OAG Risk Assessment Process

Identifying IT risks relevant to the audit
Practice aid

Office of the Auditor General of Canada

Bureau du vérificateur général du Canada

Dec–2022
Template Owner: IT Audit

Identifying IT risks relevant to the audit

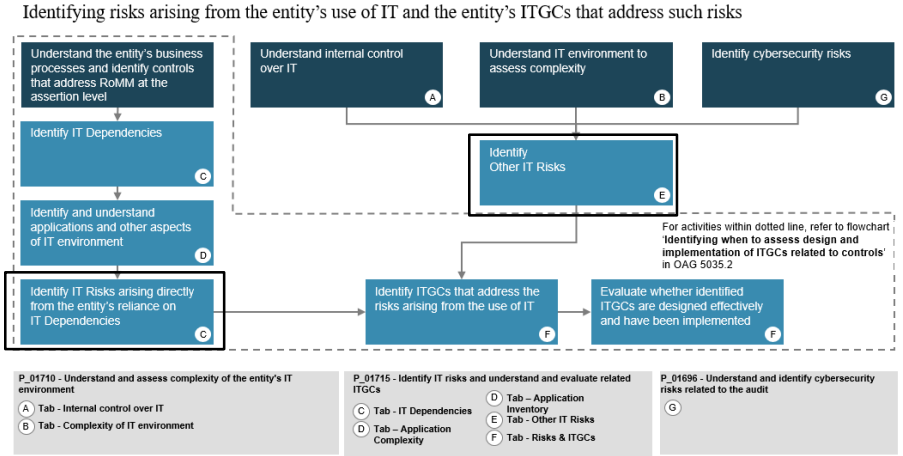
Table of contents

Identifying IT risks relevant to the audit Introduction (1 of 2)

This Practice Aid is designed to assist engagement teams when applying the OAG Risk Assessment Process in identifying whether commonly relevant IT risks are relevant to their audit. Commonly relevant IT risks are automatically displayed in the procedure “Identify IT risks and understand and evaluate related ITGCs” based upon the type of IT dependency identified by the engagement team when performing risk assessment procedures as well as the engagement team’s determination of the relevance of each of the identified IT dependencies to the audit plan. This Practice Aid provides “plain English” descriptions of each of the commonly relevant IT risks and describes circumstances when each may **not** be relevant to an audit even when the risk is commonly relevant to the IT dependency identified by the engagement team. Engagement teams can use this Practice Aid as a point of reference when determining and documenting the relevance of IT risks.

As a reminder, in applying OAG Audit 5035.2, we identify the following types of IT risks when understanding an entity’s IT environment and developing our audit plan (as highlighted by the black outlining of two boxes in the chart opposite):

- IT risks arising directly from the entity’s reliance on IT dependencies or that are the basis for our substantive procedures; and
- Other IT risks that occur at the entity-level that are not associated with underlying IT dependencies and are not application specific



This practice aid focuses on assisting engagement teams in determining the relevance of both types of risks to their engagement. For additional details about each step presented in the chart, refer to the OAG Risk Assessment Process IT Risks Quick Reference Guide.

Identifying IT risks relevant to the audit Introduction (2 of 2)

A summary of key reminders when identifying IT risks is provided on page 5 and pages 7 and 8 include a summary of the commonly relevant IT risks incorporated into the procedure "Identify IT risks and understand and evaluate related ITGCs". This practice aid also explains the typical relevance of each of the 18 IT risks to each type of IT dependency and/or other IT risks (hyperlinks to each of these risks are included in the summary on pages 7 and 8).

This document does not contain an exhaustive list of characteristics we may need to understand for the purposes of performing risk assessment procedures. The risks included in this document cover all risks and ITGCs that can be found in the procedure "Identify IT risks and understand and evaluate related ITGCs". IT risks and ITGCs identified during the audit might need to be tailored to the IT environment-specific facts and circumstances of the entity we are auditing.

This Practice Aid is not a substitute for reviewing the detailed requirements and guidance included in the OAG Audit manual. For detailed guidance refer to OAG Audit 5035.2 or contact IT Audit to assist you with any questions.

Identifying IT risks relevant to the audit
Key reminders

- 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, including identification of **controls in the control activities component** of the entity's system of internal control.
- Where we identify IT dependencies, we also identify the IT application or other aspects of the IT environment that relate to these IT dependencies and consider if they are subject to risks arising from the use of IT.
- As part of understanding the control activities component, we also need to consider if there are any entity wide IT risks (i.e., IT risks that are not associated with underlying IT dependencies and are not application specific such as ITGC wide risks, cyber risks or risks associated with new systems implementation).
- Identifying IT risks and related ITGCs arising from IT dependencies and / or Other IT risks 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.
- Where the only identified IT dependencies are system generated reports for which we plan to substantively test the reliability (i.e., completeness and accuracy) of the information included in such reports, we are not required to evaluate the design and implementation of ITGCs relevant to the system-generated reports.
- Because this can be a complex area, we may consider involving IT Audit specialists to assist in identifying IT applications and other aspects of the IT environment that may be subject to risks arising from the use of IT.
- 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.

Identifying IT risks relevant to the audit
How to use this practice aid

This practice aid helps to explain the typical relevance of each of the 18 IT risks to each type of IT dependencies and/or other IT risks. The following key has been used to indicate the expected applicability of each risk to the different types of IT dependencies or other IT risks:

When does it arise? IT dependency type and/or Other IT risks	**Automated controls**	**System-generated reports**	**Calculations**	**Restricted access/SoD**	**Interfaces**	**Other IT risks**

The colour coding for each of the IT dependencies determines the typical relevance of the IT risk:

	The risk is typically relevant to the audit
	The risk may or may not be relevant depending on the specific circumstances of the entity
	The risk is typically not relevant for this type of IT dependency/other IT risk sources

This practice aid also identifies ITGCs to address the IT risks. For audits with no prior IT involvement, the recommended ITGCs will be noted with a **(recommended)** following the control. Note that on page 14, the **(*recommended)** on the first ITGC indicates that this ITGC may be recommended based on the authentication settings. For more information on identifying appropriate ITGCs, please contact IT audit.

Identifying IT risks relevant to the audit
Summary of commonly relevant IT risks

(Click on Risk to navigate to additional details)

ITGC domain	Risk	Automated controls	System generated reports	Calculations	Restricted access/SoD	Interfaces	Other IT risks
ITGC wide considerations	Duties are not appropriately segregated						✓
	Governance of IT processes is not established						✓
Access to programs and data	Application end-users bypass systems-enforced authorization and segregation of duties controls				✓		
	High-risk/powerful accounts (e.g., super-user) bypass systems-enforced authorization and segregation of duties controls	✓	✓	✓	✓	✓	
	Improper direct changes are made to underlying transaction records or master data	✓	✓	✓	✓	✓	
	Weak authentication controls or security configurations allow access rights to be circumvented	✓	✓	✓	✓	✓	
	Unauthorized physical access to facilities, equipment and resources is not prevented						✓
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	✓	✓	✓		✓	
	Unauthorized or untested changes, or failure to make necessary changes to the databases/operating system/network prevent systems from processing transaction records completely and accurately						✓
	Unauthorized or untested changes, or failure to make necessary changes to batch processes prevent systems from processing transaction records completely and accurately					✓	

Identifying IT risks relevant to the audit
Summary of commonly relevant IT risks

ITGC domain	Risk	Automated controls	System generated reports	Calculations	Restricted access/SoD	Interfaces	Other IT risks
Program development	Newly implemented (or significantly enhanced) systems incompletely or inaccurately process data (e.g., due to erroneous coding/configuration)						✓
	Transaction records and/or master data are not completely and accurately migrated						✓
Computer operations	Inappropriate changes to, manual intervention in, or failures in job scheduling					✓	
	Transaction records transferred between systems are incomplete or inaccurate					✓	
	Transaction records are lost (e.g., due to system failure) and data is not recoverable or is corrupted/duplicated in the recovery process						✓
Cybersecurity (Cybersecurity risks and controls may relate to access to programs and data, computer operations, and/or other ITGC domains)	Cyber and ransomware attacks exploit vulnerabilities resulting in manipulation and/or destruction of data that impact the financial statements or affect system availability impacting timely financial reporting						✓
	Unpatched systems lead to exploiting known security vulnerabilities resulting in the manipulation and/or destruction of data that impacts the financial statements or affects system availability impacting timely financial reporting						✓
	Ransomware attacks result in inaccessible systems impacting system availability and the entity's ability to prepare financial reporting on a timely basis						✓

Note - Vendor setup/modifications and wire transfers are two common exposures that could give rise to a cybersecurity risk, however as these do not arise from the use of IT they are not part of this practice aid.

ITGC wide considerations

Risk	**Duties are not appropriately segregated**					
What is the risk?	**Lack of segregation of duties relating to the operation of ITGCs results in users having the ability to bypass controls relating to access and changes to applications, data and other aspects of the IT infrastructure.** This ITGC wide IT risk relates to whether a lack of segregation of duties in IT processes and IT controls may give rise to an IT risk. For example, if there is no physical separation of duties and / or members of other departments (such as finance) can perform IT related activities.					
When does it arise? IT dependency type and/or Other IT risks	**Automated controls**	**System generated reports**	**Calculations**	**Restricted access/SoD**	**Interfaces**	**Other IT risks**
When could this IT risk not be relevant to the audit?	This risk is likely to always be relevant to the audit, as our understanding of how the entity manages this risk contributes towards our audit response to the fraud risk of management override of controls (from an IT perspective, this risk comprises system enforced authorization and segregation of duties).					
Examples of IT dependencies that give rise to this risk	• N/A. Not related to IT dependencies.					
ITGCs to address the IT risk (tailor as appropriate for the entity's specific controls)	• Policies are maintained for segregation of duties within IT **(recommended)**					

ITGC wide considerations

Risk	**Governance of IT processes is not established**					
What is the risk?	**Lack of governance over the IT environment may result in an ineffective system of internal control over IT.** As with any other function within an entity, a clear governance structure (including policies, procedures, training, etc.) is important to support an effective system of internal control. Controls addressing this risk are key to ensuring that direct ITGCs are designed, implemented and operated effectively.					
When does it arise? IT dependency type and/or Other IT risks	**Automated controls**	**System generated reports**	**Calculations**	**Restricted access/SoD**	**Interfaces**	**Other IT risks**
When could this IT risk not be relevant to the audit?	This risk links to our understanding of the IT environment. This risk is not relevant to the audit if we conclude that there is appropriate governance within the entity's IT environment.					
Examples of IT dependencies that give rise to this risk	• N/A. Not related to IT dependencies.					
ITGCs as to address the IT risk (tailor as appropriate for the entity's specific controls)	• Governance structures over IT processes are established and implemented **(recommended)**					

Access to programs and data

Risk	**Application end-users bypass systems-enforced authorization and segregation of duties controls**
What is the risk?	**Users have been assigned access rights above and beyond or incompatible (from a segregation of duties perspective) with their role and/or responsibilities.** Controls at the application level that automate authorization tasks or enforce segregation of duties depend on the effectiveness of application access controls. This risk arises when management relies on the system to segregate duties or restrict access. When access is granted to data or functionality above and beyond a user's role or responsibilities (e.g., a junior member of the finance function with access to bonus data), or, when users are granted a combination of access rights which is incompatible with effective segregation of duties, (i.e., a combination of access rights which allow users to override authorization or segregation of duties controls, for example access to post and approve journals). This risk is usually linked to the risk "Weak authentication controls or security configurations allow access rights to be circumvented" in page 14.
When does it arise? IT dependency type and/or Other IT risks	**Automated controls** | **System generated reports** | **Calculations** | **Restricted access/SoD** | **Interfaces** | **Other IT risks**
When could this IT risk not be relevant to the audit?	This risk is always relevant to the audit when there is a Restricted access/SoD IT dependency.
Examples of IT dependencies that give rise to this risk	• Automated workflow approval of journal entries (SoD). • Access to payroll data is restricted to the Chief Financial Officer (restricted access).
ITGCs to address the IT risk (tailor as appropriate for the entity's specific controls)	• Access requests to the application are properly reviewed and authorized by management **(recommended)** • Access rights to applications are periodically monitored for appropriateness • Terminated application user access rights are removed on a timely basis **(recommended)**

Access to programs and data

Risk	High-risk/powerful accounts (e.g., super-user) bypass systems-enforced authorization and segregation of duties controls
What is the risk?	**Users have been assigned "administrator" or other privileged access rights which allows them to circumvent segregation of duties or restricted access and change controls.** This risk arises when users can create, modify or delete users and/or make changes to system functionality, bypassing the need for review or authorization. Users who are members of the IT function often have a higher level of access. In some cases users outside the IT function may also have a higher level of access. There are valid reasons for this level of access to be granted, as these users may need this access to configure IT dependencies (e.g., create and manage automated approval thresholds for payments) or administer access (e.g., creating user accounts for new employees and limiting what they can access to the applications, transactions and data they need to perform their job role and responsibilities). This risk is usually linked to the risk "Weak authentication controls or security configurations allow access rights to be circumvented" in page 14.
When does it arise? IT dependency type and/or Other IT risks	**Automated controls** · **System generated reports** · **Calculations** · **Restricted access/SoD** · **Interfaces** · **Other IT risks**
When could this IT risk not be relevant to the audit?	**For restricted access and segregation of duties:** • This risk is always relevant to the audit when there is a Restricted access/SoD IT dependency. **For automated controls, system generated reports, calculations and interfaces:** • **Coded:** This risk would not be relevant to the audit in the event that the system functionality cannot be changed, (i.e., the IT dependencies in scope are not subject to change by any user without accessing the software code and the entity has no access to the code (e.g., application licensed from a third party vendor with no access to the code and there are no customizations)). • **Configured:** This risk would not be relevant to the audit in the event that the entity **has appropriate segregation of duties within the IT department** (i.e., the consideration of restricted access to prevent unauthorized change and supporting ITGCs are typically addressed by IT Risks in the Program Change IT Domain and there are no IT users who could develop changes and unilaterally release them into the live environment without changes going through an independent review and approval before they are released).
Examples of IT dependencies that give rise to this risk	• Access to make changes to the consolidation rules in the consolidation application is restricted to IT users. • Any Automated controls, system generated reports, calculations and interfaces that are configured and/or customized.
ITGCs to address the IT risk (tailor as appropriate for the entity's specific controls)	• Access requests to the database/data file are properly reviewed and authorized by management • Terminated database/data file user access rights are removed on a timely basis • Super-user/administrative database/data file transactions or activities and sensitive generic IDs are monitored • Access rights to the database/data file are periodically monitored for appropriateness • Super-user/administrative operating system/network transactions or activities and sensitive generic IDs are monitored • Access rights to the operating system/network are periodically monitored for appropriateness • Access requests to the operating system/network are properly reviewed and authorized by management • Terminated operating system/network user access rights are removed on a timely basis • Super-user/administrative application transactions or activities and sensitive generic IDs are monitored • Privileged-level access (e.g., systems administrators) is authorized and appropriately restricted **(recommended)**

Access to programs and data

Risk	**Improper direct changes are made to underlying transaction records or master data**
What is the risk?	**Standing data is changed or deleted without appropriate review or authorization.** Transactional data or standing data (e.g., vendor master data) is usually stored in a database. Typically, IT users known as database administrators will have edit access to the databases in order to make changes or data corrections. When this access is not limited to authorized activities, there is a risk that financially relevant data is changed or deleted without appropriate approval. This risk is usually linked to the risk "Weak password controls or security configurations allow access rights to be circumvented" in page 14.
When does it arise? IT dependency type and/or Other IT risks	**Automated controls** | **System generated reports** | **Calculations** | **Restricted access/SoD** | **Interfaces** | **Other IT risks**
When could this IT risk not be relevant to the audit?	This risk will likely be relevant to the audit as it impacts the integrity of financial reporting and should be considered not only from an IT risk perspective but also from the perspective of a fraud risk of management override of control.
Examples of IT dependencies that give rise to this risk	It is a risk relating to the integrity of financial data overall, however it can also arise from calculations or system generated reports that pull standing data, for example: • A foreign currency translation calculation drawing standing FX rates as defined by the entity • A system generated report that pulls customers' data
ITGCs to address the IT risk (tailor as appropriate for the entity's specific controls)	• Super-user/administrative database/data file transactions or activities and sensitive generic IDs are monitored • Super-user/administrative application transactions or activities and sensitive generic IDs are monitored • Access requests to the database/data file are properly reviewed and authorized by management **(recommended)** • Access requests to the application are properly reviewed and authorized by management **(recommended)** • Access rights to the database/data file are periodically monitored for appropriateness • Access rights to applications are periodically monitored for appropriateness • Terminated database/data file user access rights are removed on a timely basis **(recommended)** • Terminated application user access rights are removed on a timely basis **(recommended)**

Access to programs and data

Risk	**Weak authentication controls or security configurations allow access rights to be circumvented**
What is the risk?	**Weak passwords or security configurations allow unauthorized access.** While we consider authentication controls and security configurations distinctly from the other risks and controls, this risk is typically considered together with one or more of the other Access to Programs and Data risks (as addressed on pages 11 to 13) when making our assessment. This includes other authentication mechanisms, such as two factor authentication (2FA), for example when the user's password is entered, a code is sent to the user's mobile phone and must also be entered before gaining access. This risk can differ at the application, operating system and database layers.
When does it arise? IT dependency type and/or Other IT risks	**Automated controls** | **System generated reports** | **Calculations** | **Restricted access/SoD** | **Interfaces** | **Other IT risks**
When could this IT risk not be relevant to the audit?	**For restricted access and segregation of duties:** This risk is always relevant to the audit when there is a Restricted access/SoD IT dependency. **For automated controls, system generated reports, calculations and interfaces:** This risk is typically considered together with one or more of the other Access to Programs and Data risks (as addressed on pages 11 to 13) and therefore, if the engagement team concluded the other Access to Programs and Data risks are relevant to these types of IT dependency, this risk will also be relevant.
Examples of IT dependencies that give rise to this risk	• System access to make changes to vendor master data is restricted and segregated from the approval of payments.
ITGCs to address the IT risk (tailor as appropriate for the entity's specific controls)	• Passwords to the operating system/network and security configurations are set in an effective manner **(*recommended)** • Passwords to the database/data file and security configurations are set in an effective manner **(recommended)** • Passwords to applications and security configurations are set in an effective manner **(recommended)**

Access to programs and data

Risk	**Unauthorized physical access to facilities, equipment and resources is not prevented**					
What is the risk?	**Unauthorized physical access can result in data and systems being unavailable or processed inaccurately/incompletely.**					
When does it arise? IT dependency type and/or Other IT risks	**Automated controls**	**System generated reports**	**Calculations**	**Restricted access/SoD**	**Interfaces**	**Other IT risks**
When could this IT risk not be relevant to the audit?	This risk is likely not to be relevant to the audit in most engagements. However, engagement teams need to consider how likely it is that the data needed to produce the financial statements will be impacted by unauthorized physical access when taken in the context of the wider control environment. When an entity has outsourcing arrangements such as SaaS, PaaS or IaaS or a third party data center, if the team concludes that this IT risk, related to physical access, is relevant to the audit, it will be important that the risk is addressed by controls within the scope of the service organization's service auditor's report over internal controls and any relevant Complementary User Entity controls will need to be implemented by the entity we audit.					
Examples of IT dependencies that give rise to this risk	• N/A. Physical access risks are not normally considered to directly impact risks arising from IT dependencies					
ITGCs to address the IT risk (tailor as appropriate for the entity's specific controls)	• Physical security measures are in place **(recommended)**					

Program change

Risk	**Unauthorized or untested changes, or the failure to make necessary changes to application configurations and/or application programs prevent systems from processing transaction records completely and accurately**
What is the risk?	**Reliance on system functionality that is processing inaccurate data, inaccurately processing data or both.** Configuration is an important aspect in many applications as it aligns the way the system works to the entity's needs. **For Application Configuration Changes**: Users (IT or business users) may bypass change controls and make unauthorized changes to application configuration settings. In addition, the entity may fail to make changes that are necessary to configuration (e.g., changes that are required to be implemented due to new regulations, accounting standards or policies). **For Application Program Changes:** Code is written into the application inherent functionality, typically by the vendor, and cannot be changed to fit the entity's needs unless IT or other users can make changes to the code, in which case this risk arises. The risk also arises when there is a need to change code due to changes in, for example, financial reporting or regulatory changes and the code is not changed. This risk also arises when third parties have access to make changes to the code directly into the entity's IT environment. This risk can be considered together with incident management risks, i.e., the risks that defects or errors in the processed changes are not detected and resolved. Differentiating configuration changes from program changes: configuration changes alter the behaviour of the application without the need to modify the code (e.g., selecting configurable options for approval thresholds).
When does it arise? IT dependency type and/or Other IT risks	**Automated controls** | **System generated reports** | **Calculations** | **Restricted access/SoD** | **Interfaces** | **Other IT risks**
When could this IT risk not be relevant to the audit?	**For Application Configuration Changes:** This risk is not relevant to the audit if there are no IT dependencies that are configured/configurable. **For Application Program Changes:** This risk is not relevant to the audit if the entity does not have in-house development or coding or when developers (including third parties) cannot make changes to the coded functionality.
Examples of IT dependencies that give rise to this risk	**For Automated controls, system generated reports and calculations:** •This risk is relevant to any IT dependency that has been configured or is configurable. For example, a three way match automated control that can be configured to match under a certain threshold (e.g., the matching would happen if the difference is less than 5%) **For interfaces:** •This risk is typically relevant if the interface or batch process depends on a program to trigger the transfer of data.
ITGCs to address the IT risk (tailor as appropriate for the entity's specific controls)	• Changes to application configurations and/or application programs are adequately tested and approved before being migrated into production **(recommended)** • Changes processed to application configurations and/or application programs are periodically monitored for appropriateness • Development, testing and production environments are segregated for changes to application configurations and/or application programs **(recommended)**

Program change

Risk	**Unauthorized or untested changes, or failure to make necessary changes to the databases/operating system/network prevent systems from processing transaction records completely and accurately**					
What is the risk?	**Changes, or failure to make changes to the IT environment in which applications run (i.e., database(s), operating systems and network(s)) may result in inaccurate data being processed or the systems inaccurately processing data or both.** Changes (or failure to make changes) may result in the application not continuing to function as intended and/or users not being able to access the application (i.e., the application crashes or freezes). This risk needs to be considered when there are major upgrades to the IT infrastructure. This risk can be considered together with incident management risks, i.e., the risks that defects or errors in the processed changes are not detected and resolved.					
When does it arise? IT dependency type and/or Other IT risks	**Automated controls**	**System generated reports**	**Calculations**	**Restricted access/SoD**	**Interfaces**	**Other IT risks**
When could this IT risk not be relevant to the audit?	If the only changes to the IT environment have been routine vendor-supplied patches or hot-fixes at the operating system layer, then this risk would likely not be relevant to the audit. If the audit plan does not involve testing the operating effectiveness of ITGCs, this risk would likely not be relevant to the audit.					
Examples of IT dependencies that give rise to this risk	• N/A. Unauthorized or untested changes, or failure to make changes to database (s) operating systems/network (s) risks are not normally considered to directly impact risks arising from IT dependencies					
ITGCs to address the IT risk (tailor as appropriate for the entity's specific controls)	• Changes to the operating system/network adequately tested and approved before being migrated into production • Changes processed to the Operating System/Network are periodically monitored for appropriateness • Changes to databases are adequately tested and approved before being migrated into production • Changes processed to databases are periodically monitored for appropriateness • Development, testing and production environments are segregated for changes to operating system/network • Development, testing and production environments are segregated for changes to databases					

Program change

Risk	**Unauthorized or untested changes, or failure to make necessary changes to batch processes prevent systems from processing transaction records completely and accurately**
What is the risk?	**Data is not transferred completely/accurately between systems or multiple transactions which are automatically processed as a single group are not processed.** An interface is the transfer of transactional data from one application to another (e.g., inventory levels at a warehouse from a warehouse management system to the finance application). A batch process is when there are automatic updates set up in the system that replace what would normally have had manual input (e.g., automatically updating the pricing data relating to an investment product on a daily basis). Unauthorized changes to these processes or, failures to make required changes, may result in incomplete and/or inaccurate of financial data. This risk can be considered together with incident management risks, i.e., the risks that defects or errors in the processed changes are not detected and resolved.
When does it arise? IT dependency type and/or Other IT risks	Automated controls | System generated reports | Calculations | Restricted access/SoD | **Interfaces** | Other IT risks
When could this IT risk not be relevant to the audit?	This risk will always be relevant to the audit for interfaces or multiple transactions which are automatically processed as a single group through batch processes.
Examples of IT dependencies that give rise to this risk	• Interface between a warehouse management system and a finance application • Interface between a point of sale system and a finance application • Batch updates of pricing data
ITGCs to address the IT risk (tailor as appropriate for the entity's specific controls)	• Changes to application configurations are adequately tested and approved before being migrated into production • Changes processed to application configurations are periodically monitored for appropriateness • Development, testing and production environments are segregated for changes to application configurations • Only approved and tested changes are made to the batch scheduler **(recommended)**

Program development

Risk	**Newly implemented (or significantly enhanced) systems incompletely or inaccurately process data (e.g., due to erroneous coding/configuration)**					
What is the risk?	**New applications being implemented, or existing applications being significantly modified, could inaccurately process data.** This could be due to the system not behaving as the business users intended, either because requirements were misunderstood and this was not identified in testing, or because a conscious decision was made to go live despite known defects.					
When does it arise? IT dependency type and/or Other IT risks	**Automated controls**	**System generated reports**	**Calculations**	**Restricted access/SoD**	**Interfaces**	**Other IT risks**
When could this IT risk not be relevant to the audit?	If no new applications or other aspects of the IT environment are implemented or significantly modified during the period then this risk is likely not relevant to the audit.					
Examples of IT dependencies that give rise to this risk	• N/A. Risks arising from newly implemented or significantly modified systems are not normally considered to directly impact risks arising from IT dependencies.					
ITGCs to address the IT risk (tailor as appropriate for the entity's specific controls)	• New systems/enhancements are adequately tested and approved before being migrated into production **(recommended)** • Problems during program development are monitored and resolved • Appropriate training is performed					

Program development

Risk	**Transaction records and/or master data are not completely and accurately migrated**					
What is the risk?	**Data is not transferred completely or accurately when there is a new system implementation/migration.** When an entity implements a new application and/or migrates the existing application to another database, server or to the Cloud, there is a risk that standing data such as vendor master data, sub-ledgers data or transactional data may not be transferred completely and/or accurately.					
When does it arise? IT dependency type and/or Other IT risks	**Automated controls**	**System generated reports**	**Calculations**	**Restricted access/SoD**	**Interfaces**	**Other IT risks**
When could this IT risk not be relevant to the audit?	This risk will likely be relevant only when the entity undertakes a system implementation, if data from an old application will not be migrated to the new application (i.e., when the new application will only be used to process transactions prospectively from the date of implementation).					
Examples of IT dependencies that give rise to this risk	• N/A. Risks arising from the migration of transaction records and/or master data are not normally considered to directly impact risks arising from IT dependencies					
ITGCs to address the IT risk (tailor as appropriate for the entity's specific controls)	• Data is properly migrated/converted **(recommended)**					

Computer operations

Risk	**Inappropriate changes to, manual intervention in, or failures in job scheduling**
What is the risk?	**Data is not transferred completely/accurately between systems or multiple transactions which are automatically processed as a single group are not processed due to inappropriate changes to batch processes (manual or otherwise) or issues when the batch processes are executed.** A batch process is when there are automatic updates set up in the system that replace what would normally have had manual input for multiple transactions that are processed as a single group (e.g., automatically updating the pricing data relating to an investment product on a daily basis). If these batch processes are changed or there are errors or failures when they are executed, this may result in incomplete and/or inaccurate of financial data.
When does it arise? IT dependency type and/or Other IT risks	Automated controls · System generated reports · Calculations · Restricted access/SoD · **Interfaces** · Other IT risks
When could this IT risk not be relevant to the audit?	This risk will always be relevant to the audit for interfaces or multiple transactions which are automatically processed as a single group automatic updates through batch processes.
Examples of IT dependencies that give rise to this risk	• Daily batch updates of pricing data • Monthly automatic updates of foreign exchange rates in financial reporting application.
ITGCs to address the IT risk (tailor as appropriate for the entity's specific controls)	• Errors in production processing are identified and resolved • Only approved and tested changes are made to the batch scheduler **(recommended)**

Computer operations

Risk	**Transaction records transferred between systems are incomplete or inaccurate**
What is the risk?	**Data is not transferred completely/accurately between applications.** An interface is the transfer of transactional data from one application to another. This risk specifically relates to information that needs to be transferred from one application to another in order for ITGCs to operate effectively (e.g., when information relating to joiners, movers or leavers is automatically transferred from an HR system to the identity management system used by the IT department to manage access, so access can be granted on a timely basis and aligned to the joiner's roles and responsibilities or access can be terminated on a timely basis when a staff member leaves the company).
When does it arise? IT dependency type and/or Other IT risks	**Automated controls** | **System generated reports** | **Calculations** | **Restricted access/SoD** | **Interfaces** | **Other IT risks**
When could this IT risk not be relevant to the audit?	This risk is not relevant to the audit when there are no transaction records transferred between systems that are significant to IT General Controls (i.e., in order for the ITGCs to operate effectively they do not need to receive information or records from another system).
Examples of IT dependencies that give rise to this risk	• Automated access termination relies on leavers data automatically transferred from the HR system; • The active employees within the Finance Department data, including their roles, is transferred automatically from the Human Resources system to the access management tool the IT department uses to perform periodic reviews of access rights
ITGCs to address the IT risk (tailor as appropriate for the entity's specific controls)	• Errors in production processing are identified and resolved **(recommended)** • Only approved and tested changes are made to the batch scheduler

Computer operations

Risk	**Transaction records are lost (e.g., due to system failure) and data is not recoverable or is corrupted/duplicated in the recovery process**					
What is the risk?	**Data is lost, corrupted or duplicated.** By not being able to access complete and accurate data that is relevant to financial reporting, the entity will not be able to produce complete and accurate financial statements. This risk is linked to the cybersecurity risk relating to ransomware, see page 26.					
When does it arise? IT dependency type and/or Other IT risks	Automated controls	System generated reports	Calculations	Restricted access/SoD	Interfaces	**Other IT risks**
When could this IT risk not be relevant to the audit?	If the team has not determined there is a risk of material misstatement relating to data loss/data corruption as a result of a cyber incident, this risk may not be relevant to the audit.					
Examples of IT dependencies that give rise to this risk	• N/A. Risks arising from backups or data availability are not normally considered to directly impact risks arising from IT dependencies					
ITGCs to address the IT risk (tailor as appropriate for the entity's specific controls)	• Data is appropriately backed up and recoverable **(recommended)**					

Cybersecurity

Risk	**Cyber and ransomware attacks exploit vulnerabilities resulting in manipulation and/or destruction of data that impact the financial statements or affect system availability impacting timely financial reporting**					
What is the risk?	**The entity cannot prevent or limit damage caused by cyber attacks.** A vulnerability is a weakness in a system that could be exploited or triggered by a threat source (e.g., a hacker). All systems have some level of vulnerability and if not managed by the entity through their cybersecurity program it could result in data loss, data destruction or prevent the entity from accessing the systems, impacting their ability to operate and report on a timely basis.					
When does it arise? IT dependency type and/or Other IT risks	**Automated controls**	**System generated reports**	**Calculations**	**Restricted access/SoD**	**Interfaces**	**Other IT risks**
When would this not represent a risk of material misstatement (RoMM) (*)	This would not represent a risk of material misstatement if, based on the understanding of the entity's cybersecurity risk assessment and the common exposure "Intrusion prevention/detection and monitoring", including understanding the entity's incident monitoring program and network architecture, the engagement team determines cyber or ransomware attacks do not give rise to a risk of material misstatement of the entity's financial statements.					
Examples of IT dependencies that give rise to this risk	• N/A. Risks arising from vulnerabilities are not normally considered to directly impact risks arising from IT dependencies.					
ITGCs to address the IT risk (tailor as appropriate for the entity's specific controls)	• An intrusion prevention/detection program is in place to ensure security incidents are monitored and reported to relevant stakeholders **(recommended)** • A patch management program is in place to ensure security vulnerabilities are addressed, monitored and reported **(recommended)** • Financially significant data is backed up on an appropriate basis and periodically tested for recoverability **(recommended)**					

(*) Given the nature and pervasiveness of cyber crime, all entities may be subject to cyber risks; however engagement teams need to consider whether these are relevant to the entity in relation to how the entity's business model integrates the use of IT and how common cybersecurity exposures may give rise to **risks of material misstatement** to the financial statements. See OAG Audit 5035.2 – Cybersecurity Risk Assessment Considerations for further guidance and refer to additional risk considerations in the procedure 'Understand and identify cybersecurity risks related to the audit'.

Cybersecurity

Risk	**Unpatched systems lead to exploiting known security vulnerabilities resulting in the manipulation and/or destruction of data that impacts the financial statements or affects system availability impacting timely financial reporting**
What is the risk?	**Known vulnerabilities are not fixed through a patch, increasing the risk of these vulnerabilities being exploited in a cyber attack.** When a vendor becomes aware that an application or other software contains a potential security issue, they would typically fix the issue by distributing a patch or software update which entities need to implement in order to protect themselves from being hacked. If the patch is missed or not applied on a timely basis, it could result in hackers accessing the entity's system(s).
When does it arise? IT dependency type and/or Other IT risks	Automated controls | System generated reports | Calculations | Restricted access/SoD | Interfaces | **Other IT risks**
When would this not represent a risk of material misstatement (RoMM) (*)	Unpatched systems would not represent a risk of material misstatement if, based on the understanding of the entity's cybersecurity risk assessment and the common exposure "Patch management", including understanding the entity's patch management policies and procedures, the engagement team determines unpatched systems do not give rise to a risk of material misstatement of the entity's financial statements.
Examples of IT dependencies that give rise to this risk	• N/A. Risks arising from unpatched systems are not normally considered to directly impact risks arising from IT dependencies.
ITGCs to address the IT risk (tailor as appropriate for the entity's specific controls)	• A patch management program is in place to ensure security vulnerabilities are addressed, monitored and reported **(recommended)**

(*) Given the nature and pervasiveness of cyber crime, all entities may be subject to cyber risks; however engagement teams need to consider whether these are relevant to the entity in relation to how the entity's business model integrates the use of IT and how common cybersecurity exposures may give rise to **risks of material misstatement** to the financial statements. See OAG Audit 5035.2 – Cybersecurity Risk Assessment Considerations for further guidance and refer to additional risk considerations in the procedure 'Understand and identify cybersecurity risks related to the audit'.

Cybersecurity

Risk	**Ransomware attacks result in inaccessible systems impacting system availability and the entity's ability to prepare financial reporting on a timely basis**					
What is the risk?	**The entity cannot access data and/or systems relevant to financial reporting.** Ransomware is malicious software that makes data or systems unusable until the victim makes a payment ('ransom'). This risk is related to the risk "Transaction records are lost (e.g., due to system failure) and data is not recoverable or is corrupted/duplicated in the recovery process" (see page 23).					
When does it arise? IT dependency type and/or Other IT risks	**Automated controls**	**System generated reports**	**Calculations**	**Restricted access/SoD**	**Interfaces**	**Other IT risks**
When would this not represent a risk of material misstatement (RoMM) (*)	Ransomware would not represent a risk of material misstatement if, based on the understanding of the entity's cybersecurity risk assessment and the backup and recovery common exposure, including understanding the entity's backup strategy and recovery plans, the engagement team determines a ransomware attack does not give rise to a risk of material misstatement of the entity's financial statements.					
Examples of IT dependencies that give rise to this risk	• N/A. Risks arising from ransomware are not normally considered to directly impact risks arising from IT dependencies.					
ITGCs to address the IT risk (tailor as appropriate for the entity's specific controls)	• Financially significant data is backed up on an appropriate basis and periodically tested for recoverability **(recommended)**					

(*) Given the nature and pervasiveness of cyber crime, all entities may be subject to cyber risks; however engagement teams need to consider whether these are relevant to the entity in relation to how the entity's business model integrates the use of IT and how common cybersecurity exposures may give rise to **risks of material misstatement** to the financial statements. See OAG Audit 5035.2 – Cybersecurity Risk Assessment Considerations for further guidance and refer to additional risk considerations in the procedure 'Understand and identify cybersecurity risks related to the audit'.