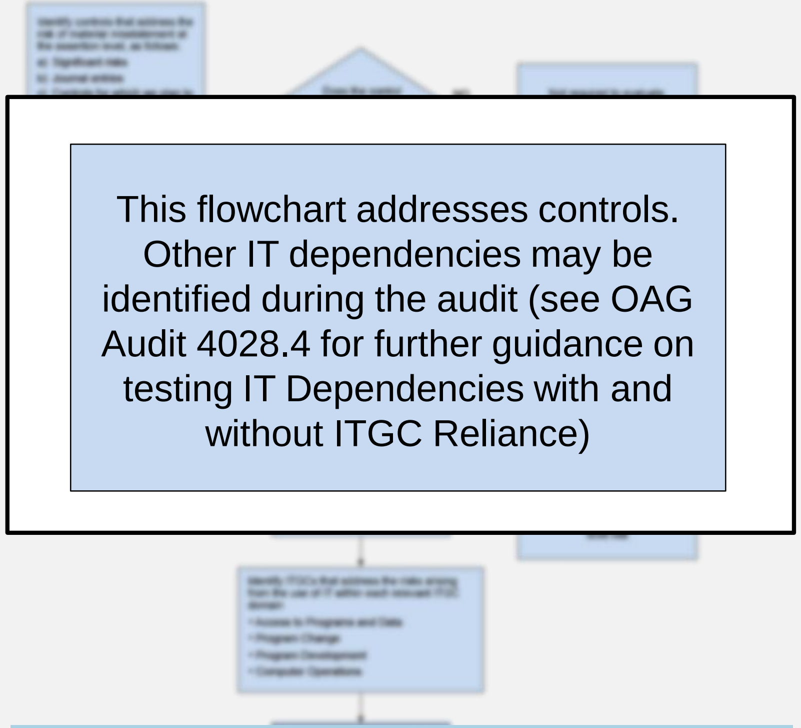
Understand the entity’s business processes and identify controls that address RoMM at the assertion level

Identify IT Dependencies C

Identify and understand applications and other aspects of IT environment D

Identify IT Risks arising directly from the entity’s reliance on IT Dependencies C

Identifying when to assess design and implementation of ITGCs related to controls.



This flowchart addresses controls. Other IT dependencies may be identified during the audit (see OAG Audit 4028.4 for further guidance on testing IT Dependencies with and without ITGC Reliance)

If the IT dependency has been identified as being relevant to the audit because it will be used as a basis for substantive audit procedures (e.g., system-generated report used when testing the net realizable value of inventory and not used in a control in the control activities component), apply the same process presented in the flowchart as if the IT dependency was a control in the control activities component.

Procedure – Identify IT risks and understand and evaluate related ITGCs

IT Risks Practice Aid

Other IT Risks

Obtaining an understanding of the entity's processes related to cybersecurity in the areas below help to understand and identify cybersecurity risks.

1 **Risk Assessment** – Understand how the entity's risks assessment process considers cybersecurity.

2 **Roles and Responsibilities** – Understand the entity's established roles and responsibilities over cybersecurity, such as Chief Information Officer (CISO), CIO, or Cybersecurity Risk Officer.

3 **Safeguarding of Assets** - Understand the entity's process for safeguarding material digital/electronic assets that are included on its balance sheet and subject to cybersecurity risk (e.g., intellectual property, patents, copyrighted material, trade secrets) and management's process for identifying these assets and prioritising their protection.

4 **Security Breaches** - Understand the entity's controls and procedures to monitor and detect security breaches or incidents.

5 **Disclosure or Risks and Incidents** - Understand the entity's processes for disclosing cybersecurity risks and incidents (in accordance with reporting requirements).

6 **Common Cybersecurity Exposures** - Understand whether common cybersecurity exposures may represent a risk of material misstatement to the financial statements and how the entity addresses the risk.

Procedure – Understand and identify cybersecurity risks related to the audit

IT Risks Practice Aid

Identify cybersecurity risks

G

ɔr activities within dotted line, refer to ɔwchart '**Identifying when to assess esign and implementation of ITGCs lated to controls**' in OAG Audit 5035.2

identified
ed effectively
plemented

F

5 - Understand and identify cybersecurity lated to the audit

Office of the Auditor General of Canada

Bureau du vérificateur général du Canada

Other IT Risks

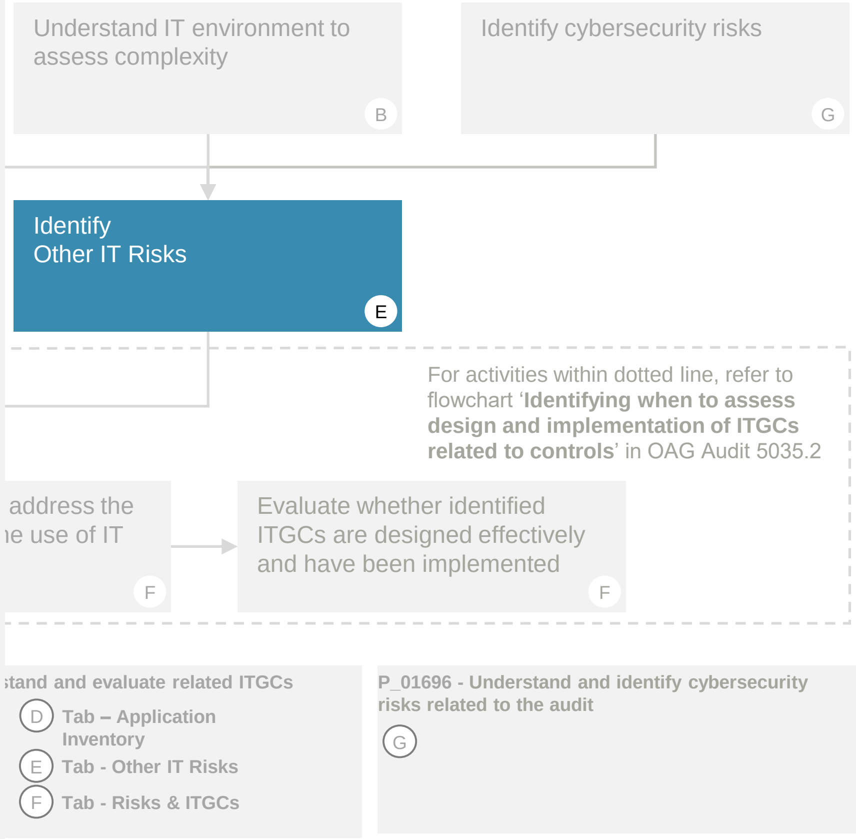
Other IT risks including cybersecurity risks:

Entity level IT risks
IT risks that arise at an entity level and may not be specific to an application or other aspects of the IT environment such as insufficient segregation of incompatible duties/access rights.

Application-specific IT risks
Application-specific IT risks that are not directly associated with a specific IT dependency such as program development or data migration. These risks are identified based on your understanding of the entity and its IT environment (e.g., awareness of a new system implementation may lead you to identify a data migration risk related to moving data from the old application to the new one)

Procedure – Identify IT risks and understand and evaluate related ITGCs

IT Risks Practice Aid



Understand IT environment to assess complexity B

Identify cybersecurity risks G

Identify Other IT Risks E

For activities within dotted line, refer to flowchart '**Identifying when to assess design and implementation of ITGCs related to controls**' in OAG Audit 5035.2

address the ne use of IT F

Evaluate whether identified ITGCs are designed effectively and have been implemented F

stand and evaluate related ITGCs
D Tab – Application Inventory
E Tab - Other IT Risks
F Tab - Risks & ITGCs

P_01696 - Understand and identify cybersecurity risks related to the audit
G

ITGCs that address the risks arising from the use of IT

In identifying ITGCs that address IT risks we consider the following 4 domains:

Access to programs and data

The domain objective is to ensure that only authorized access is granted to the IT applications and other aspects of the IT environment upon authentication of a user's identity. Controls over access include the processes used by the entity to add, delete, and change users and their related access rights according to the control objectives established in the design of the control.

Program Change

The domain objective is to ensure that changes to the IT application and other aspects of the IT environment are requested, authorized, performed, tested, and implemented to achieve management's IT control objectives.

Program development

The domain objective is to ensure that IT applications and other aspects of the IT environment are developed, configured, and implemented to achieve management's control objectives.
This includes development or acquisition or implementation controls and data conversion controls.

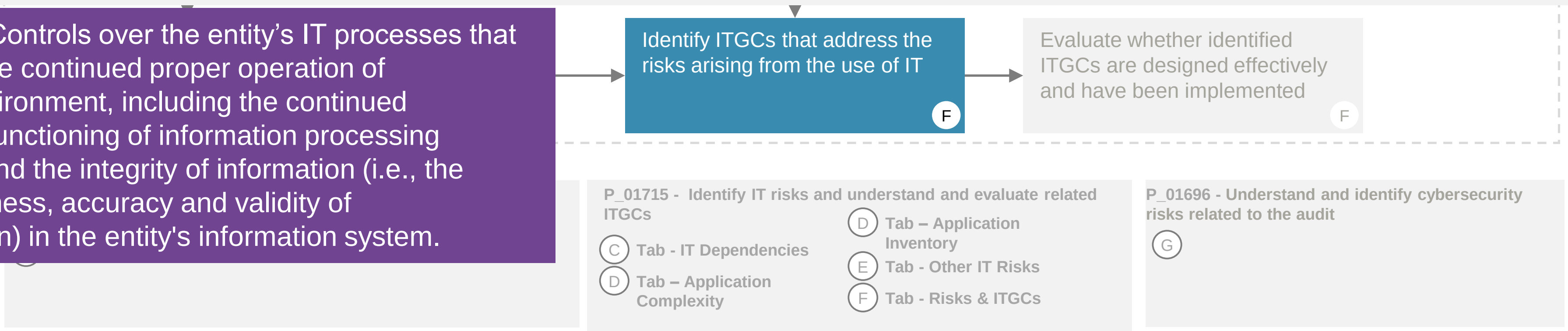
Computer operations

The domain objective is to ensure that information in the IT applications and other aspects of the IT environment is processed completely and accurately in accordance with management's control objectives, and that processing problems are identified and resolved completely and accurately to maintain the integrity of financial data.

Procedure – Identify IT risks and understand and evaluate related ITGCs

IT Risks Practice Aid

ITGCs – Controls over the entity's IT processes that support the continued proper operation of the IT environment, including the continued effective functioning of information processing controls and the integrity of information (i.e., the completeness, accuracy and validity of information) in the entity's information system.



Identify ITGCs that address the risks arising from the use of IT F

Evaluate whether identified ITGCs are designed effectively and have been implemented F

P_01715 - Identify IT risks and understand and evaluate related ITGCs

C Tab - IT Dependencies

D Tab – Application Complexity

D Tab – Application Inventory

E Tab - Other IT Risks

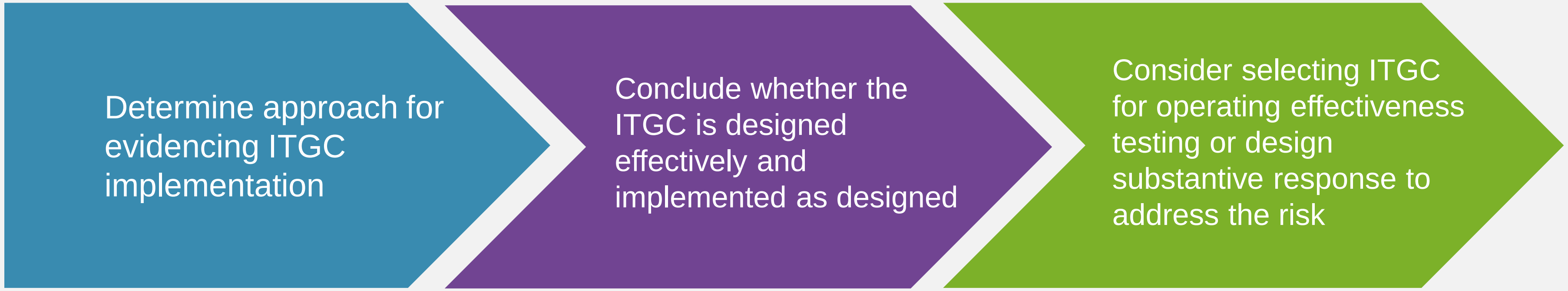
F Tab - Risks & ITGCs

P_01696 - Understand and identify cybersecurity risks related to the audit

G

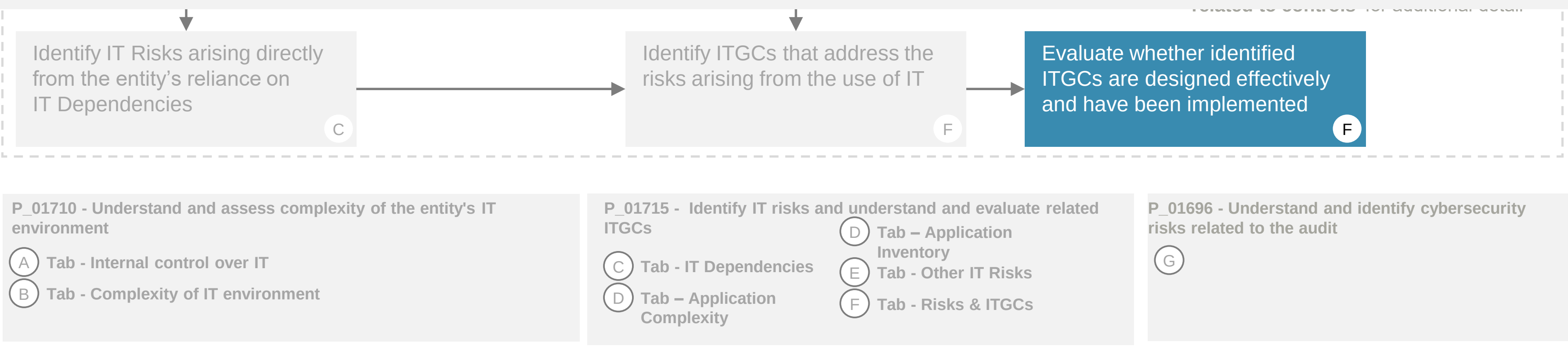
Other IT Risks

Evaluate whether identified ITGCs are designed effectively and have been implemented:


Determine approach for evidencing ITGC implementation
Conclude whether the ITGC is designed effectively and implemented as designed
Consider selecting ITGC for operating effectiveness testing or design substantive response to address the risk

Procedure – Identify IT risks and understand and evaluate related ITGCs

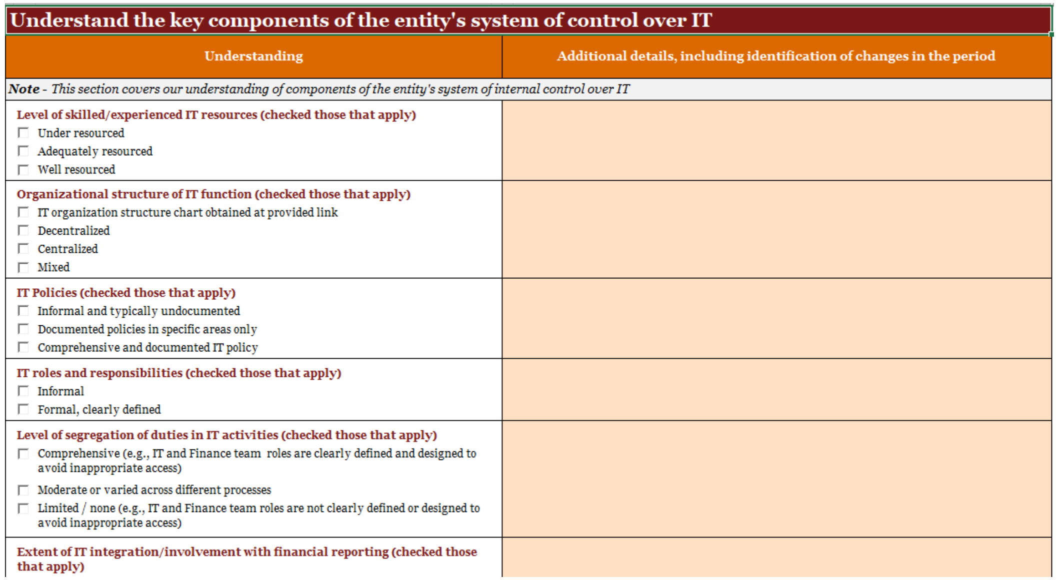
IT Risks Practice Aid


related to controls for additional detail.
Identify IT Risks arising directly from the entity's reliance on IT Dependencies
C
Identify ITGCs that address the risks arising from the use of IT
F
Evaluate whether identified ITGCs are designed effectively and have been implemented
F
P_01710 - Understand and assess complexity of the entity's IT environment
A Tab - Internal control over IT
B Tab - Complexity of IT environment
P_01715 - Identify IT risks and understand and evaluate related ITGCs
C Tab - IT Dependencies
D Tab – Application Complexity
D Tab – Application Inventory
E Tab - Other IT Risks
F Tab - Risks & ITGCs
P_01696 - Understand and identify cybersecurity risks related to the audit
G

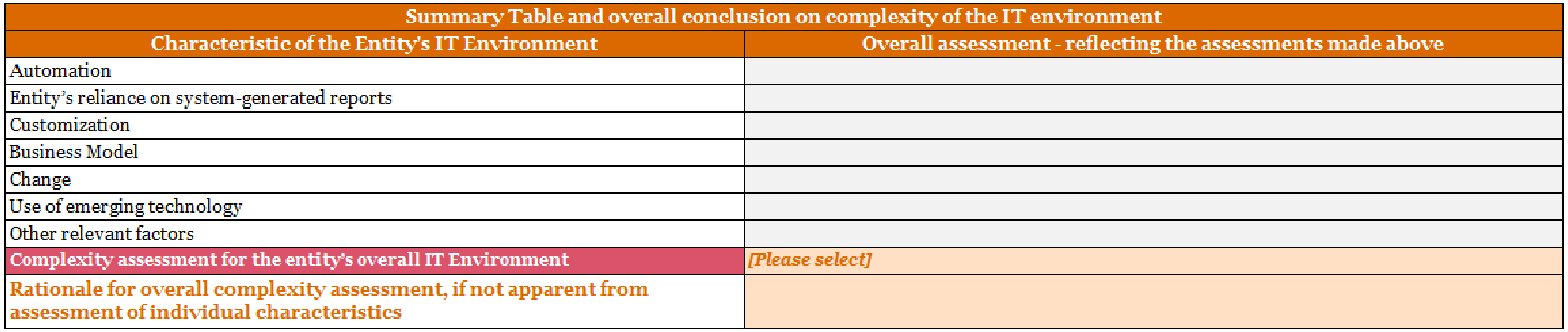
Procedure - Understand and assess complexity of the entity's IT environment

The procedure covers documentation in the following areas:

- Understanding of the key components of the entity's system of internal control over IT
- Understanding of the characteristics of the entity's IT environment
- Assessment of the complexity of the IT environment based on the understanding obtained



Understand the key components of the entity's system of control over IT	
Understanding	**Additional details, including identification of changes in the period**
Note *- This section covers our understanding of components of the entity's system of internal control over IT*	
Level of skilled/experienced IT resources (checked those that apply) □ Under resourced □ Adequately resourced □ Well resourced	
Organizational structure of IT function (checked those that apply) □ IT organization structure chart obtained at provided link □ Decentralized □ Centralized □ Mixed	
IT Policies (checked those that apply) □ Informal and typically undocumented □ Documented policies in specific areas only □ Comprehensive and documented IT policy	
IT roles and responsibilities (checked those that apply) □ Informal □ Formal, clearly defined	
Level of segregation of duties in IT activities (checked those that apply) □ Comprehensive (e.g., IT and Finance team roles are clearly defined and designed to avoid inappropriate access) □ Moderate or varied across different processes □ Limited / none (e.g., IT and Finance team roles are not clearly defined or designed to avoid inappropriate access)	
Extent of IT integration/involvement with financial reporting (checked those that apply)	



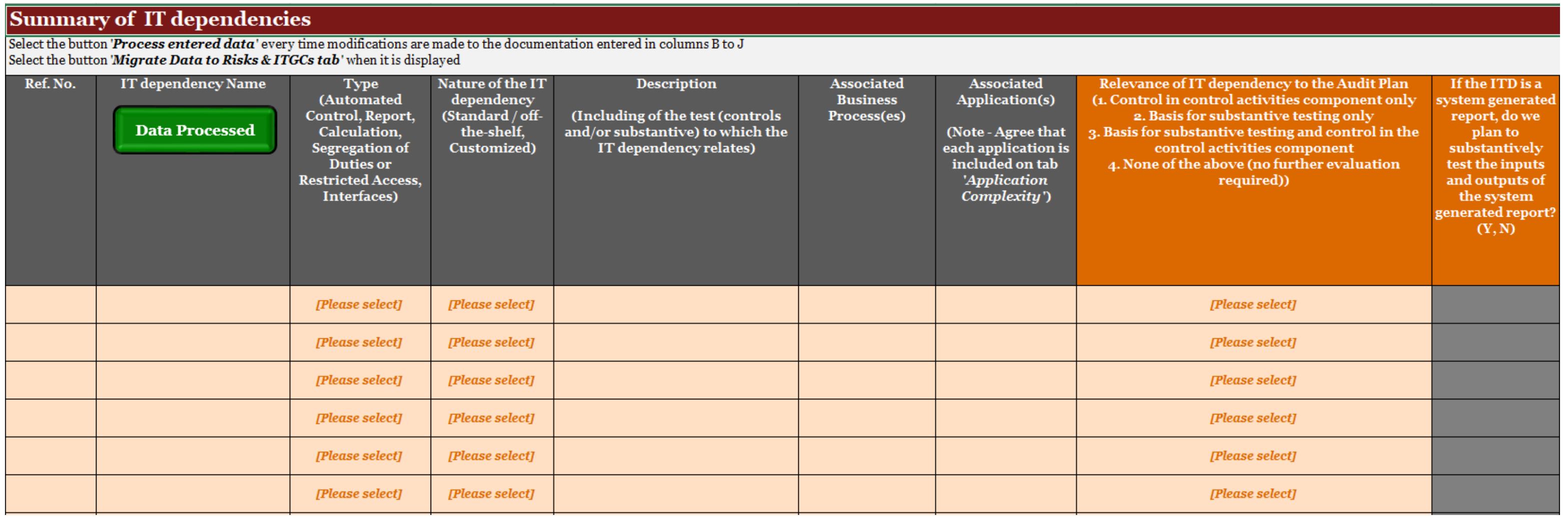
Summary Table and overall conclusion on complexity of the IT environment	
Characteristic of the Entity's IT Environment	**Overall assessment - reflecting the assessments made above**
Automation	
Entity's reliance on system-generated reports	
Customization	
Business Model	
Change	
Use of emerging technology	
Other relevant factors	
Complexity assessment for the entity's overall IT Environment	***[Please select]***
Rationale for overall complexity assessment, if not apparent from assessment of individual characteristics	

Procedure - Identify IT risks and understand and evaluate related ITGCs

Go to 2 of 2

The procedure covers documentation in the following areas:

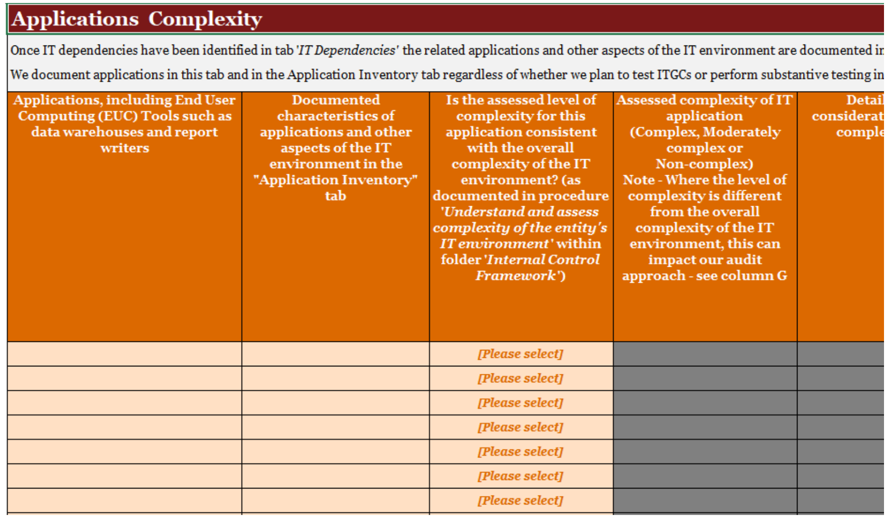
- Summary of IT dependencies identified during the audit, as well as their type, nature and relevance to the audit plan
- Identification of commonly relevant IT risks based on the type of IT dependency using automation embedded in the procedure
- Applications and other aspects of the IT environment that are being relied upon by the IT dependencies
- Assessment of the complexity of the identified applications



Summary of IT dependencies

Select the button '***Process entered data***' every time modifications are made to the documentation entered in columns B to J
Select the button '***Migrate Data to Risks & ITGCs tab***' when it is displayed

Ref. No.	IT dependency Name Data Processed	Type (Automated Control, Report, Calculation, Segregation of Duties or Restricted Access, Interfaces)	Nature of the IT dependency (Standard / off-the-shelf, Customized)	Description (Including of the test (controls and/or substantive) to which the IT dependency relates)	Associated Business Process(es)	Associated Application(s) (Note - Agree that each application is included on tab '*Application Complexity*')	Relevance of IT dependency to the Audit Plan (1. Control in control activities component only 2. Basis for substantive testing only 3. Basis for substantive testing and control in the control activities component 4. None of the above (no further evaluation required))	If the ITD is a system generated report, do we plan to substantively test the inputs and outputs of the system generated report? (Y, N)
		[Please select]	*[Please select]*				*[Please select]*	
		[Please select]	*[Please select]*				*[Please select]*	
		[Please select]	*[Please select]*				*[Please select]*	
		[Please select]	*[Please select]*				*[Please select]*	
		[Please select]	*[Please select]*				*[Please select]*	
		[Please select]	*[Please select]*				*[Please select]*	



Applications Complexity

Once IT dependencies have been identified in tab '*IT Dependencies*' the related applications and other aspects of the IT environment are documented in
We document applications in this tab and in the Application Inventory tab regardless of whether we plan to test ITGCs or perform substantive testing in

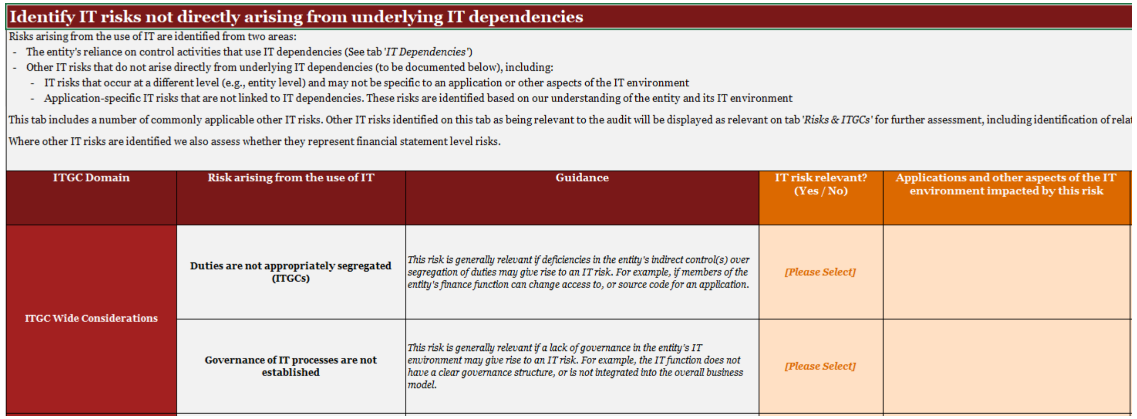
Applications, including End User Computing (EUC) Tools such as data warehouses and report writers	Documented characteristics of applications and other aspects of the IT environment in the "Application Inventory" tab	Is the assessed level of complexity for this application consistent with the overall complexity of the IT environment? (as documented in procedure '*Understand and assess complexity of the entity's IT environment*' within folder '*Internal Control Framework*')	Assessed complexity of IT application (Complex, Moderately complex or Non-complex) Note - Where the level of complexity is different from the overall complexity of the IT environment, this can impact our audit approach - see column G	Detail considerat comple
		[Please select]		
		[Please select]		
		[Please select]		
		[Please select]		
		[Please select]		
		[Please select]		
		[Please select]		

Procedure - Identify IT risks and understand and evaluate related ITGCs

Back to 1 of 2

The procedure covers documentation in the following areas:

- Identification of IT risks not directly arising from the underlying IT dependencies, including cybersecurity risks
- Assessment of the relevance of the IT risks and identification of ITGCs addressing those risk
- Evaluation of the design and implementation of the ITGCs
- Determination of the planned response to the identified IT risks (testing of operating effectiveness of controls or substantive procedures)



Identify IT risks not directly arising from underlying IT dependencies

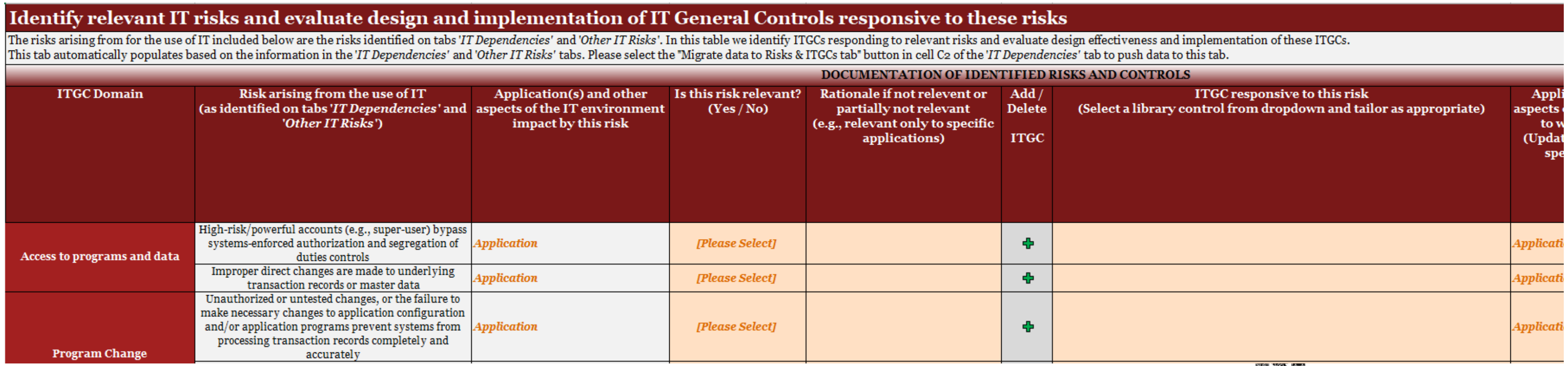
Risks arising from the use of IT are identified from two areas:

- The entity's reliance on control activities that use IT dependencies (See tab *'IT Dependencies'*)
- Other IT risks that do not arise directly from underlying IT dependencies (to be documented below), including:
  - IT risks that occur at a different level (e.g., entity level) and may not be specific to an application or other aspects of the IT environment
  - Application-specific IT risks that are not linked to IT dependencies. These risks are identified based on our understanding of the entity and its IT environment

This tab includes a number of commonly applicable other IT risks. Other IT risks identified on this tab as being relevant to the audit will be displayed as relevant on tab *'Risks & ITGCs'* for further assessment, including identification of relat

Where other IT risks are identified we also assess whether they represent financial statement level risks.

ITGC Domain	Risk arising from the use of IT	Guidance	IT risk relevant? (Yes / No)	Applications and other aspects of the IT environment impacted by this risk
ITGC Wide Considerations	**Duties are not appropriately segregated (ITGCs)**	*This risk is generally relevant if deficiencies in the entity's indirect control(s) over segregation of duties may give rise to an IT risk. For example, if members of the entity's finance function can change access to, or source code for an application.*	*[Please Select]*	
	Governance of IT processes are not established	*This risk is generally relevant if a lack of governance in the entity's IT environment may give rise to an IT risk. For example, the IT function does not have a clear governance structure, or is not integrated into the overall business model.*	*[Please Select]*	



Identify relevant IT risks and evaluate design and implementation of IT General Controls responsive to these risks

The risks arising from for the use of IT included below are the risks identified on tabs *'IT Dependencies'* and *'Other IT Risks'*. In this table we identify ITGCs responding to relevant risks and evaluate design effectiveness and implementation of these ITGCs.
This tab automatically populates based on the information in the *'IT Dependencies'* and *'Other IT Risks'* tabs. Please select the "Migrate data to Risks & ITGCs tab" button in cell C2 of the *'IT Dependencies'* tab to push data to this tab.

DOCUMENTATION OF IDENTIFIED RISKS AND CONTROLS

ITGC Domain	Risk arising from the use of IT (as identified on tabs *'IT Dependencies'* and *'Other IT Risks'*)	Application(s) and other aspects of the IT environment impact by this risk	Is this risk relevant? (Yes / No)	Rationale if not relevent or partially not relevant (e.g., relevant only to specific applications)	Add / Delete ITGC	ITGC responsive to this risk (Select a library control from dropdown and tailor as appropriate)	Appli aspects to w (Updat spe
Access to programs and data	High-risk/powerful accounts (e.g., super-user) bypass systems-enforced authorization and segregation of duties controls	*Application*	*[Please Select]*		✚		*Applicati*
	Improper direct changes are made to underlying transaction records or master data	*Application*	*[Please Select]*		✚		*Applicati*
Program Change	Unauthorized or untested changes, or the failure to make necessary changes to application configuration and/or application programs prevent systems from processing transaction records completely and accurately	*Application*	*[Please Select]*		✚		*Applicati*

OAG Copyright

©Her Majesty the Queen in Right of Canada, as represented by the Auditor General of Canada, 2022

COPYRIGHT NOTICE—This document is intended for internal use. It cannot be distributed to or reproduced by third parties without prior written permission from the Copyright Coordinator for the Office of the Auditor General of Canada. This includes email, fax, mail and hand delivery, or use of any other method of distribution or reproduction.

CPA Canada Licence Agreement

© 2022 Chartered Professional Accountants of Canada. All Rights Reserved.
© 2022 IFRS Foundation. All Rights Reserved.
© 2022 International Federation of Accountants. All Rights Reserved.
© 2022 American Institute of Certified Public Accountants (CSAE 3416). All Rights Reserved."

CPA Canada Handbook sections and excerpts are reproduced herein for your non-commercial use with the permission of The Chartered Professional Accountants of Canada ("CPA Canada"). These may not be modified, copied or distributed in any form as this would infringe CPA Canada's copyright.

Reproduced, with permission, from the CPA Canada Handbook, The Chartered Professional Accountants of Canada, Toronto, Canada.