

- that are associated with SUTs (refer to activity '[Identify SUTs](#)') or related parties (refer to activity '[Obtain an understanding of related party processes and controls](#)');
- that are associated with journal entries and other adjustments (refer to activity '[Evaluate the design and implementation of control activities over journal entries and other adjustments](#)'); or
- where we cannot obtain sufficient evidence through substantive testing alone; or
- process control activities:
 - that we are testing over the accuracy and completeness of internal information and the RDE(s) to evaluate the reliability of such information (see activity '[Test management's controls over the accuracy and completeness of internal information](#)'); or
 - that, in our professional judgment, we consider it appropriate to understand in order to enable us to effectively identify and assess the risk of material misstatement and design further audit procedures; and
- general IT controls that address 'relevant RAFITs' associated with 'relevant automated controls' or data integrity risks (refer to question '[Under what circumstances do we obtain an understanding of general IT controls](#)').

[What is an example of the differences and relationship between process activities and control activities?](#)

[ISA | 1343.11410]

Consider the following example — the credit limit illustrates the differences and relationship between process activities and control activities.

Process activities	Customers place their purchase orders electronically. These orders are captured in the entity's enterprise resource planning (ERP) system and processed for fulfilment.
Identified risk	Customers could exceed their established credit limit.
Control activities to address the identified risk	The entity's ERP system compares the open receivables from the customer plus the submitted purchase order amount to the established customer credit limit. If the total amount of open receivables and purchase orders exceeds the credit limit, the purchase order is not processed further. Each purchase order not processed is followed-up manually.

[Why do we evaluate the design and implementation of process control activities?](#) [ISA | 1343.1800]

We evaluate the design and implementation of process control activities as a part of our risk assessment activities to provide an appropriate basis for the identification, assessment of and response to risks of material misstatement.

Even though our identification and assessment of RMMs is based on inherent risk, evaluating the design and implementation of process control activities provides a contextual understanding that may be helpful when we identify and assess risks, including:

- the PRPs (the 'where' and the 'how' a misstatement could occur); and
- the control activities management have designed and implemented to mitigate them.

[How do we evaluate the design of a process control activity?](#) [ISA | 1343.12135]

Evaluating the *design* of a process control activity involves considering whether the control is capable of effectively preventing, or detecting and correcting material misstatements, either individually or in combination with other controls.

Determining whether a control has been designed effectively means determining if the control activity:

- satisfies the company's control objectives by addressing the PRPs it is intended to address, and
- operates at a level of precision that 'would' prevent or detect and correct a material misstatement.

We evaluate design through inquiry, *in combination with* observation and/or inspection.

[How do we evaluate the implementation of a process control activity?](#) [ISA | 1343.12136]

The *implementation* of a process control activity means that the control exists and that the entity is using it.

We evaluate implementation through inquiry, *in combination with* observation and/or inspection.

Determining whether a control has been implemented means determining whether the control exists and whether the entity is using it.

[What do we consider when we evaluate the design and implementation of a process control activity?](#) [ISA | 1343.12138]

The table below sets out the items we consider when we evaluate the design and implementation of a process control activity.

We specifically understand the criteria / threshold for investigation used to identify outliers and for each attribute, whether the control operator uses judgment.

What do we understand about a control?	Description
Control objective	The risk the control is intended to mitigate - i.e., the relevant PRPs the control addresses.
Anti-fraud control	Controls designed to detect, prevent or deter fraud.
Nature and type of control	'Nature' refers to whether the control is manual or automated.

	'Type' refers to whether the control is preventive or detective.
<u>Frequency</u>	Frequency with which the manual control activity is performed: <ul style="list-style-type: none"> • annually • quarterly • monthly • weekly • daily • recurring • ad hoc
<u>Authority and competence of the control operator</u>	The level of competence and authority necessary to operate a manual control. Understanding who typically operates the control and why they do so may be useful, so that we can define what level of competence and authority is necessary.
<u>Judgment involved</u>	Subjectivity in determining whether something is an outlier and/or whether an outlier is correct/ reasonable.
<u>Level of precision</u>	The level of precision, including the criteria/threshold for investigation used to identify outliers.
<u>Investigation and resolution process</u>	If the control activity involves judgment, evaluating the steps performed by the control operator to investigate and resolve outliers.
<u>Information relied on in the performance of the control activity</u>	Information used when performing the control (e.g., system reports, manually prepared spreadsheets, data), including the relevant data elements.
Documentation maintained	A description of the documentation maintained to evidence the performance of the control activity

What is a control operator? [ISA | 1343.8445]

The control operator is a term used to describe who or what performs the control. In a manual control, the control operator is the individual who performs the control. In an automated control, the control operator is the IT system.

What if a control activity is ineffective in its design and/or implementation? [ISA | 1343.2200]

If we determine that a control activity is ineffective in its design and/or implementation (refer to activity '[Determine whether a deficiency in ICFR exists and describe it](#)'), we:

- conclude that there is a deficiency;
- do not plan to rely on or test the operating effectiveness; and
- consider the effect of that deficiency on the procedures we plan to perform as part of our response to an RMM and modify them accordingly.

[What are example process control activities related to cash and cash equivalents?](#) [ISA | 1343.8446]

Process control activities related to cash and cash equivalents may include process control activities over the segregation of duties required, such as for:

- Opening and closing bank accounts; and
- Ability to access cash (authorized signers).

Additional relevant business process control activities related to cash and cash equivalents may include process control activities over accurate classification of cash and cash equivalents.

1.3.1 Understand whether the control activity addresses the control objective

[ISA | 7624]

What do we do?

Understand whether the control activity appropriately addresses the control objective.

Why do we do this?

We understand the objective of a control activity to evaluate whether the control is appropriately addressing the PRP (process control activities) or RAFIT (GITCs), as appropriate, that it was designed to address.

If we do not have a sufficient understanding of the control objective, we are not able to determine whether a control is effectively designed or implemented

Execute the audit

[How do we determine whether the design of a control activity achieves its objective?](#) [ISA | 7624.12221]

To evaluate whether a control addresses each PRP or RAFIT it is intended to address, we understand how the control activity is performed, which means identifying control attributes. Control attributes are the specific procedures performed by the control operator that make-up the control activity and are important to the design of the control.

Another way of thinking about control attributes is that they are the parts of the control that addresses the risk(s) the control is intended to address. For example, if it's important that the control operator reconciles A to B, then that's a control attribute. If it's not important whether the reconciliation is saved to file folder A or B when complete, then that is not a control attribute.

See the following list for more example control attributes for example process control activities.

Control Description	Example Control Attributes - How the control activity is performed
Fixed asset sub-ledger to general ledger reconciliation	Control operator agrees the fixed asset subledger report to the fixed asset reconciliation.
	Control operator agrees the fixed asset general ledger amount to the fixed asset reconciliation.
	Control operator reconciles the two amounts within \$10,000.
	Control operator investigates any outliers (i.e., differences greater than \$10,000) and decides on how to resolve the differences.
Physical inventory reconciliation	Control operator agrees quantities per the final physical inventory count sheets to the reconciliation. (Other controls operated over the physical inventory observation, resulting in the final count sheets.)
	Control operator agrees the pre-adjustment sub-ledger balance to the reconciliation
	Control operator checks that for any inventory item with a count difference greater than \$5,000, a second count was performed per the count sheets.
	Control operator agrees result of the reconciliation to the adjusting journal entry and checks on a test basis that the quantities in the post-adjustment sub-ledger agree to the count sheets.
Management review of the revenue forecast used in the valuation of a goodwill reporting unit	Control operator agrees the historical data presented on the forecast spreadsheet to the prior year financial statements (i.e. the control operator reconciles completeness and accuracy of data used in the operation of the control to its source)
	Control operator sets an expectation for year one revenue growth based on review of the following internal and external sources:

	<ul style="list-style-type: none"> • peer group company 3-year historical growth; • peer group 12-month prospective growth forecast, when available; • industry analyst 12-month revenue forecast for the relevant industry; • internal sales group revenue goals by product line, and comparison of past sales goals with sales results.
	<p>Control operator sets an expectation for year 2-5 revenue growth based on the following internal and external sources:</p> <ul style="list-style-type: none"> • Five-year historical company-specific and industry-specific historical growth trends; • Internal sales group revenue goals by product line, and comparison of past sales goals with sales results.
	<p>Control operator compares the revenue forecast for the terminal value to the 10-year average rate of inflation for the relevant currency and investigates differences greater than 0.5% of revenue.</p>
	<p>Control operator compares the actual forecast for each of the periods listed with the expectation and investigates outliers that differ by more than USD 10 million or 1.5% of the expectation. Outliers are investigated and resolved with persuasive supporting evidence or adjustment to the forecast.</p>
System A is configured to process orders for active customers within their credit limit (less outstanding AR + pending order totals)	<p>The system does not process orders for inactive customers.</p>
	<p>The system processes orders for active customers.</p>
	<p>The system places the order on a hold status and does not process the order, if the order exceeds the customer's credit limit (less outstanding AR + pending order totals).</p>
The General Ledger (GL) system is configured to accurately and completely	<p>The GL system is configured to map fixed asset transactions to GL account codes based on the fixed asset type assigned to the</p>

<p>map GL account codes to fixed asset transactions based on the fixed asset type assigned to the transactions.</p>	<p>transactions. There are two fixed asset types that are mapped as follows:</p> <p>Fixed asset type ABC: GL account code 123</p> <p>Fixed asset type DEF: GL account code 456</p>
	<p>When a fixed asset transaction is processed in the GL system, it will automatically post the transaction to the GL account code based on the fixed asset type.</p>
	<p>The GL system is configured to post fixed asset transactions to a suspense account if the transaction's fixed asset type has not been mapped to a specific GL account code.</p>
<p>At each period-end, the control operator(s) reviews each note in the financial statements to assess the fair presentation, completeness and accuracy of the required disclosures.</p>	<p>Control operator completes an accounting disclosure checklist and compares it to each note.</p>
	<p>Control operator agrees or reconciles information in the disclosures to the underlying accounting records.</p>
	<p>Control operator reviews the accuracy of the qualitative (accounting policies or principles) and quantitative (financial) information for accuracy and whether the information is fairly presented.</p>

For examples of general IT control attributes, refer to question '[How do we determine whether the design of a general IT control achieves its objective?](#)'.

Do all control activities have attributes? [ISA | 7624.12222]

Yes, all control activities have at least one attribute. Depending upon how the control is defined by the entity, controls may have more than one attribute as shown in the examples included in the table above.

What if a control activity is ineffective in its design and/or implementation? [ISA | 7624.2200]

If we determine that a control activity is ineffective in its design and/or implementation (refer to activity '[Determine whether a deficiency in ICFR exists and describe it](#)'), we:

- conclude that there is a deficiency;
- do not plan to rely on or test the operating effectiveness; and
- consider the effect of that deficiency on the procedures we plan to perform as part of our response to an RMM and modify them accordingly.

1.3.2 Understand whether the control is an anti-fraud control [ISA | 1344]

What do we do?

Understand whether the control is an anti-fraud control (the objective of the control is to prevent, detect, or deter fraud).

Why do we do this?

Entities put anti-fraud controls in place to detect, prevent and deter fraud. Since certain process control activities are designed to address fraud risks in the audit, this influences how we approach testing those controls.

Execute the Audit

What is an anti-fraud control? [ISA | 1344.1600]

An anti-fraud control is a:

- Process control activity that directly addresses an identified risk of fraud at the assertion-level or financial statement-level; or
- CERAMIC control that supports the effective functioning of process control activities that directly address an identified risk of fraud.

When do we identify a process control activity as an anti-fraud control? [ISA | 1344.1500]

We identify a process control activity as an anti-fraud control when:

- we have identified a fraud risk at the assertion level or financial statement level; and
- the process control activity directly mitigates the identified fraud risk, either on its own or in combination with other control activities.

Can a process control activity that addresses risks of both fraud and error be an anti-fraud control? [ISA | 1344.12141]

Yes. When a process control activity addresses both a fraud risk and an inherent risk of error, we identify the process control activity as an anti-fraud control.

What are some examples of anti-fraud controls? [ISA | 1344.1601]

Examples of anti-fraud controls include controls:

- over significant unusual transactions, particularly those that result in late or unusual journal entries;
- over period-end financial reporting process, including controls over non-standard journal entries and adjustments;
- over transactions with related parties, including significant related-party transactions outside the entity's normal course of business;
- related to accounting estimates that give rise to significant risks;

- that mitigate incentives for, and pressures on, management to falsify or inappropriately manage financial results;
- designed to prevent, deter and detect fraud (e.g. controls to promote a culture of honesty and ethical behavior); and
- specific controls designed to mitigate specific risks of fraud (e.g. controls to address risks of intentional misstatement of specific accounts).

How do we consider the risk of management override when we evaluate anti-fraud process control activities? [ISA | 1344.1700]

When we identify process risk points and determine which process control activities are relevant to the audit, we also consider the risk of management override of controls. This includes the risks related to the recording of inappropriate journal entries and other adjustments. Specifically, we identify process risk points related to the recording of journal entries and other adjustments and the process control activities that address them.

Process control activities that address the risk of management override of controls through the recording of journal entries and other adjustments may:

- be performed by control operators who are not subject to management control, such as an independent internal audit function that reports directly to those charged with governance; and/or
- have established appropriate segregation of duties that reduce opportunities for an individual within an organization to both perpetrate and conceal fraud.

Examples of anti-fraud process control activities that may be designed and implemented by an entity to address the risk of management override of controls through the recording of inappropriate journal entries and other adjustments include:

- prevention of executive management from independently initiating, authorizing, or recording journal entries within the IT system; and
- internal audit reviewing journal entries, other adjustments and related supporting documentation for possible override of controls as an objective party.

1.3.3 Understand the nature and type of the control

[ISA | 1345]

What do we do?

Obtain an understanding of the nature and type of the control

Why do we do this?

Our understanding of the nature and type of a control helps us:

- update our risk assessment; and
- identify types of potential misstatements and factors that affect our assessment of risks.

Execute the Audit

[What is the 'nature' of a control?](#) [ISA | 1345.1300]

The 'nature' of a control refers to whether the control is manual or automated.

[What are manual controls?](#) [ISA | 1345.1400]

Manual controls are performed by people. They may not be consistently applied because of the chance for human error.

[What are automated controls?](#) [ISA | 1345.1500]

Automated controls are performed by IT systems in the same way each time they operate.

[How do IT systems perform automated controls?](#) [ISA | 1345.12144]

IT systems perform automated controls using system configurations that apply business logic to data - i.e. logic that governs data input, processing and output. These configurations may be programmed into any of the 'layers of technology' that comprise IT system - e.g. applications, databases.

[How are automated controls configured in vendor-purchased software?](#) [ISA | 1345.12145]

Automated controls in software developed by and purchased from vendors can be configured by changing various settings in the IT systems ("configured automated controls").

[How are automated controls configured in custom-developed software?](#) [ISA | 1345.12146]

Automated controls in custom-developed software can be configured by either changing the IT system's source code ("coded automated controls") or by changing settings that have been coded into the IT system ("configured automated controls").

[How do we determine whether the nature of the control activity is more suitable than another in addressing a PRP or RAFIT?](#) [ISA | 1345.1600]

The table below sets out examples of factors to consider in determining the suitability of controls.

Nature of control activity	Factors to consider
Manual controls	<p>Manual controls may be more suitable where judgment and discretion are necessary, including controls related to:</p> <ul style="list-style-type: none"> • large, unusual or non-recurring transactions; • circumstances where errors are difficult to define, anticipate or predict; • changing circumstances where a control response outside the scope of an existing automated control is necessary; and • monitoring the effectiveness of automated controls. <p>Manual controls may be less suitable for:</p> <ul style="list-style-type: none"> • high-volume or recurring transactions and situations that can be anticipated or predicted and prevented, or detected and corrected, by automated controls; and • activities that can be adequately designed for automated performance.

<p>Automated controls</p>	<p>Automated controls may include activities such as:</p> <ul style="list-style-type: none"> • calculations; • posting to accounts (e.g., the system configured so that certain transactions can only be posted to predefined accounts); • configuration of system-generated reports; and • edit and control routines performed within applications. <p>Automated controls continue to execute a given control (e.g. extending prices on invoices, performing edit checks) in exactly the same way until:</p> <ul style="list-style-type: none"> • the program logic (including the tables, files or other permanent data used by the control) is changed; or • the automated control is otherwise overridden.
----------------------------------	--

[Are there any additional risks for manual controls?](#) [ISA | 1345.1700]

Manual controls may be less reliable than automated controls because they can be more easily bypassed, ignored or overridden. They are also more prone to simple errors and mistakes.

We cannot assume that a manual control will be applied consistently each and every time it is performed.

[Can a manual control have an automated component?](#) [ISA | 1345.1800]

No. Manual controls often rely on or use the output of another automated control. While these activities might seem to be only one control, two distinct controls are working together to address the objective of the control.

When this occurs, we identify two different controls and evaluate them separately.

[What are the different types of control activities?](#) [ISA | 1345.1900]

Control activities are either preventive or detective. It is important for entities to have controls of both types.

[What are preventive control activities?](#) [ISA | 1345.12147]

Preventive control activities are proactive. They help reduce the risk of errors or fraud before they occur.

For example, when we lock the door to our house, we are operating a preventive control.

[What are detective control activities?](#) [ISA | 1345.12148]

Detective control activities identify errors or fraud after they have occurred.

For example, a security alarm helps us identify when someone enters our house inappropriately. Without the alarm, we would be unable to tell if someone has bypassed our preventive control (the door lock) and entered our house.

[What are the different categories of automated process control activities?](#) [ISA | 1345.1930]

The following are the different categories of common automated process control activities we may identify and example controls for each category:

Automated process control activity category	Example controls
System access controls, including enforcing segregation of duties	<ul style="list-style-type: none"> Access to change credit limits in the IT system is restricted only to those in the credit department and those in the credit department do not have access to create a sales order or ship confirm an order. Access to approve claim payments between \$10K and \$25K is restricted to the Claims Payment Supervisor. Access to open and close periods within the general ledger IT system is restricted to the Finance System admin group.
System configuration controls	<ul style="list-style-type: none"> The system is configured to approve invoices that match the purchase order and goods shipped. Unmatched invoices are flagged for resolution (3-way match control). The system is configured to apply customer payments to the appropriate customer account The system is configured to completely and accurately calculate interest credited based on policy plan codes. The system is configured to prevent unbalanced journal entries. The system is configured to validate premium codes assigned to policies based on the policy type. The system is configured to completely and accurately assign accounts receivable transactions to an aging bucket based on the invoice due date. The system is configured to completely and accurately report purchase orders that were pended as a result of a customer exceeding their credit limit. The system is configured to completely and accurately accumulate and report transactions based on product type.
Interface controls	<ul style="list-style-type: none"> The system is configured to produce an error when the number of records processed does not agree to the number of records recorded in the interface file header record. The system is configured to completely and accurately add general ledger account codes to transactions based on interface mapping rules.

	<ul style="list-style-type: none"> The system is configured to produce an error log of interfaced transactions that could not be processed due to missing data elements.
Other	<ul style="list-style-type: none"> There are many types of automated controls, and not all of them fall in these categories. Any automated control that addresses a PRP may be added and categorized as 'Other.'

What are the different categories of automated general IT controls? [ISA | 1345.6300]

The following are the different categories of common automated general IT controls (GITCs) we may identify and example controls for each category:

Automated General IT Control Category	Example controls
System access controls	<p>Access to update workflow configurations in the ticketing system is restricted to the IT support team.</p> <p>Access to migrate changes to the production environment is restricted to authorized production support personnel and segregated from personnel responsible for system development activities.</p> <p>Access to add or update approval configurations in the identity access management system is restricted to the IT security management team.</p> <p>Accounts with privileged access rights, including super-user administrative and system accounts, is restricted to authorized personnel commensurate with job responsibilities.</p> <p>Access to make changes to system jobs is restricted to authorized personnel in IT operations.</p>
System configuration controls	<p>The identity access management system routes access requests to the appropriate approver based on the type of access being requested.</p> <p>The ticketing system routes change requests to the appropriate system business owner and IT owner for approval to implement the change after all required testing signoffs have been obtained.</p> <p>Changes are automatically deployed by the change deployment application after all required approvals have been logged into the application.</p> <p>Dual authentication is enforced for users attempting to access operating system administrator functions.</p> <p>Application password configurations enforce the following password rules: 1) minimum of eight characters, 2) complexity to include at least</p>

	one number and one special character, 3) change every 90 days, and 4) history of 10 previous passwords.
Interface controls	On a nightly basis, the active directory automated termination interface program is configured to check that all terminated employees' status information in the human resource system has been completely and accurately transferred to the active directory employee status database.
Other	There are many types of automated controls, and not all of them fall in these categories. Any automated GITC that addresses a RAFIT may be added and categorized as 'Other.'

What are process control activities over the safeguarding of assets? [ISA | 1345.2000]

Process control activities over the safeguarding of assets are controls that management puts in place to prevent or detect the unauthorized acquisition, use or disposition of assets that could result in a material misstatement to the financial statements.

When we identify process risk points related to such unauthorized activity, we identify the controls that mitigate those process risk points.

Examples of common safeguarding controls include:

- segregating duties;
- periodically comparing the results of cash, security and inventory counts with accounting records;
- enforcing appropriate management approval before an employee enters into a contract that binds the entity to certain obligations; and
- enforcing appropriate authorization for access to computer programs and data files.
- safeguarding controls do not physically protect assets or prevent bad business decisions. Their objective is to mitigate associated risks of material misstatement.

For example, suppose an entity identifies process risk points related to the unauthorized disposition - i.e. theft - of inventory.

Security measures in place to prevent theft include locks on the warehouse and cameras to monitor the inventory.

These types of security measures are advisable, but they are generally outside the scope of Internal Control over Financial Reporting (ICFR).

From an ICFR perspective, relevant safeguarding controls over the risk of theft include:

- timely inventory counts and reconciling the reported inventory balance to the inventory counts; and
- a control to determine that material losses are appropriately *disclosed* in the financial statements, where required (even when the losses are appropriately *recorded* in the financial statements).

What additional procedures do we perform when a control is manual? [ISA | 1345.2100]

When a control is manual, we also seek to:

- understand the frequency of the manual control; and
- understand the authority and competence of the control operator.

What additional procedures do we perform when a control is automated? [ISA | 1345.8883]

When a control is automated, we identify relevant layers of technology, relevant RAFITs and evaluate the design and implementation of GITCs that address those relevant RAFITs. We may document this either:

- for each automated control that we evaluate the design and implementation of, or
- as part of our understanding of IT, when we do not plan to rely on any automated controls, and GITC are a) informal and, therefore, unable to be evaluated for design and implementation, or b) expected to be ineffective (i.e., resulting in a control deficiency).

Do we evaluate automated process control activities before general IT controls? [ISA | 1345.2300]

We order our tests of automated process control activities and general IT controls depending on which controls we determine may be ineffective. It is advantageous to evaluate the controls that are most likely to fail first. This helps to avoid wasting time testing controls that we may be unable to rely on.

For example, when we find that general IT controls are ineffective and they therefore do not support the continued operation of the automated process control activities, we may test other controls that do not rely on the deficient general IT controls. Testing automated process control activities that are affected by the general IT control deficiency is unnecessary.

Conversely, when we find automated process control activities are ineffective, testing general IT controls that support only those ineffective automated controls is also unnecessary.

1.3.4 Understand the frequency of manual controls

[ISA | 1346]

What do we do?

IF the nature of the control is manual THEN obtain an understanding of the frequency of the manual control.

Why do we do this?

When we evaluate whether a control is appropriately designed, we consider how often the control occurs.

Understanding the frequency of performance helps us determine whether the control is designed to achieve its objective in a timely manner. Additionally, the frequency of performance and the level of precision are related for process control activities.

- Precision of a process control activity is increased when it is performed more frequently.
- When a process control activity is not performed frequently enough to prevent, or detect and correct, material misstatements, we cannot conclude that it has been appropriately designed.

Execute the Audit

What is the frequency of a control? [ISA | 1346.1300]

Frequency relates to how often the control is performed. For example, a control could be performed:

- annually;
- quarterly;
- monthly;
- weekly;
- daily;
- recurring (e.g. performed multiple times per day);
- ad-hoc (e.g. when a certain type of transaction or activity occurs); or
- continuously (e.g. automated control activities).

Annual, quarterly, monthly, weekly, and daily controls are referred to as 'periodic controls'.

How do we determine the frequency of a manual control for the purpose of determining the sample size? [ISA | 1346.12158]

We determine the frequency of a manual control by considering its actual frequency and thinking about the number of times the control operation occurs (number of occurrences).

Where a periodic (not recurring) manual control has multiple occurrences, because it operates over parts of accounts/ transactions, we determine the sample size by considering the number of occurrences of the manual control.

For example, we are testing the operating effectiveness of monthly bank reconciliations performed on 100 bank accounts, where RAWTC is Base:

- Our control frequency is 12 months x 100 accounts = 1,200 occurrences in the period. The occurrence is akin to recurring per the table below.
- We consider this equivalent frequency and the RAWTC of Base and refer to the control sample size table to determine a sample size of 25.
- We select these 25 items from multiple points in the year and not just 1 month.

If the frequency or occurrence of a manual control sits between categories, we use the higher of the categories when determining our control sample size.

For example, we are testing the operating effectiveness of monthly bank reconciliations performed on 12 bank accounts, where RAWTC is Base:

- Our control frequency is 12 months x 12 accounts = 144 occurrences in the period. Therefore, occurrence is somewhere between weekly and daily.
- We refer to the table below and determine the equivalent frequency for this control to be daily. Based on the control sample size table, we select a sample of 15 items.

For example, if a manual control is performed twice a week and therefore occurs 104 times in the period, the frequency is somewhere between weekly and daily. We refer to the table below and determine the equivalent frequency to be daily. As the control's RAWTC is Base, we refer to the control sample size table and select a sample of 15 items.

Therefore, when a manual control, including an ad-hoc control, has a number of occurrences that it operates in the period we think about the following in determining the appropriate sample size:

Number of occurrences	Equates to the following frequency only when determining the sample size
1	Annual
2-4	Quarterly
5-12	Monthly
13-52	Weekly
53-366	Daily
>366	Recurring

How do we determine the frequency of a manual control for the purpose of determining the sample size where an entity uses an annual calendar structure with 13 periods or 53 weeks and has controls that operate each period or week? [ISA | 1346.158376]

When an entity uses a 13-period annual calendar (13 periods in a 12-month year) and has a control that operates each period (13 occurrences), we may treat the control as having a monthly control frequency despite it occurring more than 12 times. Similarly, when an entity has an annual period that includes 53 weeks, we may treat a control that operates each week as having a weekly control frequency despite it occurring more than 52 times.

For example, a retail entity may divide an annual period into 13 periods shorter than calendar months. If RAWTC is Significant, our control sample size for the monthly periodic control (13 occurrences) is 3.

Can a control be performed on an ad-hoc basis? [ISA | 1346.1400]

Yes. A control may occur only when a certain type of transaction or activity occurs (including when a control deficiency is identified).

For example, if system access is given to an employee not suitable for their role (inappropriate access determined to be the result of a control deficiency), then management may implement an ad-hoc GITC to determine whether the employee used that inappropriate access.

What sample size do we use to test the operating effectiveness of manual ad-hoc controls? [ISA | 1346.158377]

We determine the number of occurrences of the control in the period and determine the equivalent frequency of the control in accordance with the table in question '[How do we determine the frequency of a manual control for the purpose of determining the sample size?](#)'. We then refer to the control sample size table to determine the sample size to be used in testing the control.

What if we are evaluating the design and implementation of an ad-hoc control that relies on another control? [ISA | 1346.8466]

When we evaluate the design and implementation of an ad-hoc control and the design of the ad-hoc control relies on another control, such that the ad-hoc control would not operate effectively if the other control was ineffective, then we evaluate the design and implementation of both controls.

Fact pattern

An entity prepares a technical accounting memorandum for each significant unusual transaction that is entered into during the period. The memorandum summarizes the details of the:

- transaction (i.e. the nature, terms and business purpose of the transaction);
- involvement of related parties in the transaction (if any);
- entity's accounting for the transaction; and
- disclosures related to the transaction in the entity's financial statements.

The Chief Financial Officer (CFO) reviews the technical accounting memorandum to determine the accuracy of the transaction's details and the appropriateness of the accounting for and disclosure of the transaction in the entity's financial statements. The process control activity only occurs when a significant unusual transaction occurs during the period.

The entity also has other process control activities in place to identify significant unusual transactions entered into during the period. These include a review of board minutes and a listing of contracts the entity has entered into during the period by the entity's controller.

Analysis

In this case, we evaluate the design and implementation of both process control activities - i.e. the process control activities that identify when a significant unusual transaction occurs and that it has been appropriately accounted for and disclosed.

What's the relationship between frequency and achieving the control objective? [ISA | 1346.1500]

We consider the frequency of a control's performance in relation to the control objective. The precision of a process control activity is increased when it is performed more frequently.

When we evaluate whether a control is appropriately designed, we ask: 'Does the control operate at a frequency that would achieve its objective (e.g. to prevent or detect a material misstatement in the case of a process control activity) in a timely manner?'

For example, suppose an entity has a control to detect improper access to a folder with confidential information that supports the financial statements but the control only operates annually. The frequency of the control may not be sufficient to meet the control objective as it may not detect the improper access in a timely manner to prevent the potential manipulation of the information and a misstatement in the financial statements.

1.3.5 Understand the authority and competence of the manual control operator [ISA | 1347]

What do we do?

IF a control is a manual control, THEN obtain audit evidence about whether the person performing the control possesses the necessary authority and competence to perform the control effectively.

Why do we do this?

Manual controls rely on the control operator to have sufficient levels of *both* authority and competence. These two qualities work together and controls are designed effectively when they are both present. More authority doesn't compensate for a lack of competence, and vice versa.

Even when controls are designed to effectively (e.g. to prevent or detect errors or fraud that could result in a material misstatement in the case of a process control activity), if the control operator does not have *both* the necessary authority and competence, the control cannot be designed effectively and we do not place reliance on it.

Execute the Audit

What is a control operator? [ISA | 1347.8445]

The control operator is a term used to describe who or what performs the control. In a manual control, the control operator is the individual who performs the control. In an automated control, the control operator is the IT system.

What is authority? [ISA | 1347.1300]

The Merriam-Webster dictionary defines 'authority' as "power to influence or command thought, opinion, or behavior."

A person may perform the control effectively. But when they do not have the *authority* within the organization to enforce the control's results, the control cannot achieve its objective.

How do we assess authority? [ISA | 1347.1400]

We assess the authority of the control operator by obtaining an understanding of the organizational structure. The control operator must have the ability to sufficiently challenge process owners in a way that would influence their behavior.

Fact pattern

Accounting Associate A reviews and authorizes all journal entries posted each month. Certain journal entries are posted by the associate's supervisor and other supervisors.

Analysis

Based on the entity's structure, Accounting Associate A does not have the right level of authority to sufficiently challenge the legitimacy of a journal entry - i.e. they wouldn't be able to challenge a supervisor about a questionable journal entry that the supervisor posted.

The control operator doesn't have the right level of authority, so the team concludes that the control is not designed effectively to address the process risk point.

What is competence? [ISA | 1347.1500]

Competence relates to the abilities, knowledge or skills that enable a person to effectively perform their job responsibilities. The competence of a person performing a control may either support or limit the control's effectiveness.

When a control operator does not have the necessary abilities, knowledge or skills to perform the control the way it was designed, it may not be able to achieve its objective.

How do we assess competence? [ISA | 1347.1600]

We assess the competence of the control operator by obtaining an understanding of the individual's education and experience with the subject matter. We consider a variety of sources, including:

- educational level;
- our experience with the control operator's work (i.e. review of any deficiencies or misstatements in prior periods);
- qualifications, licensing, membership in a professional body and other forms of external recognition;
- relevance of the control operator's capabilities to the control's subject matter; and
- circumstances that may threaten the control operator's objectivity.

Fact pattern

An engagement team notes that the director of accounting is responsible for reviewing certain components of the entity's income tax provision, such as the valuation allowance analysis. The director of accounting is a licensed accountant.

The director of accounting oversees the tax department, which prepares the entity's income tax provision. The director of accounting has little training on how to determine whether a valuation allowance is necessary (or whether recognizing a deferred tax asset is appropriate) and no experience in accounting for income taxes.

Analysis

The team concludes that the director of accounting does not have the competence to perform an effective review and the control is not designed effectively.

How do we assess authority and competence when there are multiple control operators? [ISA | 1347.12156]

When there are multiple control operators (e.g., a homogeneous control performed in multiple locations), we assess whether all the control operators have the necessary authority and competence to perform the control effectively. This may entail either assessing the authority and competence of all control operators individually or the applicable role(s) in the entity's organization that is assigned to perform the control.

How do we evaluate the authority and competence of the control operator of a control activity involving judgment? [ISA | 1347.1800]

As the level of judgment and complexity increases in the manual control activity, the level of authority and competence necessary from the control operator (i.e. the control operator's knowledge, skills and experience) also increases.

We think about whether the control operator is different from the process owner-this is something that we do for all control activities, but often in complex processes or estimates, the line between a process owner and a control operator may become "blurred".

[Can management use a third party as a control operator?](#) [ISA | 1347.1900]

Yes. In some cases, management may use a third party to assist with financial reporting functions, including performing controls. For example, a smaller entity with limited accounting and financial reporting personnel may engage an external party to operate a control. However, management maintains responsibility for appropriate oversight.

[How do we assess competence when management used a third party?](#) [ISA | 1347.2000]

We assess the competence of third parties used by management in the same way we evaluate control operators. We consider the combined competence of entity personnel and third parties.

Management may use third parties when the entity does not have available internal resources or the technical expertise to effectively execute controls over a particular area of accounting or financial reporting - e.g. complex tax transactions, derivative accounting. When management, combined with a hired third party, have the necessary abilities, knowledge or skills to perform the control, we may conclude that they are competent.

However, management retains responsibility for:

- supervising the third party; and
- understanding and evaluating the third party's work in operating the control.

When an external third party provides inaccurate information or reaches an incorrect conclusion, management is still responsible for internal controls and accurate financial reporting - i.e. for identifying material misstatements in the work performed by the third party.

If management uses a specialist to operate a control, we assess whether they are competent by considering our procedures to:

- assess the knowledge, skill, ability and relationship of the management's specialist; and
- evaluate the work of a management's specialist.

Refer to activity '[Perform specific procedures when using the work of a management's specialist](#)' for further guidance.

[Do we assess authority and competence for manual general IT controls?](#) [ISA | 1347.2100]

Yes. When a general IT control is manual, we assess the authority and competence of the control operator.

For example, suppose an entity has a monitoring control over the periodic review of access rights. We assess whether the person performing the control has:

- knowledge of who should and should not have access rights; and

- the authority to restrict or grant access rights.

1.3.6 Understand if judgment is involved in the control activity [ISA | 1348]

What do we do?

Determine if judgment is involved in the operation of the control activity

Why do we do this?

Controls involving judgment are often implemented in complex areas that have the potential for a higher risk of material misstatement, which increases the persuasiveness of the evidence we obtain to determine that the control is designed and operating effectively. Obtaining sufficient appropriate audit evidence about the design and operating effectiveness of these controls is more difficult than for other controls.

Execute the Audit

How do we determine if a control activity involves judgment? [ISA | 1348.1301]

A control activity involves judgment if there is judgment or subjectivity in:

- applying the criteria for investigation to identify outliers, and/or
- determining whether the outlier subject to investigation/resolution is correct/reasonable,

for any individual control attribute.

In many cases, when there is judgment in the underlying accounting for the transaction, there is likely to be judgment involved in the control activity.

In a control that compares recorded amounts with expectations, the control operator uses judgment in setting the criteria for investigation to identify outliers, which we consider when we evaluate the precision of the control. But there is also judgment in determining whether outliers constitute errors because outliers may or may not result in errors. Therefore, this control involves judgment.

In an automated three-way match control, there is no judgment in determining whether the items match. The fact that there may be a threshold (e.g., any transaction where the three documents do not match within \$100 is not processed) creates a question about whether that threshold is sufficiently precise, but it does not introduce judgment into the control. Therefore, this automated control does not involve judgment. In a separate manual control, a control operator reviews the report and uses judgment to determine whether the items over \$100 are errors. This separate manual control involves judgment.

What is criteria for investigation? [ISA | 1348.8447]

Criteria for investigation is the threshold or criteria used in the operation of the control to identify outliers for further investigation and/or resolution.

For some controls, there may be no threshold or criteria applied such that any difference is identified, investigated and resolved.

For other controls, there may be a pre-defined quantitative threshold, a variable quantitative threshold, or qualitative criteria such that some differences but not all differences are identified as outliers.

[What is an outlier?](#) [ISA | 1348.1300]

An 'outlier' is an item that meets the criteria for investigation established in the control's design for which further investigation and resolution either as part of the control or as a separate control is necessary.

An outlier may occur frequently or infrequently, depending on the nature of the control.

[Do all control activities involve judgment?](#) [ISA | 1348.1400]

No. Many controls activities involve objective comparisons of information - e.g. data within a three-way match control either agrees or it does not. Other control activities involve the control operator making decisions when applying the criteria for investigation to identify outliers or to determine how to resolve an outlier.

Some control activities can include some control attributes that involve no judgment and others that do involve judgment.

For example, a fixed asset reconciliation control has the following control attributes:

- *Control attribute #1:* Control operator agrees the fixed asset subledger report to the fixed asset reconciliation.
- *Control attribute #2:* Control operator agrees the fixed asset general ledger amount to the fixed asset reconciliation.
- *Control attribute #3:* Control operator investigates reconciling items above \$10,000 (i.e., outliers), investigates by inspecting the supporting documentation and makes a decision as to whether the reconciling item is indicative of an error in the account balance. Resolution is based on the control operator's discretion and so this control attribute involves judgment.

In determining whether a control activity has judgment, it is helpful to think about whether:

- a simple automated control could perform the control attribute (unlikely to involve judgment); or
- a person thinks and makes decisions in performing the control attribute (likely to involve judgment).

[Can general IT controls involve judgment?](#) [ISA | 1348.8449]

Yes. However, although many general IT controls (GITCs) do not involve judgment, for those that do, the control operator investigates all identified outliers. One example of a GITC that involves judgment is management's periodic review of user access to the IT system, where any difference from standard access rights for a role is treated as an outlier and investigated.

For example, the entity has a GITC where business/functional managers quarterly review user access of their direct reports to determine whether user access is appropriately restricted, which has the following control attributes:

- *Control attribute #1:* User access reviews across relevant IT systems are enforced in accordance with the defined frequency of the review as per the entity's policy.
- *Control attribute #2:* Business unit/team managers commensurate with the entity's IT delegation of authority perform user access reviews for their team members across the relevant IT systems and they investigate all instances where, according to the entity's policies, a user has access that is unauthorized or not commensurate with job responsibilities. If access is considered to be inappropriate, it is communicated to the team that modifies user access.

In control attribute #2, resolution is based on the business unit/team manager's discretion and so this control attribute involves judgment.

[What is different about evaluating the design of judgmental control activity?](#) [ISA | 1348.1600]

When we evaluate the design of a control activity that involves judgment, we obtain more persuasive evidence than we do for controls involving no judgment, especially relating to understanding any judgmental criteria applied by the control operator for identifying and investigating outliers.

Not only does this call for additional attention to understand the criteria for investigation, we pay attention to the consistent application of judgmental criteria through the tests of implementation and operating effectiveness.

[What is different about evaluating the implementation of a judgmental control activity?](#) [ISA | 1348.1700]

When evaluating the implementation of a control activity that has judgment, we expand on our evaluation of the control activity to include:

- evaluating the steps performed by the control operator to identify and investigate outliers, including whether outliers were or would be appropriately identified; and
- evaluating the conclusions reached in the control operator's investigation, including whether all outliers were appropriately investigated and whether corrective actions were taken as needed.

[How do we evaluate the control operator's steps to identify and investigate outliers?](#) [ISA | 1348.12164]

We put ourselves in the role of the control operator and assess whether the steps performed align with our understanding obtained through our evaluation of the design of the control activity. At the same time, because the control activity involves judgment, we also assess whether the control operator's steps are capable of identifying outliers that individually or in the aggregate may lead to material misstatement (directly or indirectly).

As a result of our evaluation, we may identify:

- *design deficiencies:* the control as designed is not capable of identifying all outliers that individually or in the aggregate may lead to material misstatement (directly or indirectly); or
- *implementation deficiencies:* the control operator did not perform the control as designed to identify all outliers.

1.3.7 Understand the level of precision of the process control activity and evaluate the factors affecting the level of precision [ISA | 1349]

What do we do?

Obtain an understanding of the precision of the process control activity by evaluating how each applicable factor affects the level of precision.

Obtain an understanding of the precision of the process control activity and, for controls that involve judgment, evaluate how each applicable factor affects the level of precision.

Why do we do this?

Understanding the precision of a process control activity helps us understand whether the control is designed to meet its objective - i.e. whether the control operates with sufficient precision to prevent, or detect and correct, a material misstatement in a timely manner over the financial statement assertions it is intended to address.

Understanding a control's precision therefore helps us understand the maximum size of misstatement that the control is designed to permit.

When a control:

- is not designed to operate with sufficient precision; or
- does not operate effectively with sufficient precision,

then it does not provide sufficient appropriate evidence to address the relevant process risk points (PRPs).

Execute the Audit

What is the level of precision? [ISA | 1349.1301]

The precision of a process control activity is essentially the size of a potential misstatement the control would prevent, or detect and correct, when it operates effectively.

So, a control's precision is the maximum size of a misstatement that could be accepted based on the control's design and operation.

What is a 'would' level of assurance? [ISA | 1349.12086]

When we consider a control's precision, we evaluate whether the control is designed to operate at a 'would' level.

We have coined the phrase 'would-level control' because the standards require reasonable assurance that a control would prevent, or detect and correct, a material misstatement in a timely manner. In this context, 'would' means 'probable'.

For a control to function properly as a process control activity, it needs to operate in a manner that allows us to confidently say it would - i.e. probably will - prevent or detect and correct a material misstatement.

When we consider whether a control is precise enough, we place ourselves in the role of the control operator and determine whether:

- the control's design considers the appropriate control characteristics and objectives; and
- the criteria for investigation are set at a level that would prevent, or detect and correct, a material misstatement every time the control operates

[What factors affect the level of precision?](#) [ISA | 1349.1501]

Several factors affect a control's level of precision. A well-designed control takes into account each of the below factors regarding its precision level. Example circumstances that indicates higher or lower precision levels are listed alongside each of the factors:

Precision factors:	Higher precision	Lower precision
Level of aggregation	Control operates over individual transactions (i.e. no aggregation)	Control operates over balances or accounts (i.e. an aggregated level)
Consistency of performance	Control operates on a consistent basis with a predefined frequency (e.g. daily or multiple times a day)	Control does not operate consistently or operates without a predefined frequency (e.g. ad hoc)
Predictability of expectations	When the control involves developing expectations about reported amounts, there are key performance indicators or other information that indicate a strong relationship allowing management to develop more precise expectations	When the control involves developing expectations about reported amounts, key performance indicators or other information either do not exist or do not have a strong relationship and thus, do not allow management to develop precise expectations
Criteria for investigation	No threshold is applied, such that all differences are identified and investigated (i.e. all differences are considered outliers)	Thresholds are applied, such that not all differences are identified or investigated (i.e. not all differences are considered outliers). The total number of occurrences of the control is uncertain, which results in

	uncertainty in whether the threshold is appropriate.
--	--

What is criteria for investigation? [ISA | 1349.8447]

Criteria for investigation is the threshold or criteria used in the operation of the control to identify outliers for further investigation and/or resolution.

For some controls, there may be no threshold or criteria applied such that any difference is identified, investigated and resolved.

For other controls, there may be a pre-defined quantitative threshold, a variable quantitative threshold, or qualitative criteria such that some differences but not all differences are identified as outliers.

What is an outlier? [ISA | 1349.1300]

An 'outlier' is an item that meets the criteria for investigation established in the control's design for which further investigation and resolution either as part of the control or as a separate control is necessary.

An outlier may occur frequently or infrequently, depending on the nature of the control.

Enhanced | How do we understand and evaluate the level of precision of a process control activity?

[ISA | 1349.12088]

We obtain an understanding of the factors listed above and for each applicable factor evaluate how it is affecting the level of precision of the process control activity (e.g., higher or lower precision).

What is the difference in evaluating the precision of an automated process control activity? [ISA | 1349.12089]

We evaluate three factors for automated process control activities as the 'predictability of expectations' factor is not applicable as automated controls do not involve developing expectations.

Additionally, the 'consistency of performance' factor is indicative of higher precision for automated controls as, by their nature, they are designed to operate on a recurring basis and consistently each time they are performed.

Core and Less Complex | How do we understand and evaluate the level of precision of a process control activity? [ISA | 1349.12088]

We think about the factors listed above in our evaluation of the precision of the control. For process control activities that involve judgment, we evaluate how each applicable factor is affecting the level of precision of the process control activity (i.e. higher or lower precision).

What is the impact of our precision evaluation on our overall evaluation of the process control activity design? [ISA | 1349.12090]

Our evaluation of the precision factors informs our overall evaluation of the process control activity design. The table below sets out example circumstances related to evaluated precision of a process control activity and the effect on our evaluation of the control design.

Example circumstances	Effect on the evaluation of the control design
-----------------------	--

Lower precision control	<p>The control's ability to function at the 'would' level becomes less likely, increasing skepticism about its ability to function at the 'would' level.</p> <p>If not already concluded as a design deficiency, it may be necessary to obtain more persuasive evidence about the control's design and effectiveness.</p>
Inherent imprecision of the estimate exceeds the precision of the control	<p>A control cannot operate more precisely than the inherent imprecision of the estimate. However, well designed controls are not designed to operate less precisely than the inherent imprecision.</p> <p>This may occur for significant accounting estimates - e.g. Allowance for credit loss for banks, insurance reserves, goodwill impairment, business valuations, legal contingencies, warranty reserves.</p> <p>It may be necessary to identify additional controls to appropriately address the estimate's RMM. For example, we may include controls that address the risk of management bias, such as controls over:</p> <ul style="list-style-type: none"> • consistent application of the methodology used to determine the estimate; and • the estimate's placement within a range of reasonable results.
Risk of bias related to precision	<p>For controls that have judgment, we remain alert to the risk of bias in the design (including precision) and execution of the controls.</p> <p>This risk increases for controls where the inherent uncertainty of the estimate exceeds the established risk tolerance. It may be necessary to identify separate controls to address the risk of bias in estimates.</p>

Can the criteria for investigation change over time? [ISA | 1349.1500]

Yes. The control operator may need to set dynamic criteria for investigation for a control to operate at the 'would' level of assurance.

Adjustments to the criteria may be in response to changes in external and internal factors - e.g. the nature or subject matter of the review control.

How might management determine when it is necessary to adjust the criteria for investigation? [ISA | 1349.12096]

Management may identify necessary adjustments to the criteria for investigation through controls that consider the continuing appropriateness of the criteria to identify outliers, particularly those control activities that involve judgment. These controls may operate as part of the control itself (i.e., a control attribute) or as a separate control.

Control activities that do not involve judgment may be re-evaluated when the nature of transactions change. Control activities involving judgment may be re-evaluated periodically regarding of the degree of uncertainty inherent in the control's subject matter, especially for significant accounting estimates.

When the number of outliers identified by a control activity changes from period to period, it may indicate that it is necessary to adjust the control's design.

Example

Enhanced | How do we evaluate a process control activity's precision? [ISA | 1349.2000]

Fact pattern 1

An entity's enterprise resource planning (ERP) IT system performs an automated three-way match control as part of the purchasing process. The control identifies differences between:

- the vendor invoice;
- the related purchase order; and
- the receiving documentation.

At the end of each day, an accountant in the accounts payable department generates a system report showing all differences on the purchase transactions processed that day.

In a separate manual control activity, a control operator reviews the report daily and investigates any difference over \$10.

Analysis 1

Precision factors:	Automated control evaluation	Manual control evaluation
Level of aggregation	The controls operate with no aggregation, such as the individual transaction or item level, which indicates higher precision.	
Consistency of performance	The control is designed to operate consistently each time it is performed and at a predefined frequency, which indicates high precision.	The steps performed by the control operator to investigate the outliers, while somewhat dependent on the facts of the outlier, is still fairly consistent, which

		<p>is to contact the sources of the supporting documents (i.e. vendor, receiving department, and purchaser) to confirm the accuracy of the documents. These steps generally identify the root cause of the differences and the control operator is able to obtain updated documentation to resolve the outlier.</p> <p>The control is designed to operate consistently each time it is performed and at a pre-defined frequency, which indicates high precision.</p>
Predictability of expectations	As the automated control does not involve developing expectations, this factor is not applicable to our precision evaluation.	The control attributes do not involve developing expectations. Accordingly, this factor is not applicable.
Criteria for investigation	The system generated report includes all differences in the purchase transactions processed. The criteria for investigation in the automated control has no threshold for investigation. As such, any differences are considered outliers, which indicates higher precision. Refer to separate manual control for assessment of the pre-defined threshold applied to the report.	The control attributes involve a pre-defined quantitative threshold to identify outliers for investigation and resolution. \$10 is the threshold for investigation. Management determined this threshold to be appropriate based on the volume of purchasing transactions entered on an annual basis (approximately 110,000). We determined that even if 100% of the transactions were inaccurately recorded in the financial statements by \$9, the aggregate impact

		to the financial statements would be less than \$1M,. Based on performance materiality, the engagement team deems the criteria for investigation set for this control indicates higher precision.
--	--	---

Fact pattern 2

A bank reconciliation is prepared for each bank account monthly and reviewed by the assistant controller. The assistant controller performs their review by:

- Agreeing the bank balance to the bank statement
- Agreeing the general ledger balance to the general ledger
- Reviewing supporting documentation for reconciling items greater than \$10,000

Analysis 2

Precision factors:	Evaluation
Level of aggregation	The reconciliation is performed at the bank account level but involves a reconciliation of the complete population of transactions during the period, which indicates higher precision.
Consistency of performance	The control is designed to operate consistently each time it is performed and at a predefined monthly frequency, which indicates higher precision. The steps performed by the control operator to investigate the outliers, while somewhat dependent on the facts of the reconciling item, are still fairly consistent, which is to review the supporting documents and evaluate whether the reconciling item is indicative of an error in the account balance and has been appropriately resolved.
Predictability of expectations	The control attributes do not involve developing expectations. Accordingly, this factor is not applicable.
Criteria for investigation	The control attributes involve a pre-defined quantitative threshold over which outliers are investigated and resolved.

	<p>\$10,000 is the threshold for investigation. Management determined this threshold to be appropriate.</p> <p>Based on the performance materiality set by the engagement team, and considering other relevant factors, including:</p> <ul style="list-style-type: none"> • average bank balance compared to the threshold • the number of bank accounts • the number of misstatements historically detected, <p>the engagement team concurs with management's assessment that the criteria for investigation set for this control results in sufficient precision to detect and correct material misstatement.</p>
--	--

What do we think about when evaluating precision? [ISA | 1349.1800]

Fact pattern 1

Evaluation	
Example consideration	Whether the criteria for investigation are appropriate to address the control objective
Objective of the control (PRP)	Depreciation expense is recorded completely and accurately
Control description	A control is designed to compare periodic income statement balances including depreciation expense and review fluctuations greater than \$100,000,
Evaluation of the design	<p>The criteria for investigation may help to assess consistency between periods but it would not be effective at detecting situations where depreciation should have fluctuated but did not (e.g., new additions to fixed assets, changes in useful lives, significant dispositions, etc.).</p> <p>The control would not be effectively designed on its own to address the PRP.</p>

Fact pattern #2

Evaluation	
Example consideration	Whether the criteria for investigation to identify and investigate outliers is appropriate to address the control objective
Objective of the control (PRP)	Allowance for doubtful accounts receivable is valued appropriately
Control description	At each period-end, the control operator reviews customer A/R balances past due for more than 120 days to determine whether a reserve should be recorded.
Evaluation of the design	If the A/R write-off history suggests that receivables past due from 90 days or more are susceptible to write-off, we may determine that the criteria for investigation is not sufficiently precise.

1.3.8 Understand the steps taken to identify, investigate and resolve outliers, if applicable [ISA | 1350]

What do we do?

IF the control activity involves judgment, THEN obtain an understanding of the steps performed by the control operator to identify, investigate and resolve outliers.

Why do we do this?

When a control activity includes attributes that involve judgment, we understand how the control operator identifies, investigates, and resolves outliers to appropriately evaluate the control activity.

Execute the Audit

What is different about evaluating the implementation of a judgmental control activity? [ISA | 1350.1700]

When evaluating the implementation of a control activity that has judgment, we expand on our evaluation of the control activity to include:

- evaluating the steps performed by the control operator to identify and investigate outliers, including whether outliers were or would be appropriately identified; and
- evaluating the conclusions reached in the control operator's investigation, including whether all outliers were appropriately investigated and whether corrective actions were taken as needed.

How do we evaluate the control operator's steps to identify and investigate outliers? [ISA | 1350.12164]

We put ourselves in the role of the control operator and assess whether the steps performed align with our understanding obtained through our evaluation of the design of the control activity. At the same time, because the control activity involves judgment, we also assess whether the control operator's steps are capable of identifying outliers that individually or in the aggregate may lead to material misstatement (directly or indirectly).

As a result of our evaluation, we may identify:

- *design deficiencies*: the control as designed is not capable of identifying all outliers that individually or in the aggregate may lead to material misstatement (directly or indirectly); or
- *implementation deficiencies*: the control operator did not perform the control as designed to identify all outliers.

What is criteria for investigation? [ISA | 1350.8447]

Criteria for investigation is the threshold or criteria used in the operation of the control to identify outliers for further investigation and/or resolution.

For some controls, there may be no threshold or criteria applied such that any difference is identified, investigated and resolved.

For other controls, there may be a pre-defined quantitative threshold, a variable quantitative threshold, or qualitative criteria such that some differences but not all differences are identified as outliers.

What is an outlier? [ISA | 1350.1300]

An 'outlier' is an item that meets the criteria for investigation established in the control's design for which further investigation and resolution either as part of the control or as a separate control is necessary.

An outlier may occur frequently or infrequently, depending on the nature of the control.

Is an outlier a misstatement? [ISA | 1350.12091]

Not always. Outliers do not necessarily lead to misstatements. Rather, it triggers the control operator to further investigate in order to:

- confirm the appropriateness of the outlier;
- identify whether or not the outlier:
 - is an error that needs correction; or
 - otherwise indicates that the related account balance contains an error; and
- determine whether further information or activities are needed to resolve the matter.

How do the criteria for investigation affect the level of precision of a process control activity? [ISA | 1350.12092]

The criteria for investigation influences how precisely a process control activity is designed to operate. A control's precision is the magnitude of a potential misstatement that would be prevented, or detected and corrected, based on the control's design and operation.

When an entity has not set objective criteria for investigation, we face challenges in understanding whether the process control activity is designed to consistently operate at an appropriate level of

precision to achieve the control's objective - i.e. operate at the 'would' level. The outliers identified through a process control activity's operation may help us understand or confirm the control's precision and the criteria that the control operator uses to identify items for investigation.

What do we do if no outliers are identified by an entity in a performance of a control activity? [ISA |

1350.12094]

Our evaluation of the design and implementation of a control activity with no outliers identified by the control operator will depend on whether we are able to conclude that:

- the control activity is designed effectively with sufficient precision to:
 - directly prevent, or detect and correct material misstatement in a timely manner over the financial statement assertions it is intended to address (process control activities); or
 - address the relevant RAFIT (GITCs); and
- in the time period subject to the control activity, no outliers would have been identified.

Otherwise, the control activity is deemed to be ineffectively designed and/or implemented.

1.3.9 Understand information relied on in the performance of the control activity [ISA | 1351]

What do we do?

IF information is used by the control operator to perform the control activity, THEN evaluate the relevance AND reliability of that information.

Why do we do this?

Control activities often use multiple sources of information to achieve their desired objective. Some of this information is the subject of the control activity itself, and some is relied on by the entity to perform the control activity.

When a control activity relies on information not subject to one or more of the control's attributes, we evaluate the relevance and reliability of that information because it is important to the design and effective operation of the control (i.e., its ability to achieve the desired objective).

Execute the Audit

When does a control activity rely on the relevance and reliability of information to achieve its objective?

[ISA | 1351.1300]

A control relies on the relevance and reliability of information when information is used by the control operator as part of the control activity in order to achieve its objective - e.g. to address the process risk points (PRPs).

For example, suppose a control operator uses an exception report to identify and investigate instances where a customer has exceeded their credit limits and to analyze reserves for a specific customer (the control activity).

The control operator relies on the exception report in order to achieve the objectives of the control activity.

A control operator does not rely on the relevance and reliability of information when the information is the subject of one or more of the control's attributes.

For example, in order to address the RMM "Cash and cash equivalent balances are not accurately recorded or do not exist", we identify a process control activity where the control operator reconciles the balance of a cash account per the general ledger to the balance of a cash account per the bank statements.

The control operator does not rely on the relevance and reliability of the cash balance per the general ledger, as the cash balance per the general ledger is the subject of the control itself. However, the control operator does rely upon the bank statement, the listing of deposits and wires (receipts) in transit and the listing of checks and wires (disbursements) outstanding when performing the control activity. In other words, the control activity relies on the relevance and reliability of this information to achieve its objectives.

[What types of information can the performance of a control activity rely on?](#) [ISA | 1351.1400]

A control activity can rely on information from:

- reports generated directly from IT systems (i.e. system-generated reports);
- reports generated using report writers that interface with IT systems (i.e. custom reports);
- schedules created using end-user computing applications (i.e. end-user computing schedules); and
- information created by external information sources (e.g. management's experts, information providers).

[What are system-generated reports?](#) [ISA | 1351.1500]

System-generated reports are reports configured directly within an entity's IT systems. These reports may be:

- built into off-the-shelf IT systems from software vendors; or
- custom-created by either the software vendor or management to meet the specific needs of the entity.

[What are custom reports?](#) [ISA | 1351.1600]

Custom reports are reports created and configured by management using a separate report writer application - e.g. reports from a report writer such as Crystal Reports or created by running queries tailored by the end-user using source code.

[What are EUC applications?](#) [ISA | 1351.1700]

EUC (End-user computing) applications are IT systems in which end users, rather than computer programmers, can create working applications. Entities often use end-user computing applications as part of its financial reporting and business processes. Hence, audit evidence may come in the form of

an end-user computing schedule (e.g. spreadsheet software or simple databases). Such schedules are not typically identified as a layer of technology.

[What are EUC schedules?](#) [ISA | 1351.12104]

EUC schedules are schedules created using an EUC application. Examples include:

- spreadsheets (e.g. Microsoft Excel files);
- custom databases (e.g. Microsoft Access files);
- ad hoc queries; and
- stand-alone desktop applications.

[How do we evaluate the relevance of information?](#) [ISA | 1351.12107]

We evaluate whether the information, including each 'relevant data element' (RDE), is sufficiently relevant for the objective of the procedure.

As part of this evaluation, we consider the relationship of the information and RDEs to the objective of the procedure, the design and timing of the procedure and, where applicable, each RMM and significant account / relevant assertion that is being addressed.

Sometimes, the relevance of the information used in our audit is clear from the description of the procedure and the RMM(s) and significant account(s) / relevant assertion(s) that are being addressed. If the relevance of the information would not be clear to an experienced auditor, we specifically document the relevance of the information in these circumstances.

For example, if it is not clear from the description of the procedure, an engagement team documents why information on the disposal of a Level 3 investment on 28-Feb (subsequent to year-end) is used as audit evidence over the fair value of that investment recorded in the financial statements as of 31-Dec.

[How do we evaluate the reliability of information used in control activities?](#) [ISA | 1351.2100]

The table below indicates how we may evaluate the reliability of information used in control activities (including automated process control activities and GITCs) when we are relying on and testing controls as part of our response to an RMM:

If the information is used:	Internal Information	External Information
As the subject of the control activity	Reliability of the information is addressed by testing the control (one or more of the control attributes) itself.	Reliability of the information is addressed by testing the control (one or more of the control attributes) itself.
By the control operator to perform the control activity	Test management's controls over the accuracy and completeness of the information, direct-test the accuracy and completeness	We obtain an understanding of how the control operator is satisfied with the reliability of the information and determine the appropriate

	of the information or use a mixed approach instead.	audit procedures to evaluate the reliability of the information.
Solely by KPMG to select items to test the control activity	Test management's controls over the accuracy and completeness of the information, direct-test the accuracy and completeness of the information or use a mixed approach instead.	N/A - scenario is not expected to arise.

What do we do if management uses system generated reports in its controls but does not rely on automated control activities and GITCs to produce complete and accurate reports ? [ISA | 1351.159419]

In some circumstances, when the volume and complexity of transactions are lower, management may not rely on the automated control activities and GITCs to produce complete and accurate reports. Instead, it may have a manual control activity(ies) that is(are) sufficient to evaluate the accuracy and completeness of the data. For example, the control operator reconciles the reports back to the hard copy documentation and recalculates the mathematical accuracy of the calculations in the reports.

If we have not identified any automated process control activities (or any that depend on GITCs), we may plan to test the manual process control activity(ies).

What does 'validity' mean in the context of information and how does it relate to our risk assessment and our evaluation of the accuracy and completeness of information? [ISA | 1351.8517]

Validity means that recorded transactions represent economic events that actually occurred or were executed according to prescribed procedures. Validity is generally achieved through process control activities that include the authorization of transactions as specified by an entity's established policies and procedures (that is, approval by a person having the authority to do so.)

We obtain an understanding of how transactions are authorized when we obtain our understanding of the flow of transactions within a business process, including the flow of information. This includes understanding how transactions are initiated, authorized, processed, and recorded in systems, until reflected in the entity's financial records. Our understanding provides a basis for us to identify and assess RMMs.

Accuracy, completeness, and validity represent risks that exist within an entity's information system that we take into consideration when identifying process risk points (PRPs) and/or risks arising from IT (RAFITS) and the control activities which address the PRPs/RAFITS (see question '[Which control activities do we understand and are relevant to the audit?](#)' for further information).

Do we always test the 'authorization' of transactions and other information? [ISA | 1351.8518]

No. Validity is generally achieved through control activities; therefore, we only test for authorization when we decide to evaluate the design and implementation or test the operating effectiveness of control activities.

Example

What do we think about when understanding the information relied on? [ISA | 1351.8456]

Fact pattern 1

Evaluation	
Example consideration	Whether the control relies on appropriate (relevant and reliable) information in the performance of the control activity to address the control objective
Objective of the control (PRP)	Allowance for doubtful accounts receivable is valued appropriately
Control description	At each period-end, the control operator reviews the entity-wide A/R aging report to assess the reasonableness of the allowance for doubtful accounts
Evaluation of the design	The control may address the control objective if the entity only operates domestically and has one line of business with similar receivable terms for all of its customers. However, if the entity has operations in different countries or regions or has multiple lines of businesses and the receivable terms for its sales transactions are dissimilar, an entity-wide A/R aging report may not be appropriate to meet the control objective.

Fact pattern 2

Evaluation	
Example consideration	Whether the control relies on appropriate (relevant and reliable) information in the performance of the control activity to address the control objective

Objective of the control (PRP)	Future minimum lease liabilities disclosures are complete, accurate and fairly presented.
Control description	<p>At period-end, the control operator reviews the lease note, including agreeing amounts to underlying schedules for completeness and accuracy.</p> <p>[Note: There is another control where the control operator completes a disclosure checklist and assesses the completeness and fair presentation of the accounting policies disclosed.]</p>
Evaluation of the design	The control may address the control objective if the underlying schedule with future minimum lease liability amounts is assessed for relevance and reliability as a control attribute in this control or in a separate control.

How may we identify information relied on in an automated process control activity? [ISA | 1351.8510]

Scenario 1

Fact pattern

The engagement team has identified the following process risk point (PRP) and the automated process control activity that addresses this PRP:

- PRP: Purchase invoices are not all entered accurately into the system
- Automated process control activity description: The system automatically approves purchase invoices information for posting to the general ledger and payment when the purchase invoice information matches to the purchase order and goods receipt information in the system. Exceptions are flagged as unmatched and are not processed without manual intervention.

We determine whether we have evaluated whether the information used in the control is sufficiently reliable.

Analysis

The purchase invoice information is the subject of the automated process control activity as the control is testing that the entered information for the purchase invoice is correct. The reliability of the purchase invoices is addressed by testing the control itself.

The purchase order information and the goods receipts information are not subject to one or more of the control's attributes and is information relied on by the control. The purchase order and goods receipt are information and we evaluate the relevance and reliability of that information, because it is relied on by the three-way-match, by testing control activities over the accuracy and completeness of that information or by direct-testing the accuracy and completeness of that information.

Scenario 2

Fact pattern

The engagement team has identified the following process risk point (PRP) and the automated process control activity that addresses this PRP:

- PRP: Incomplete or inaccurate recognition of interest expense
- Automated process control activity description: Oracle Financials automatically calculates the monthly interest expense and records the expense in the general ledger based on the interest rates in the interest rate table and the long term debt balance at month end for each loan included in the loan balance.

We determine whether we have evaluated whether the information used in the control is sufficiently reliable.

Analysis

Both the interest rates and the loan balances are information used in the automated process control activity. When taking a controls approach to evaluating information, we identify the PRPs and/or RAFITs and control activities related to data input, integrity and extraction and manipulation risks of the information in the interest rate table and loan balances, which may include identifying GITCs over the database.

Alternatively, we may direct-test that the information used in the interest expense calculation is consistent with the bank's daily interest rate and loan balance at the period end; however, to the extent that the loan balance has been substantively tested separately, we may not perform additional procedures in relation to the reliability of the loan balance.

The interest rate is not part of the flow of information into the financial statements and we are only testing the control activities over the interest rate or direct-testing the interest rate because it is information used in the interest rate calculation automated process control activity.

1.4 Understand how the entity has responded to RAFITs [ISA | 1355]

What do we do?

Obtain an understanding of how the entity has responded to risks arising from IT.

Why do we do this?

Risks arising from IT (RAFITs) pose a risk to the continued effective operation of automated controls as well as to the integrity of data and information within IT systems. Therefore, we understand how the entity has responded to RAFITs when we identify and evaluate the design and implementation of automated controls or we take a controls approach to evaluate the reliability of data and information within IT systems.

Execute the Audit

How do we obtain an understanding of how the entity has responded to RAFITs? [ISA | 1355.1400]

We obtain an understanding of how the entity has responded to RAFITs by:

- identifying the relevant layers of technology and risks arising from IT (RAFITs); and
- identifying and evaluating the design and implementation of relevant general IT controls (GITCs).

1.4.1 Identify relevant layers of technology and RAFITs [ISA | 1354]

What do we do?

Identify the layers of technology and risks arising from IT that are relevant to the effective operation of automated controls or the integrity of data and information within the IT system.

Why do we do this?

Identifying the relevant layers of technology (application, database, operating system, or network) helps us identify the relevant RAFITs within those layers, which in turn helps us identify the GITCs that address those RAFITs.

Execute the Audit

What are the layers of technology that comprise an IT system? [ISA | 1354.10387]

IT systems are comprised of four types of layers of technology (also referred to as IT system layers or IT layers), which are the application, database, operating system and network layers (the last three layers may be collectively referred to as IT infrastructure). Each of these layers of technology may present risks arising from IT (RAFITs) to be controlled by management so that:

- automated controls operate and function effectively; or
- the integrity of data and information sourced from an entity's IT system is maintained.

The table below provides a description of each of the layers of technology.

Layer	Description
Application	<p>Applications are the layers of IT systems designed to perform one or many functions, tasks or activities - often to capture, process or extract data. Applications often include an interface accessed by an end-user.</p> <p>An IT application is a program or a set of programs that is used in the initiation, processing, recording and reporting of transactions or information. Examples of the application layer of an IT system include:</p> <ul style="list-style-type: none"> • ERP systems, such as SAP and Oracle; • report writers, • emerging technologies, such as robotic process automation (RPA), artificial intelligence; and • transaction-processing systems, such as a CRM or billing system.

Database	Databases are the layers of IT systems that organize a collection of data or information so that it can be easily accessed, managed and updated. This includes data warehouses, which are separate applications that we consider as a database layer. SQL Server and Oracle DB, as well as stand-alone data repositories and data warehouses, are examples of the database layer of an IT system. Technologies such as MS SQL Server may be used by an entity for multiple IT systems to access information in the database.
Operating system	Operating systems are the layers of IT systems that control the basic operation of a computer and provide a software platform on which to run other software, such as applications and databases. The operating system generally works behind the scenes and is usually not manipulated directly by the end user. UNIX, LINUX, Microsoft Windows and MacOS are examples of the operating system layer of an IT system.
Network	Networks are the layers of IT systems that transport information or data between computers, either within an organization or between organizations. Access to IT applications may be restricted to users on a particular network - e.g. users cannot access an IT application outside of a local area network (LAN) or virtual private network (VPN). Wide area networks (WANs), LANs and VPNs are examples of the network layer of an IT system.

When is a layer of technology relevant? [ISA | 1354.8678]

A layer of technology is relevant when there is one or more relevant RAFITs within that layer of technology.

What is a RAFIT? [ISA | 1354.1300]

A RAFIT represents the susceptibility of automated controls to ineffective design or operation, or risks to the integrity of information in the entity's information system, due to ineffective design or operation of general IT controls. In other words, a RAFIT represents any condition that could affect the effective operation of automated controls or the integrity of data and information within an entity's IT system.

How is a PRP different from a RAFIT? [ISA | 1354.10538]

The table below shows the main differences between PRPs and RAFITs:

	Process risk point (PRP)	Risk arising from IT (RAFIT)
--	--------------------------	------------------------------

Addressed by:	Process control activities	General IT controls
Identified:	When we obtain an understanding of business processes and the financial reporting process and we plan to evaluate the design and implementation of process control activities	<ul style="list-style-type: none"> - After identifying automated controls that we intend to evaluate design and implementation of (including automated process control activities that address PRPs), or - When evaluating the reliability of internal information by testing management's controls and we decide to address the data integrity risk within the IT system through testing GITCs
Defined as:	Point in the entity's process that a misstatement could, individually or in aggregate, yield a material misstatement to the financial statements. We describe the PRP as the 'where' and the 'how' in the entity's process that misstatement could be introduced	The susceptibility of automated controls to ineffective design or operation, or risks to the integrity of information in the entity's information system, due to ineffective design or operation of general IT controls. In other words, a RAFIT represents any condition that could affect the effective operation of automated controls or the integrity of data and information within an entity's IT system.

What is a relevant RAFIT? [ISA | 1354.8680]

A "relevant RAFIT" is a RAFIT where there is a "reasonable possibility" that the RAFIT could prevent the effective operation of the related automated control and/or integrity of data within the IT system. 'Reasonable possibility' means a more than remote possibility and it is therefore a low threshold.

Do we always identify a relevant RAFIT in each IT process? [ISA | 1354.8681]

No. Not all IT processes affect the effective operation of automated controls or the integrity of data and information within an IT system.

For example, program development may not affect the effective operation of automated controls or the integrity of data and information if the entity did not develop or acquire a new IT system in the current period.

Similarly, IT risks in the computer operations process related to backup and recovery may not affect the effective operation of automated controls or the integrity of data and information.

What is the complete list of RAFITs? [ISA | 1354.8682]

The complete list of RAFITs for each IT process is set out in the table below.

IT process	Risks arising from IT (RAFITS)
Access to programs and data	<p>1.1 APD - Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data.</p> <p>1.2 APD - Logical access permissions (new or modified) are granted to users and accounts (including shared or generic accounts) that are inappropriate (i.e., unauthorized or not commensurate with job responsibilities).</p> <p>1.3 APD - Logical access permissions are not revoked in a timely manner.</p> <p>1.4 APD - Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities).</p> <p>1.5 APD - Physical access to facilities housing IT systems and/or electronic media is unauthorized or not commensurate with job responsibilities.</p>
Program changes	<p>2.1 PC - Changes to IT programs were inappropriate (i.e., unapproved or do not function as intended).</p> <p>2.2 PC - Changes to IT configurations were inappropriate (i.e., unapproved or do not function as intended).</p> <p>2.3 PC - Logical access to implement changes to IT system program or configurations into the production environment is inappropriate (i.e., unauthorized or not commensurate with job responsibilities).</p>
Program acquisition and development	<p>3.1 PD - IT system developments (new components or significant changes) are unapproved or do not function as intended.</p> <p>3.2 PD - Incomplete, redundant, obsolete or inaccurate data is migrated to the production environment of acquired, newly developed or existing IT systems.</p>
Computer operations	<p>4.1 CO - System jobs, processes, and/or programs do not function as intended, resulting in incomplete, inaccurate, untimely or unauthorized processing of data.</p> <p>4.2 CO - Logical access to make changes to system jobs, processes, and/or programs is unauthorized or not commensurate with job responsibilities.</p>

	4.3 CO - Financial data backups are not able to be recovered in a timely manner.
--	--

[Can we identify a RAFIT that is not in the list of RAFITs? \[ISA | 1354.8683\]](#)

No. RAFITs are finite and we have captured a complete list of RAFITs at the appropriate level of granularity.

[Under what circumstances do we identify relevant layers of technology and RAFITs? \[ISA | 1354.1400\]](#)

We identify relevant layers of technology and RAFITs when we:

- plan to rely on and test the operating effectiveness of automated control activities,
- evaluate the design and implementation of automated control activities, even though we do not plan to test their operating effectiveness (e.g., when we evaluate the design and implementation of an automated process control activity that addresses a significant risk or over journal entries). However, when GITCs are a) informal and, therefore, unable to be evaluated for design and implementation or b) expected to be ineffective (i.e. resulting in a control deficiency), we may document our understanding of relevant layers of technology, RAFITs and GITCs in summary as part of our understanding of the IT environment rather than identifying the individual layers of technology, RAFITS and GITCs for each automated control activity, or
- decide to address the data integrity risk within the entity's IT system through testing GITCs, when testing management's controls over the accuracy and completeness of internal information to evaluate the reliability of such information.

[How may we document our understanding of relevant layers of technology, RAFITs and GITCs in summary as part of our understanding of the IT environment? \[ISA | 1354.8899\]](#)

When we evaluate the design and implementation of automated control activities but we do not plan to test their operating effectiveness, and GITCs are a) informal and, therefore, unable to be evaluated for design and implementation or b) expected to be ineffective (i.e. resulting in a control deficiency), we may document our understanding of relevant layers of technology, RAFITs and GITCs in summary as part of our understanding of the entity's IT processes within our understanding of the IT environment.

For example, consider an entity with the following circumstances:

- Has a less complex IT environment
- Uses System A, a single commercial accounting software application
- GITCs are not always formalized and documented
- We identified GITC deficiencies in the previous audit
- We have evaluated the design and implementation of an automated control that addresses a significant risk, but we do not plan to rely on the operating effectiveness of that control

Our understanding of the entity's IT processes may include the following:

IT process	Description
Access to programs and data	The IT Manager and the Accounting Manager (as a backup) have security administrative responsibility to administer access to the system. The prior year deficiency related to the privileged access GITC was not remediated in the current

	<p>year¹. RAFITs related to access to programs and data in system A are considered relevant to automated controls and they are addressed by the following steps in the process.</p> <p>The process to provision access is initiated when the Accounting department identifies a new user that needs access. Generally, the Accounting Manager sends a request either verbally or via email to the IT Manager requesting a new user account. The emails are not always retained².</p> <p>The user is required to change the password upon initial logon. The entity has password rules in place for minimum password length, password expiration, and complexity requirements.</p> <p>The process to de-provision access occurs when the IT Manager is notified of an employee resignation or termination. Upon notification of termination, the IT Manager will revoke the terminated employees' access. The IT Manager indicated that he does not always retain documentation to evidence the timely removal of access².</p> <p>There is no data processing Center, as the system is maintained on the cloud.</p>
<p>Footnotes</p> <p>¹ KPMG identifies this as a deficiency</p> <p>² Since the entity has a less complex IT environment and uses a single commercial accounting software application, GITCs may not always be formalized and documented, which in this case is considered appropriate for the size and complexity of the entity and its IT environment.</p>	

Remember: When documenting our understanding of IT processes, we obtain an understanding for all four IT processes even if we identify a deficiency in one process. In this example, only one row was completed to illustrate example documentation when a deficiency is identified.

How do we identify relevant layers of technology and RAFITs? [ISA | 1354.1500]

To identify relevant layers of technology and RAFITs, we identify:

- The layer of technology where the automated control operates or where the data and information within an IT system exists;
- The layers of technology that are relevant to the effective operation of automated controls or the integrity of data and information within an IT system; and
- the RAFITs within those layers of technology where there is a "reasonable possibility" that the RAFIT could prevent the effective operation of automated controls or the integrity of data and information within an IT system.

We identify the relevant layers of technology and RAFITs concurrently. Even though we start by thinking about what layers of technology are applicable to the automated control or integrity of data within an IT system, we cannot determine that they are relevant if we don't identify one or more relevant RAFITs. In order to assess whether a layer of technology may be relevant, we think about qualitative factors such as where the automated control operates or where the data resides (see

question "[What factors may we think about when identifying relevant layers of technology?](#)" for example factors).

In order to assess whether there is a "reasonable possibility" that the RAFIT could prevent the effective operation of the related automated control and/or integrity of data within the IT system, we think about qualitative factors such as the entity's ability to make code changes or configuration changes (see question "[What factors may we think about when determining when a RAFIT is relevant?](#)" for example factors).

[Can multiple 'layers of technology' be relevant? \[ISA | 1354.8685\]](#)

Yes. Although automated controls are programmed into a particular layer of technology within an IT system, and information we plan to rely on is obtained from the database layer, the RAFITs that are relevant to the effective operation of automated controls and the integrity of data and information can exist in multiple layers of technology that make up an IT system.

[Can an automated control have no relevant layers of technology? \[ISA | 1354.8686\]](#)

A layer of technology is relevant when there is one or more relevant RAFITs within that layer of technology. In the unlikely circumstances when we don't identify any relevant RAFITs for an automated control, we won't have any relevant layers of technology.

For example, we may not identify any relevant layers of technology when we determine it is appropriate to test the operating effectiveness of an automated process control activity throughout the period (see activity '[Test automated process control activities throughout the period, if appropriate](#)').

[What factors may we think about when identifying relevant layers of technology? \[ISA | 1354.8687\]](#)

We start by identifying the layers of technology that are likely to contain RAFITs. For each of those layers, we consider if there are any relevant RAFITs. This enables us to identify the relevant layers of technology and RAFITs.

When the application layer is relevant, the database(s) that stores the data processed by the automated control is typically also relevant. Similarly, because an IT system's ability to operate is often dependent on the operating system and IT applications and databases may be directly accessed from the operating system, the operating system is typically relevant.

The network layer may be identified when an IT system interacts with vendors or external parties through the internet. Generally, RAFITs on the network layer are related to network segmentation/remote access and are not relevant to automated controls. The network layer may be relevant when an entity has web-facing applications used in financial reporting and we identify cybersecurity risks that lead to the identification of an RMM. As part of obtaining an understanding of management's cybersecurity risk assessment, we inquire about how the entity's management evaluates and manages cybersecurity risks across the entity at the network layer. See question "[What does obtaining an understanding of management's cybersecurity risk assessment include?](#)" for more information

To determine if the layer of technology is relevant, we think about the RAFITs and layers of technology factors in parallel. The table below sets out example factors that we may think about when determining whether a layer of technology is relevant.

IT layer factors	Example considerations
------------------	------------------------

The layer in which the automated control operates	An edit check automated process control activity is coded to flag sales transactions for inclusion on an exception report based on a configured dollar threshold flag. The automated process control activity is configured at the application layer and the flag is stored within the database layer . In this scenario, the application and database layers would likely be relevant.
Where the data resides	Relevant data elements (RDEs) presented on the accounts receivable (AR) aging report are stored in the database layer. In this scenario, the database layer would likely be relevant to the integrity of the data.
Where the source code (e.g. stored procedures) is maintained	An automated control relies on stored procedures in a database , where access to deploy a change consists of modifying the stored procedure directly in the database. In this scenario, the database layer would likely be relevant.
Where and how users access the functionality subject to system access controls	For an automated access process control activity to restrict access to change the vendor master file, users can access the functionality through the application layer . In this scenario, the application layer would likely be relevant.
Where the data, subject to the functionality being restricted, can be updated and/or modified	Consider what layer(s) of technology the data subject to the functionality is stored. The vendor master data is stored in the vendor master file database . In this scenario, the database layer would likely be relevant.
Whether special user privileges in other layers of technology can access the data	Accounts at the operating system layer have special privileges to make updates to the vendor master file in a way that would impact the ongoing operation of the automated process control activity. For example, in a Unix operating system, the root account has special privileges, including the ability to make direct updates to the vendor master file, bypassing application layer security. In this scenario, the operating system layer would likely be relevant.

[What factors may we think about when determining when a RAFIT is relevant? \[ISA | 1354.8688\]](#)

The table below sets out example factors, scenarios and considerations that we may think about when determining when a RAFIT is relevant.

RAFIT factors	Example scenarios	Example considerations
<p>Whether the entity has access to make code changes</p> <p>Refer to the question "What are automated controls?" and sub-questions for more information on coded and configured automated controls.</p>	<p>An entity has access to make code changes at the operating system layer. For a coded automated control where changes are migrated from the operating system layer quality assurance environment to the production environment, the following RAFITs at the operating system layer would likely be relevant:</p> <ul style="list-style-type: none"> • 2.3 PC: Logical access to implement changes to IT system program or configurations into the production environment is inappropriate (i.e., unauthorized or not commensurate with job responsibilities). • 1.1 APD: Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data. • 1.3 APD: Logical access permissions are not revoked in a timely manner. • 1.4 APD: Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities). 	<p>When an entity has access to modify code, typically there are risks related to unauthorized privileged access, incompatible job responsibilities (i.e. segregation of duties), and authentication in relation to the layer where the code can be changed. Because generally only privileged users are able to make code changes, we focus on RAFITs related to privileged user access (1.4 APD), supported by identification and authentication mechanisms (1.1 APD) and the specific access to be able to promote such changes (2.3 PC). Risks related to end users making code changes are considered remote, so 1.2 APD is not likely a relevant RAFIT. 1.3 APD may be likely, to the extent it relates to removal of privileged accounts.</p>
<p>Whether the entity has access to make configuration changes</p>	<p>An entity has access to make configuration changes at the application layer. For a configured automated control where configuration changes are implemented directly in the application layer, the following RAFITs at the application layer would likely be relevant:</p> <ul style="list-style-type: none"> • 2.3 PC: Logical access to implement changes to IT system program or configurations into the production environment is inappropriate (i.e., unauthorized or not commensurate with job responsibilities). 	<p>This factor is relevant to situations where the entity has access to modify configurable settings for IT systems where automated controls reside. When an entity has access to modify configurable settings, similar to situations where the entity has access to modify code, there is a risk that individuals or privileged users could make configuration changes in production</p>

	<ul style="list-style-type: none"> • 1.1 APD: Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data. • 1.3 APD: Logical access permissions are not revoked in a timely manner. • 1.4 APD: Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities). 	<p>without going through the appropriate configuration change management process.</p> <p>The RAFITs related to privileged users (1.4 APD), promotion to production (2.3 PC) supported by identification and authentication mechanisms (1.1 APD) and the specific access to change configurations are likely relevant (2.3 PC). 1.3 APD may be likely relevant, to the extent it relates to removal of privileged accounts. The likelihood end users would be able to do this is considered remote, so 1.2 APD is not likely a relevant RAFIT.</p>
Process to approve and test source code changes to production	<p>Changes to a coded automated process control activity are performed in-house. The entity's change management process requires business and IT management approvals before initiating the change as well as testing of the change prior to migration to production. In this scenario, the following RAFIT at the application layer would likely be relevant:</p> <ul style="list-style-type: none"> • 2.1 PC: Changes to IT programs were inappropriate (i.e., unapproved or do not function as intended). 	<p>This factor is relevant to situations where code changes are made to IT systems where automated controls reside and the process the entity has implemented to approve and test those changes. This may include IT systems that are developed in-house, outsourced to a third party, or purchased from a vendor.</p> <p>When changes are made to IT systems, typically there are risks related to implementing unapproved program changes and program changes not functioning as intended (2.1 PC). In addition to these risks, please see the 'Whether the entity has access to make code changes' factor for additional considerations.</p> <p>Note this factor is focused on risks related to the approval</p>

		and testing of source code changes and is separate from the factor that considers the risks related to logical access to implement changes to IT system programs into the production environment (2.3 PC)
<p>Process to approve and test configuration changes to production</p> <p>This factor will also be relevant when the entity does not have direct access to source code but is responsible for evaluating updates and upgrades provided by the vendor before installing on the live environment.</p>	<p>Changes to application configurations associated with an automated control are performed at the application layer. The entity's configuration change process requires business management approvals before initiating the change as well as testing of the change prior to applying the change to production. In this scenario, the following RAFIT at the application layer would likely be relevant:</p> <ul style="list-style-type: none"> • 2.2 PC: Changes to IT configurations were inappropriate (i.e., unapproved or do not function as intended). 	<p>This factor is relevant to situations where configurations changes are made to IT systems where automated controls reside and the process the entity has implemented to approve and test those changes. This may include IT systems that are developed in-house, outsourced to a third party, or purchased from a vendor.</p> <p>When configuration changes are made to IT systems, typically there are risks related to implementing unapproved configuration changes and configuration changes not functioning as intended (2.2 PC). In addition to these risks, please see the 'Whether the entity has access to make configuration changes' factor for additional considerations.</p> <p>Note this factor is focused on risks related to the approval and testing of configuration changes and is separate from the factor that considers the risks related to logical access to implement configurations into the production environment (2.3 PC).</p>

User type	<p>An entity grants regular business end users access to the application layer functionality that allows changes to the vendor master file. In this scenario, the following RAFITs at the application layer would likely be relevant:</p> <ul style="list-style-type: none"> • 1.1 APD: Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data. • 1.2 APD: Logical access permissions are granted (new or modified) to users and accounts (including shared or generic accounts) that are inappropriate (i.e., unauthorized or not commensurate with job responsibilities). • 1.3 APD: Logical access permissions are not revoked in a timely manner. • 1.4 APD: Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities). <p>As another example, database administrators have direct access to make changes to the vendor master file. In this scenario, the following RAFITs at the database layer would likely be relevant:</p> <ul style="list-style-type: none"> • 1.1 APD: Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data. • 1.2 APD: Logical access permissions are granted (new or modified) to users and accounts (including shared or generic accounts) that are inappropriate (i.e., unauthorized or not commensurate with job responsibilities). 	<p>This factor is relevant when testing system access controls. We consider the type of user (e.g. regular business end user, system administrator, database administrator, system accounts, shared accounts, etc.) at each layer of technology, that has access to the functionality or data subject to the automated control.</p> <p>This means that risks related to inappropriate end user access (1.1 APD - 1.3 APD) as well as those related to privileged user access (1.4 APD) are likely relevant.</p> <p>We expect these RAFITs to be relevant to system access controls in all relevant layers of technology in which the access is granted.</p>
------------------	---	---

	<ul style="list-style-type: none"> • 1.3 APD: Logical access permissions are not revoked in a timely manner. • 1.4 APD: Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities). 	
How access to functions / transactions is restricted*	<p>To manage access to functions / transactions, an entity uses security groups to assign user privileges / access rights at the application layer. The following RAFITs at the application layer would likely be relevant:</p> <ul style="list-style-type: none"> • 2.2 PC: Changes to IT configurations were inappropriate (i.e., unapproved or do not function as intended). • 2.3 PC: Logical access to implement changes to IT system program or configurations into the production environment is inappropriate (i.e., unauthorized or not commensurate with job responsibilities). • 1.1 APD: Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data. • 1.2 APD: Logical access permissions are granted (new or modified) to users and accounts (including shared or generic accounts) that are inappropriate (i.e., unauthorized or not commensurate with job responsibilities). • 1.3 APD: Logical access permissions are not revoked in a timely manner. • 1.4 APD: Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., 	<p>This factor is relevant when testing system access controls. We consider how the system access control is designed to restrict access to functions (e.g. change vendor master file) and whether security groups, roles, or profiles are used.</p> <p>We also consider the risks related to changing the security groups, roles or profiles. Since security groups, roles or profiles are generally configured into the system and not hard coded, RAFITs 2.2 PC and 2.3 PC are likely relevant. Risks related to inappropriate end user access (1.1 APD - 1.3 APD) as well as those related to privileged user access (1.4 APD) are also likely relevant as it relates to this factor.</p> <p>We expect these RAFITs to be relevant to system access controls in all relevant layers of technology in which the access is granted.</p>

	unauthorized or not commensurate with job responsibilities).	
Physical access	An entity uses an open console where changes to the system can be made. In instances where physical security risks exist, the following RAFIT would likely be relevant: <ul style="list-style-type: none"> • 1.5 APD: Physical access to facilities housing IT systems and/or electronic media is unauthorized or not commensurate with job responsibilities. 	We consider the risk that unauthorised changes can be made by individuals with access to the console.
Dependency on scheduled jobs	An entity relies on an automated system calculation control that calculates depreciation. This system calculation automatically runs based on a monthly scheduled job configured in the job scheduling application. In this example, the following RAFITs at the application layer would likely be relevant: <ul style="list-style-type: none"> • 4.1 CO: System jobs, processes, and/or programs do not function as intended, resulting in incomplete, inaccurate, untimely or unauthorized processing of data. • 4.2 CO: Logical access to make changes to system jobs, processes, and/or programs is unauthorized or not commensurate with job responsibilities. • 1.1 APD: Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data. • 1.4 APD: Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities). • 2.1 PC: Changes to IT programs were inappropriate (i.e., unapproved or do not function as intended). 	We consider risks associated with inaccurate, incomplete, untimely processing of system jobs, or unauthorized changes, including batch jobs and interfaces (e.g. risk of unauthorized program execution, deviations from scheduled processing, etc.) When the effective operation of the control activity is dependent on running at a specific point in a process or at a specific time, risks related to scheduled jobs are relevant (4.1 CO). Computer operations risks can themselves be caused by inappropriate access or inappropriate changes to the job scheduler (4.2 CO), which then means that PC and APD risks can also affect the control activity. As the job scheduler is generally both coded and configured, both 2.1 PC and 2.2 PC may be relevant, depending on how the schedule is set up. 2.3 PC is likely relevant as it relates to

	<ul style="list-style-type: none"> 2.2 PC: Changes to IT configurations were inappropriate (i.e., unapproved or do not function as intended). 2.3 PC: Logical access to implement changes to IT system program or configurations into the production environment is inappropriate (i.e., unauthorized or not commensurate with job responsibilities). 	<p>the ability to implement any change in the scheduler.</p> <p>The risk of an end user being able to access or make changes to the job scheduler is generally remote, so 1.2 APD and 1.3 APD are not likely relevant. 1.4 APD supported by 1.1 APD would likely be relevant RAFITs as it relates to this example.</p>
Dependency on backup and recovery of programs and data	<p>An entity relies on an automated interface control that transmits data from System A to System B. The interface runs automatically based on a monthly scheduled job. If there were issues with the transmission of data from System A's database to System B's database such that data was partially transmitted, the automated control activity relies on the backup and recovery of data to recover the data and re-run the interface for completeness. In this scenario, the following RAFIT at the database layer would likely be relevant:</p> <ul style="list-style-type: none"> 4.3 CO: Financial data backups are not able to be recovered in a timely manner. 	<p>This criterion is specifically directed at determining if this RAFIT is relevant, so no other RAFITs are considered here.</p>
Occurrence of data migration	<p>An entity migrates data from their legacy system to a newly acquired system. The following RAFIT at the database layer would likely be relevant:</p> <ul style="list-style-type: none"> 3.2 PD: Incomplete, redundant, obsolete or inaccurate data is migrated to the production environment of acquired, newly developed or existing IT systems. 	<p>When data is migrated from one system to another during the period, this creates the risk that such data will be corrupted, lost or does not migrate over completely or accurately. Such migrations may occur when systems are upgraded, replaced or merged.</p>
<p>*Note that access refers to the ability to make changes, it does not include "read only access"</p>		

How may the complexity of the entity's IT environment impact our identification of relevant RAFITs and GITCs? [ISA | 1354.8679]

The extent of our understanding of the IT processes varies with the nature and the circumstances of the entity and its IT environment. The complexity of the IT environment may also impact the extent to which the entity has GITCs in place, as well as the number of layers of technology that include relevant RAFITs.

For example:

- An entity that uses commercial software and does not have access to the source code to make any program changes is unlikely to have a process for program changes, but may have a process or procedures to configure the software (e.g., the chart of accounts, reporting parameters or thresholds). In addition, the entity may have a process or procedures to manage access to the application (e.g., a designated individual with administrative access to the commercial software). In such circumstances, the entity is unlikely to have or need formalized GITCs.
- In contrast, a larger entity may rely on IT to a great extent and the IT environment may involve multiple layers of technology and the IT processes to manage the IT environment may be complex (e.g., a dedicated IT department exists that develops and implements program changes and manages access rights), including that the entity has implemented formalized GITCs over its IT processes.
- When management is not relying on automated process control activities or GITCs to process transactions or maintain the data, and we have not identified any automated process control activities (or any that depend on GITCs), we may plan to directly test any information used as audit evidence involving IT and may not identify any layers of technology that include relevant RAFITs.
- When management relies on a layer of technology to process or maintain data and the volume of data is significant, and management relies upon the layer of technology to perform automated controls that we have also identified, the layer of technology is likely to include relevant RAFITs.

Examples

How do we identify relevant layers of technology and RAFITs related to automated controls and the GITCs that address them? [\[ISA | 1354.1801\]](#)

Fact pattern 1

Consider an entity that:

- Has a less complex IT environment comprised of an IT manager and two system administrators.
- Uses ABC system, a single commercial accounting software application.

As part of obtaining an understanding of the financial reporting process, the engagement team identifies several PRPs related to journal entries and relevant process control activities that address those PRPs. Among those, the engagement team identifies the following PRP and relevant automated process control activity that addresses the PRP:

Process risk point (PRP)	Incorrect or inappropriate journal entries are entered if users can self approve journals they enter.
Automated process control activity	AC-1: The ABC system is coded to prevent the preparer of a journal entry from approving the same journal entry.

Additionally, in obtaining an understanding of the IT systems, IT processes, and the evaluation of the design of the automated process control activity, the engagement team noted the following:

- The automated process control activity operates at the application layer and operates by comparing the unique user IDs of both the preparer and the reviewer of the same journal entry.
- The functionality comes delivered with the ABC system.
- The entity cannot change the functionality of the ABC system.
- ABC system source code is maintained by the vendor and the entity does not have access to make changes to the source code.
- New releases of ABC system are delivered by the vendor. The entity is responsible for evaluating whether new releases meet their business needs.
- New releases are implemented on the operating system by a system administrator. Actions performed at the operating system layer would not impact how journal entries are prevented from being prepared and approved by the same individual or the ongoing effectiveness of the automated process control activity.

Analysis 1

For the relevant automated process control activity that addresses the PRP, the engagement team identifies:

- the layer of technology where the automated process control activity operates and the layers of technology that are relevant to the effective operation of the automated process control activity;
- the RAFITs within those layers of technology where there is a "reasonable possibility" that the RAFIT could prevent the effective operation of the automated process control activity; and
- the GITCs that address the relevant RAFITs;

as set out in the table below.

AC1: The ABC system is coded to prevent the preparer of a journal entry from approving the same journal entry.			
IT system	Layer of technology	RAFIT	GITC
ABC system	Application	2.1 PC - Changes to IT programs were inappropriate (i.e., unapproved or do not function as intended).	GITC-2.1PC-1 - Changes to IT system programs are approved by the business/IT prior to implementation

			into the production environment.
			GITC-2.1PC-2 - Changes to IT system programs are tested and approved in accordance with the organization's change management policy.
Layer/RAFIT analysis: RAFIT 2.1 PC is deemed relevant on the application layer since this is the layer where the automated process control activity operates. No RAFITs related to access to programs and data have been deemed relevant as the automated process control activity is based on the system coding that determines that the preparer and the approver of the same journal entry are different, regardless of the type of user permissions they have. However, the engagement team determined there is a reasonable possibility that unapproved changes and untested changes on the application layer could affect the effective operation of the automated process control activity.			

Fact pattern 2

Consider an entity that:

- Has a less complex IT environment comprised of an IT manager and two system administrators.
- Uses ABC system, a single commercial accounting software application.

As part of obtaining an understanding of the order-to-cash process, the engagement team identifies several PRPs and relevant process control activities that address those PRPs. Among those, the engagement team identifies the following PRP and relevant automated process control activity that addresses the PRP:

Process risk point (PRP)	Inaccurate data is entered into the customer master file resulting in incorrect recording of sales.
Automated process control activity	AC-2: Access to change the customer master file is restricted to authorized personnel

Additionally, in obtaining an understanding of the IT systems, IT processes, and the evaluation of the design of the automated process control activity, the engagement team noted the following:

- The automated process control activity operates at the application layer.
- The customer master file resides within an SQL server database.

- Additions and modifications to the customer master file are performed by users within the accounts receivable department by accessing the ABC system application. Users are assigned a specific permission (i.e. direct access) to allow additions and modifications.
- The system administrators have privileged access to the ABC system application and SQL server database.
- From the engagement team's understanding of the IT processes, there was no turnover in the system administrators group from the prior period

Analysis 2

For the relevant automated process control activity that addresses the PRP, the engagement team identifies:

- the layer of technology where the automated process control activity operates and the layers of technology that are relevant to the effective operation of the automated process control activity;
- the RAFITs within those layers of technology where there is a "reasonable possibility" that the RAFIT could prevent the effective operation of the automated process control activity; and
- the GITCs that address the relevant RAFITs;

as set out in the table below.

AC-2: Access to change the customer master file is restricted to authorized personnel.			
IT system	Layer of technology	RAFIT	GITC
ABC system	Application	1.1 APD - Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data.	GITC-1.1APD-1 - Access is authenticated through unique user IDs and passwords as a mechanism for validating that users are authorized to gain access to the system. Password parameters meet company or industry standards (e.g., password minimum length and complexity, expiration, account lockout).
		1.2 APD - Logical access permissions	GITC-1.2APD-1 - Management

		are granted (new or modified) to users and accounts (including shared or generic accounts) that are inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	approves the nature and extent of user access privileges for new and modified user access, including standard application profiles/roles, and critical financial reporting transactions.
		1.3 APD - Logical access permissions are not revoked in a timely manner.	GITC-1.3APD-1 - Access for terminated or transferred users is removed or modified in a timely manner.
		1.4 APD - Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	GITC-1.4APD-1 - Every quarter, the IT managers periodically review user access of privileged users to determine whether user access is appropriately restricted.
Layer/RAFIT analysis: RAFITs 1.1 APD1 - 1.4 APD on the application layer were deemed relevant since the automated process control activity operates at the application layer and based on the category of the automated control (system access).			
SQL server database	Database	1.1 APD - Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data.	GITC-1.1APD-1 - Access is authenticated through unique user IDs and passwords as a mechanism for validating that users are authorized to gain access to the

			system. Password parameters meet company or industry standards (e.g., password minimum length and complexity, expiration, account lockout).
		1.4 APD - Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	GITC-1.4APD-1 - Every quarter, the IT managers periodically review user access of privileged users to determine whether user access is appropriately restricted.
Layer/RAFIT analysis: RAFITs 1.1 APD and 1.4 APD on the database layer were deemed relevant since the customer master file data resides within an SQL server database and the system administrators have privileged access to the SQL server database. In addition to adding and modifying the customer master file through the ABC system application, an individual with system administrator privileges to the SQL server database can also add or modify the customer master file data. 1.2 APD and 1.3 APD are not relevant to the database layer because business users (i.e. those who are not system administrators) make changes to the customer master file directly through the application layer rather than the database layer.			

Fact pattern 3

Consider an entity that:

- Has a more complex IT environment comprised of a CIO, application managers, system administrators, developers, and database administrators.
- Uses Oracle as its enterprise resource planning (ERP) system. The Oracle ERP uses an Oracle database and runs on a Unix operating system.
- The entity customized the Oracle ERP to meet the needs of the business and has access to modify the source code.

As part of obtaining an understanding of the financial reporting process, the engagement team identifies several PRPs related to journal entries and relevant process control activities that address

those PRPs. Among those, the engagement team identifies the following PRP and relevant automated process control activity that addresses the PRP:

Process risk point (PRP)	Incorrect or inappropriate journal entries are entered into Oracle ERP if users can self approve journals they enter
Automated process control activity	AC-1: The Oracle ERP system is configured to prevent the preparer of a journal entry from approving the same journal entry.

Additionally, in obtaining an understanding of the IT systems, IT processes, and the evaluation of the design of the automated process control activity, the engagement team noted the following:

- The automated process control activity operates at the application layer.
- The entity can require the preparer of a journal entry to be different from the approver by changing the Journal Workflow System setting to "enable" within the application. The setting is stored within the Oracle database.
- Privileged users on the application have elevated access, including access to change the configuration.
- Users with access to the database settings can also change the configuration setting.
- The functionality of the automated process control activity comes delivered with the Oracle ERP system.
- The automated process control activity can be changed via code or configurations.
- Oracle ERP system source code is maintained by the entity and the entity has access to make changes to the source code.
- Changes to code are implemented on the operating system and the entity restricts developer access to the operating system. Developer access to the operating system layer could impact the functionality and the ongoing effectiveness of the automated process control activity.
- Business users are not granted access to operating systems or databases.
- The automated process control activity is not reliant on a job scheduling tool or other computer operations processes.

Analysis 3

For the relevant automated process control activity that addresses the PRP, the engagement team identifies:

- the layer of technology where the automated process control activity operates and the layers of technology that are relevant to the effective operation of the automated process control activity;
- the RAFITs within those layers of technology where there is a "reasonable possibility" that the RAFIT could prevent the effective operation of the automated process control activity; and
- the GITCs that address the relevant RAFITs;

as set out in the table below.

AC1: The Oracle ERP system is configured to prevent the preparer of a journal entry from approving the same journal entry.

IT system	Layer of technology	RAFIT	GITC
Oracle ERP	Application	2.1 PC - Changes to IT programs were inappropriate (i.e., unapproved or do not function as intended).	GITC-2.1PC-1 - Changes to IT system programs are approved by the business/IT prior to implementation into the production environment.
			GITC-2.1PC-3 - Changes to IT system programs are tested prior to implementation into the production environment.
		2.2 PC - Changes to IT configurations were inappropriate (i.e., unapproved or do not function as intended).	GITC-2.2PC-1 - Changes to IT system configurations are approved by the business prior to implementation into the production environment.
			GITC-2.2PC-2 - Changes to IT system configurations are tested prior to implementation into the production environment.
		2.3 PC - Logical access to implement changes to IT system program	GITC-2.3PC-1 - Access to implement changes into the production

		<p>or configurations into the production environment is inappropriate (i.e., unauthorized or not commensurate with job responsibilities).</p>	<p>environment for the Oracle application, including configuration changes, is authorized and restricted for use only by designated system administrators, and segregated from the development environment.</p>
		<p>GITC-1.3APD-2</p> <ul style="list-style-type: none"> - On a quarterly basis, management reviews access permissions assigned to users. Any access modifications identified are evaluated and corrective action is taken. 	
		<p>1.1 APD - Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data.</p>	<p>GITC-1.1APD-1</p> <ul style="list-style-type: none"> - Access is authenticated through unique user IDs and passwords as a mechanism for validating that users are authorized to gain access to the system. Password parameters meet company or industry standards (e.g., password minimum length and complexity,

			expiration, account lockout).
	1.2 APD - Logical access permissions are granted (new or modified) to users and accounts (including shared or generic accounts) that are inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	GITC-1.2APD-1 - Management approves the nature and extent of user access privileges for new and modified user access, including standard application profiles/roles, and critical financial reporting transactions.	
		GITC-1.3APD-2 - On a quarterly basis, management reviews access permissions assigned to users. Any access modifications identified are evaluated and corrective action is taken.	
	1.3 APD - Logical access permissions are not revoked in a timely manner.	GITC-1.3APD-1 - Access for terminated or transferred users is removed or modified in a timely manner.	
	1.4 APD - Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is	GITC-1.4APD-2 - Privileged-level access (e.g., configuration, data and security administrators) in the Oracle application is	

		inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	authorized and appropriately restricted for use by designated IT system administrators.
GITC-1.3APD-2 - On a quarterly basis, management reviews access permissions assigned to users. Any access modifications identified are evaluated and corrective action is taken.			

Layer/RAFIT analysis: RAFITs 2.1 PC - 2.3 PC on the application layer were deemed relevant based on the following considerations:

- The automated process control activity operates at the application layer
- The entity configures the journal entries to require a separate approver from the preparer within the application and the settings are stored within the Oracle database.
- Privileged users on the application have elevated access, including access to change the configuration.
- Oracle ERP system source code is maintained by the entity and the entity has access to make changes to the source code

RAFITs 1.1 APD to 1.4 APD on the application layer were deemed relevant based on the following considerations:

- The automated process control activity operates at the application layer
- The entity has access to enable the configuration (e.g. journal workflow) to require the preparer of a journal entry to be different from the approver by changing the system setting to "enable" within the application.
- Privileged users on the application have elevated access, including access to change the configuration.

Unix	Operating System	1.1 APD - Identification and authentication mechanisms are not implemented	GITC-1.1APD-1 - Access is authenticated through unique user IDs and passwords
------	------------------	---	---

		<p>to restrict logical access to IT systems and data.</p>	<p>as a mechanism for validating that users are authorized to gain access to the system. Password parameters meet company or industry standards (e.g., password minimum length and complexity, expiration, account lockout).</p>
		<p>1.3 APD - Logical access permissions are not revoked in a timely manner.</p>	<p>GITC-1.3APD-1 - Access for terminated or transferred users is removed or modified in a timely manner.</p>
		<p>1.4 APD - Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities).</p>	<p>GITC-1.4APD-2 - Privileged-level access (e.g., configuration, data and security administrators) in the Unix operating system is authorized and appropriately restricted for use by designated IT system administrators.</p>
			<p>GITC-1.3APD-2 - On a quarterly basis, management reviews access permissions assigned to users. Any access modifications identified are</p>

			evaluated and corrective action is taken.
	2.3 PC - Logical access to implement changes to IT system program or configurations into the production environment is inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	GITC-2.3PC-1 - Access to implement changes into the production environment for the Unix operating system, including configuration changes, is authorized and restricted for use only by designated system administrators, and segregated from the development environment.	
		GITC-1.3APD-2 - On a quarterly basis, management reviews access permissions assigned to users. Any access modifications identified are evaluated and corrective action is taken.	

Layer/RAFIT analysis: RAFITs 2.3 PC, 1.1 APD, 1.3 APD, and 1.4 APD on the operating system layer were deemed relevant based on the following considerations:

- Oracle ERP system source code is maintained by the entity and the entity has access to make changes to the source code.
- Changes to code are implemented on the operating system and the entity restricts developer access to the operating system. Developer access to the operating system layer could impact how Oracle ERP prevents journal entries from being prepared and approved by the same user and the ongoing effectiveness of the automated process control activity.

		<p>RAFIT 1.2 APD at the operating system was not deemed relevant because the risk of unauthorized users and accounts (including shared or generic accounts) is not deemed a relevant risk since business users are not granted access to the operating system.</p> <p>RAFITS 2.1 PC - 2.2 PC were not deemed relevant at the operating system layer because changes to the application layer affect the way the automated process control activity operates and not the operating system layer. There is not a reasonable possibility that changes to the operating system itself would affect the automated process control activity.</p>	
Oracle database	Database	<p>1.1APD - Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data.</p>	<p>GITC-1.1APD-1</p> <ul style="list-style-type: none"> - Access is authenticated through unique user IDs and passwords as a mechanism for validating that users are authorized to gain access to the system. Password parameters meet company or industry standards (e.g., password minimum length and complexity, expiration, account lockout).
		<p>1.3 APD - Logical access permissions are not revoked in a timely manner.</p>	<p>GITC-1.3APD-1</p> <ul style="list-style-type: none"> - Access for terminated or transferred users is removed or modified in a timely manner.
		<p>1.4 APD - Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not</p>	<p>GITC-1.4APD-2</p> <ul style="list-style-type: none"> - Privileged-level access (e.g., configuration, data and security administrators) in the Oracle database is authorized and appropriately restricted for use

		commensurate with job responsibilities).	by designated IT system administrators.
GITC-1.3APD-2 - On a quarterly basis, management reviews access permissions assigned to users. Any access modifications identified are evaluated and corrective action is taken.			
<p>Layer/RAFIT analysis: RAFITs 1.1 APD, 1.3 APD, and 1.4 APD on the database layer were deemed relevant based on the following considerations:</p> <ul style="list-style-type: none"> • The entity configures the journal entries to require a separate approver from the preparer within the application and the settings are stored within the Oracle database. • Users with access to the database settings can also change the configuration setting. • Since the settings are stored within the Oracle database, there is a risk that unauthorized access to the journal entry settings could affect the effective operation of the automated process control activity. <p>RAFIT 1.2 APD at the database was not deemed relevant because business users are not granted access to the database.</p> <p>RAFITs 2.1 PC - 2.2 PC were not deemed relevant at the database layer because there is not a reasonable possibility that changes to the database would affect the way that the automated process control activity operated.</p>			

1.4.2 Identify and evaluate the design and implementation of relevant GITCs [ISA | 1353]

What do we do?

Identify and evaluate the design and implementation of relevant general IT controls.

Why do we do this?

Identifying and evaluating the design and implementation of GITCs that address relevant RAFITs gives us evidence to support the:

- continued effective operation of automated controls; and/or
- integrity of data and information within the IT systems that we plan to rely on as part of our audit.

Execute the Audit

What are general IT controls? [ISA | 1353.1300]

General IT controls (GITCs) are control activities over the entity's IT processes that support the continued effective operation of the IT environment, including:

- the continued effective operation of automated controls, and
- the integrity of data and information within the entity's IT system.

The IT processes are the entity's processes to manage access to programs and data, manage program changes, manage program acquisition and development, and manage computer operations (see activity '[Understand the entity's IT processes](#)' for more information).

The IT environment encompasses the IT systems the entity uses as part of its financial reporting and business processes, including its layers of technology (application, database, operating system and network), the IT processes and the IT organization (see activity '[Understand how the entity uses IT as part of financial reporting](#)' for more information).

GITCs are not expected to directly prevent, or detect and correct, material misstatements on a timely basis, but ineffective GITCs may lead to automated controls that don't operate consistently and effectively, and therefore might not prevent, or detect and correct, a material misstatement on a timely basis.

How are GITCs different from automated process control activities? [ISA | 1353.10549]

	Automated process control activities	GITCs
Purpose	Address process risk points (PRPs).	<p>Address risks arising from IT (RAFITs).</p> <p>Support the continued effective operation of the IT environment, including:</p> <ul style="list-style-type: none"> • the continued effective operation of automated controls, and <p>the integrity of data and information within the entity's IT system.</p>
Identified	When obtaining an understanding of the business processes and we intend to evaluate the design and implementation.	<p>After identifying automated controls and relevant layers of technology and RAFITs.</p> <p>When, as part of testing management's controls over the completeness and accuracy of</p>

	internal information data integrity risks are addressed by GITCs.
--	---

When we determine whether a control activity is an automated process control activity or a GITC, it is helpful to think about whether the control activity directly mitigates a PRP and an identified risk of material misstatement (RMM).

For example, consider a process control activity related to the individuals who have access to create journal entries in an entity's IT system. This directly addresses a PRP related to the creation of fraudulent journal entries.

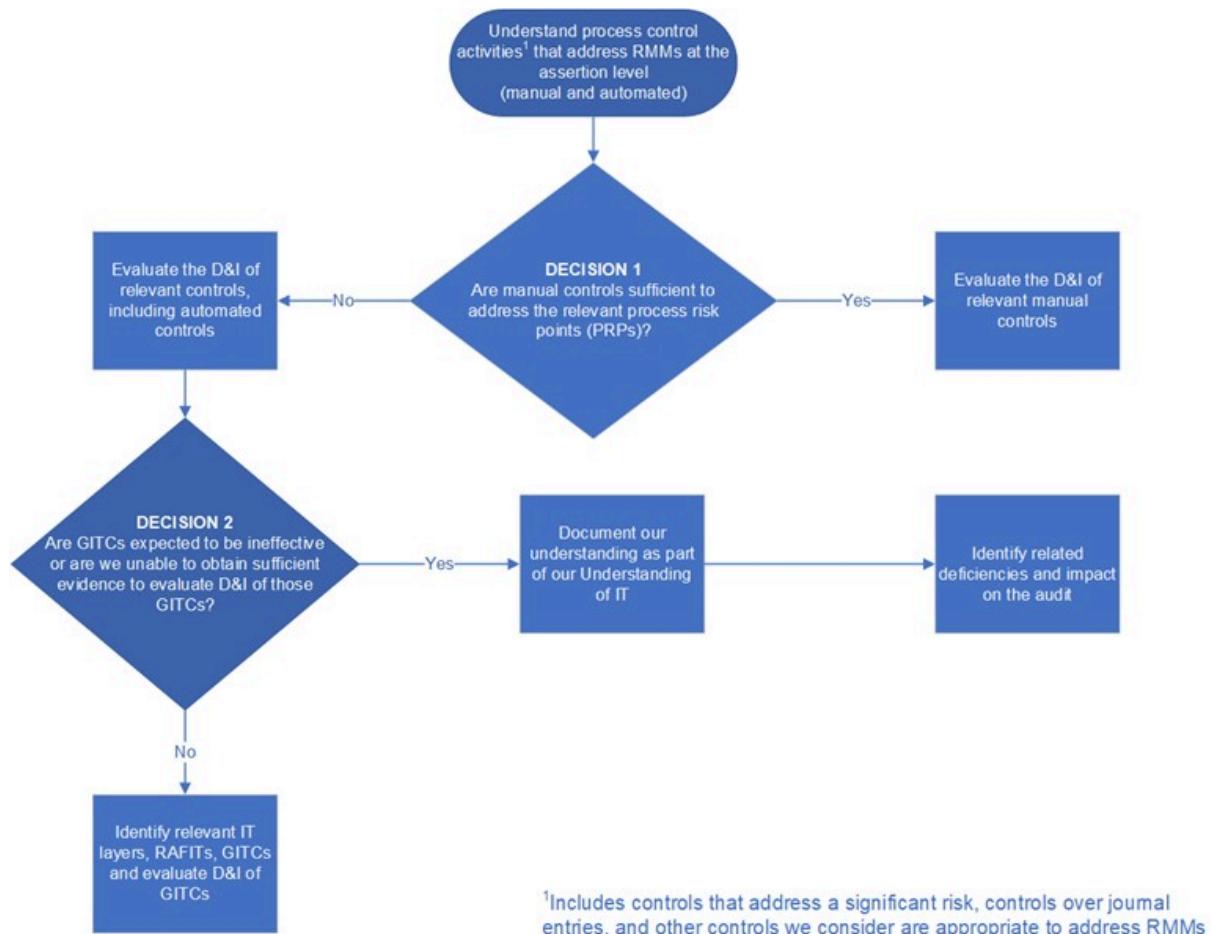
Alternatively, consider a GITC related to the creation of new users and modifications to user permissions within the IT application layer. This supports the effective operation of an automated process control activity that addresses a PRP related to the creation of fraudulent journal entries.

[Under what circumstances do we evaluate the design and implementation of GITCs?](#) [ISA | 1353.1500]

We identify and evaluate the design and implementation of GITCs where we have identified relevant layers of technology and RAFITs (see question '[Under what circumstances do we identify relevant layers of technology and RAFITs?](#)'). In our methodology we name these GITCs as 'relevant GITCs'. In practice, this means that we identify and evaluate the design and implementation of GITCs that:

- support the effective operation of automated control activities, when we:
 - plan to rely on and test the operating effectiveness of those automated control activities, or
 - evaluate the design and implementation of automated control activities, even though we do not plan to test their operating effectiveness (e.g., when we evaluate the design and implementation of an automated process control activity that addresses a significant risk or over journal entries). However, when GITCs are a) informal and, therefore, unable to be evaluated for design and implementation or b) expected to be ineffective (i.e. resulting in a control deficiency), we may document our understanding of relevant layers of technology, RAFITs and GITCs in summary as part of our understanding of the IT environment rather than identifying the individual layers of technology, RAFITS and GITCs for each automated control activity; or
- address the RAFIT(s) identified for the applicable IT system layer (e.g., database) related to data integrity risk, when we are testing management's controls over the accuracy and completeness of internal information to evaluate the reliability of such information (see question '[Are there specific risks that we consider when testing management's controls over internal information?](#)' for more information on audit considerations regarding data integrity risks).

The following decision tree provides an illustration of the decisions to be made and the implications with regards to evaluating the design and implementation of GITCs in the scenario where we evaluate the design and implementation of control activities but we do not plan to test their operating effectiveness:



How may we document our understanding of relevant layers of technology, RAFITs and GITCs in summary as part of our understanding of the IT environment? [ISA | 1353.8899]

When we evaluate the design and implementation of automated control activities but we do not plan to test their operating effectiveness, and GITCs are a) informal and, therefore, unable to be evaluated for design and implementation or b) expected to be ineffective (i.e. resulting in a control deficiency), we may document our understanding of relevant layers of technology, RAFITs and GITCs in summary as part of our understanding of the entity's IT processes within our understanding of the IT environment.

For example, consider an entity with the following circumstances:

- Has a less complex IT environment
- Uses System A, a single commercial accounting software application
- GITCs are not always formalized and documented
- We identified GITC deficiencies in the previous audit
- We have evaluated the design and implementation of an automated control that addresses a significant risk, but we do not plan to rely on the operating effectiveness of that control

Our understanding of the entity's IT processes may include the following:

IT process	Description

Access to programs and data	<p>The IT Manager and the Accounting Manager (as a backup) have security administrative responsibility to administer access to the system. The prior year deficiency related to the privileged access GITC was not remediated in the current year¹. RAFITs related to access to programs and data in system A are considered relevant to automated controls and they are addressed by the following steps in the process.</p> <p>The process to provision access is initiated when the Accounting department identifies a new user that needs access. Generally, the Accounting Manager sends a request either verbally or via email to the IT Manager requesting a new user account. The emails are not always retained².</p> <p>The user is required to change the password upon initial logon. The entity has password rules in place for minimum password length, password expiration, and complexity requirements.</p> <p>The process to de-provision access occurs when the IT Manager is notified of an employee resignation or termination. Upon notification of termination, the IT Manager will revoke the terminated employees' access. The IT Manager indicated that he does not always retain documentation to evidence the timely removal of access².</p> <p>There is no data processing center, as the system is maintained on the cloud.</p>
<p>Footnotes</p> <p>¹ KPMG identifies this as a deficiency</p> <p>² Since the entity has a less complex IT environment and uses a single commercial accounting software application, GITCs may not always be formalized and documented, which in this case is considered appropriate for the size and complexity of the entity and its IT environment.</p>	

Remember: When documenting our understanding of IT processes, we obtain an understanding for all four IT processes even if we identify a deficiency in one process. In this example, only one row was completed to illustrate example documentation when a deficiency is identified.

How do we evaluate the design and implementation of GITCs? [ISA | 1353.1505]

We evaluate the design and implementation of GITCs through inquiry in combination with observation and/or inspection.

Determining whether a GITC has been designed effectively means determining if the GITC satisfies the company's control objectives by addressing the RAFIT(s) it is intended to address.

Determining whether a GITC has been implemented means determining whether the GITC exists and whether the entity is using it.

What do we consider when we evaluate the design and implementation of a GITC? [ISA | 1353.8662]

We evaluate the design and implementation of a GITC considering the same items as when we evaluate the design and implementation of a process control activity, except for:

- anti-fraud control, and
- level of precision.

Given the different characteristics of GITCs and how they function, those characteristics aren't relevant to our evaluation. Remember that a GITC's objective is different from a process control activity's objective, specifically:

- The objective of GITCs is to address RAFITs, whereas
- The objective of process control activities is to mitigate PRPs to prevent, or detect and correct, material misstatements in the entity's financial statements.

[How do we determine whether the design of a GITC achieves its objectives?](#) [ISA | 1353.1600]

A GITC achieves its control objective when it adequately addresses each RAFIT it is designed to address.

To evaluate whether a GITC addresses each RAFIT it is intended to address, we understand how the GITC is performed, which means identifying control attributes. Control attributes are the specific procedures performed by the control operator (an individual or person for manual controls or IT systems for automated controls) that make-up the GITC and that are relevant to the design of the control.

Another way of thinking about control attributes is that they are the specific elements that are necessary for the GITC to be designed, implemented, and operating effectively. For example, if determining whether access to IT systems has been approved by an appropriate individual based on a pre-determined list is a necessary part of how a RAFIT is addressed, then that's a control attribute. If providing access within a certain number of days has no bearing on whether a RAFIT is addressed, then that is not a control attribute. The table below shows example control attributes for an example GITC.

RAFIT	GITC Description	Example Control Attributes - How the GITC is performed
1.2 APD - Logical access permissions (new or modified) are granted to users and accounts (including shared or generic accounts) that are inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	Management approves the nature and extent of user access permissions for new and modified user access in ABC system.	Control operator determines requests for new ABC system access or modification to existing ABC system access, are approved by an authorized user commensurate with the entity's IT delegation of authority.
		Control operator compares the permissions requested in the form/ticket to the entity's approved security profiles or roles by job function.
		Control operator determines that the access provisioned is consistent with access requested and approved.

[Can there be common GITCs across multiple layers of technology? \[ISA | 1353.8663\]](#)

Yes, an entity may use common IT processes across its IT environment or across certain layers of technology, in which case common RAFITs and common GITCs may be identified.

[Are there additional considerations when GITCs exist across multiple layers of technology? \[ISA | 1353.8664\]](#)

Yes, when manual GITCs exist across multiple layers of technology, we consider the shared characteristics to determine whether the GITCs are designed and implemented to operate consistently.

When manual GITCs are designed and implemented to operate consistently across multiple layers of technology, we may test the operating effectiveness of those GITCs to address the relevant RAFITs by using the common approach.

[What shared characteristics indicate a GITC operates consistently across multiple layers of technology? \[ISA | 1353.8665\]](#)

When manual GITCs exist across multiple IT systems and/or layers of technology, we consider the following characteristics to determine that the GITCs are designed and implemented to operate consistently:

Characteristics	Description
Same policies, practices, and procedures	Standard policies, practices, and procedures are followed by the control operators when performing the GITCs and any tools used in the performance of the control are the same
Same type of information used in the performance of the control	Information used by the control operators in the performance of the control is same type of information (e.g., the relevant data elements are the same and the information is generated in the same manner).
Subject to same monitoring activities	Monitoring activities are performed consistently across to monitor internal controls. Refer to activity ' Understand and evaluate monitoring activities ' for guidance.

[What is the common approach to testing the operating effectiveness of manual GITCs? \[ISA | 1353.8666\]](#)

The common approach is summarized below.

Guidance	Common approach
Applicability	Applies to manual GITCs that are designed to operate consistently across multiple layers of technology. Refer to the question 'What shared characteristics indicate a GITC operates consistently across multiple layers of technology?' for guidance.

Population	Single population across all relevant layers of technology. The completeness of the population is important in supporting GITC conclusions; therefore we do not exclude relevant IT systems and/or layers of technology nor do we include non-relevant layers of technology.
Sample size	Follow the guidance in activity ' Determine the control sample size ' .
Deficiencies	Any deviations in GITCs are considered control deficiencies. The deficiencies apply to all layers of technology in the population. It is not appropriate to isolate deficiencies to a single layer of technology when reaching a conclusion.
Conclusions	GITC conclusions apply to all relevant layers of technology included in the population.

Automated GITCs may also be designed to operate consistently across multiple layers of technology; however the testing approach is the same for all automated GITCs whether they operate over one or more layers.

How does an ineffective GITC affect our audit? [ISA | 1353.1700]

If we determine that a GITC is ineffective in its design and/or implementation (see activity '[Determine whether a deficiency in ICFR exists and describe it](#)' for more information), we:

- conclude that there is a deficiency;
- do not plan to rely on or test the operating effectiveness of that GITC.; and
- consider the effect of that deficiency on the automated controls it supports or the integrity of data used in the audit (for example, if the deficient GITC supports a process control activity, it may affect our planned audit response to an identified RMM and our assessment of CAR related to an identified RMM).

See activity '[In response to GITC deficiencies, test other GITCs, perform procedures or conclude on related automated control\(s\) and/or reliability of data within the IT system](#)' for more information on how to respond to GITC deficiencies.

Although GITC deficiencies, on their own, do not directly cause financial statement misstatements, deficient GITCs may render an automated control ineffective or the data within an IT system not reliable, and this may lead to financial statement misstatements that could be material. The significance of a GITC deficiency relates to its impact on the effectiveness of automated controls and/or integrity of data within an IT system.

Examples

How do we support our conclusion that a GITC operates consistently across multiple layers of technology? [ISA | 1353.8674]

Fact pattern

The entity has 3 relevant IT systems. Based on the engagement team's understanding of the relevant business processes, automated process control activities were identified as relevant in each of the three relevant IT systems. The following GITC was identified to address relevant RAFTs in each of the IT systems:

PC2-1: Changes to IT system programs are tested and approved prior to implementation into the production environment.

Additional information:

- The layers of technology relevant to the automated process control activities include the application and database layers.
- Following are the relevant IT systems:
 - System 1: SAP application; SQL server database
 - System 2: Oracle application; Oracle database
 - System 3: Hyperion Financial Management (HFM); SQL server database
- Based on the engagement team's understanding of IT:
 - The IT department is comprised of application development groups that support each of the IT systems - one group supports SAP; one group supports Oracle and one group supports HFM. There is one group that supports all databases.
 - The IT department follows the same program change policies, practices and procedures for all applications
 - The IT department uses the same change management ticketing tool, ServiceNow, to initiate change requests, evidence testing, track changes, and obtain approvals.
 - The control owners indicate the GITC is designed and implemented to operate consistently across all three IT systems and layers of technology.

Analysis

To evaluate the design of the GITC, the engagement team:

- Inquired of the control owners for SAP, Oracle, HFM, and databases to confirm they all follow the same change management process.
- Inspected the change management policies and procedures to determine the requirements for testing system program changes and the required approvals to indicate that testing was successful and applies to ALL relevant layers of technology
- Inspected the change management ticketing tool, ServiceNow configuration (e.g., drop-down list) that shows that all relevant layers of technology are listed.

[How do we determine the population using the common approach?](#) [ISA | 1353.8675]

Fact pattern

An entity has 10 IT systems but only 3 IT systems (systems A, B, and C) are relevant to the audit. Based on the engagement team's understanding of the relevant business processes, 3 automated process control activities were identified as relevant:

- One implemented in system A with the following RAFT: PC1 in SAP and PC 1 in SQL (SAP)
- One implemented in system B with the following RAFT: PC1 in Oracle financials and PC1 in Oracle DB

- One implemented in system C with the following RAFIT: PC1 in Hyperion and PC1 in SQL(Hyperion)

These six layers are therefore all relevant.

The engagement team identifies one GITC to address all six relevant program changes RAFITs.

Based on inquiry and inspection, it was noted that the GITC is designed and implemented to operate consistently across all the entity's relevant layers.

Management provides a listing of 3,750 changes; however, 750 changes are for layers that do not relate to any of the six layers.

The RAWTC for all three automated process control activities was assessed as base and the RAWTC for the GITC was assessed as base.

Analysis

The relevant population of program changes is 3,000. The 750 changes for systems that are not relevant to the audit are excluded from the population from which samples are selected to test the program change control.

The engagement team selects a sample of 25 operations from the population haphazardly. Provided the selection is random or haphazard, the selection does not have to include controls operations for each of the six layers although in this example it is likely to.

1.5 Understand relevant control activities that address significant risks [ISA | 576]

What do we do?

IF we determine that a significant risk, including a fraud risk, exists, THEN obtain an understanding of the relevant control activities that are intended to address the risks, by evaluating the design and implementation of those controls

Why do we do this?

As part of our risk assessment procedures, we obtain an understanding of a process to help us identify risks of material misstatement (RMMs). When we have a significant risk, including a fraud risk, we go even further, and evaluate the design and implementation of relevant control activities. This helps us better understand the risk, and informs our overall assessment of significant risks and how best to respond to them.

Execute the Audit

How do we identify relevant control activities that address a significant risk? [ISA | 576.1400]

We identify relevant control activities that address a significant risk by:

- understanding ICFR, including the entity's processes and CERAMIC;
- identifying all the process risk points related to the significant risk;

- identifying and obtaining an understanding of the control activities that address the relevant process risk points and risks arising from IT.

Not all control activities related to a significant risk may be relevant. Relevant control activities are those that address the PRP/RAFITs related to an RMM.

[How do we identify controls that address fraud risks?](#) [ISA | 576.1500]

All fraud risks are significant risks, so we identify relevant control activities that address fraud risks in the same manner as all other significant risks.

We describe process control activities that address process risk points related to a fraud risk as anti-fraud controls. There are specific considerations about the nature, timing and extent of audit procedures we design and perform to test anti-fraud controls.

A process control activity is an anti-fraud control when:

- we have identified a fraud risk at the assertion level or financial statement level; and
- that process control activity directly mitigates the identified fraud risk, either individually or when combined with other controls.

[Can anti-fraud controls also address a risk of error?](#) [ISA | 576.11815]

Yes. Some process control activities are designed to address the risk of fraud (anti-fraud controls) and the risk of error simultaneously.

An example of this might relate to an estimate that:

- has a high degree of judgment (risk of error); and
- creates an opportunity for management to intentionally manipulate assumptions to achieve a desired result (risk of fraud).

Management may implement process control activities that address risks related to determining the key assumptions, and evaluating the potential for management bias in selecting those assumptions. If so, the identified control may respond to the fraud risk and the risk of error for the estimate.

[What if control activities are not designed and implemented for significant risks?](#) [ISA | 576.2000]

Failure of the design or implementation of control activities addressing a significant risk is a deficiency in internal control and may indicate a significant deficiency. We evaluate deficiencies like this, and communicate them, as appropriate — even if we're performing a financial statement audit in which we do not intend to test the operating effectiveness of such control activities.

Examples

[How may anti-fraud controls be designed to address the risk of management override for an accounting estimate?](#) [ISA | 576.11816]

Fact pattern:

An entity prepares a cash flow forecast to support its going concern assessment. The Financial Controller prepares the forecast and the CFO reviews it.

During the engagement team's fraud planning meeting — i.e. the RAPD — they identified incentives, opportunities and rationalizations that caused them to identify a fraud risk associated

with the going concern disclosures. The team determined it may be easy for the CFO to tweak the revenue or expenses in the forecast, so that the entity's cash appeared sufficient for the relevant assessment period required by the financial reporting framework.

The entity has introduced a process control activity that is an anti-fraud control to address the risk of management override, whereby the board — i.e. those charged with governance — review the components of the going concern assessment. The board receive an analysis of each estimate used in the forecast, including:

- the range of reasonableness of each estimate;
- how that range was determined;
- how the range compares to prior periods; and
- where within the range management's estimate fell in this period compared to prior periods.

The board also receive an analysis of how the estimates as a whole affected earnings.

Analysis:

In this case, the review of each estimate by those charged with governance is an anti-fraud control designed to mitigate the risk of management bias in the estimates.

Bias may be evident in management's changes to:

- how the range of reasonable results is determined;
- where within that range their estimate falls (at the lower end, in the middle, or at the higher end); and
- how the relative placement of the point estimate changed period over period.

As this example illustrates, process control activities that are anti-fraud controls addressing the risk of management override in estimates can involve the board or audit committee. In many cases, estimates are reviewed by senior management — but that's where the risk of fraud due to management override lies. Involving the board in the review of certain assumptions can be an effective way for an entity to introduce anti-fraud controls.

1.6 Evaluate the design and implementation of process control activities over journal entries and other adjustments [ISA | 798]

What do we do?

Evaluate the design and implementation of the entity's process control activities over journal entries and other adjustments.

Why do we do this?

We identify and evaluate the design and implementation of process control activities over journal entries with a double objective:

- as part of our procedures to address the risk of management override of controls through the recording of journal entries, and
- as part of our risk assessment procedures, to address any risk identified that journal entries are susceptible of unauthorized or inappropriate intervention or manipulation due to error.

Execute the Audit

What are journal entries? [ISA | 798.1300]

Journal entries are any entries made directly within the general ledger system that are used to record transactions, allocations, adjustments and corrections. They include:

- standard journal entries used to record recurring transactions and adjustments; and
- non-standard journal entries used to record non-recurring, unusual transactions, or adjustments.

What are standard journal entries? [ISA | 798.13373]

Standard journal entries are journal entries used to record:

- recurring transactions - e.g., the day to day activities of the entity such as recurring sales, purchases, and cash disbursements; and
- recurring adjustments - e.g., adjustments related to accounting estimates that are made at each period-end such as changes in the estimate of uncollectible accounts receivable.

What are automated journal entries? [ISA | 798.13374]

Automated journal entries are standard journal entries that are automatically initiated, authorized, recorded and processed in the general ledger. The use of automated journal entries can reduce the risk of management override of controls because automated journal entries are less likely to be susceptible to unauthorized or inappropriate intervention or manipulation.

What are non-standard journal entries? [ISA | 798.13375]

Non-standard journal entries are journal entries used to record:

- non-recurring or unusual transactions - e.g., business combinations or disposals; and
- non-recurring adjustments - e.g., adjustments related to accounting estimates that are typically not made at each period-end such as the impairment of an asset.

The process and procedures used to record non-standard journal entries are typically manual journal entries.

What are manual journal entries? [ISA | 798.13376]

Manual journal entries are journal entries that are initiated by an individual and manually entered into the general ledger system. The use of manual journal entries can increase the risk of management override of controls because manual journal entries are more likely to be susceptible to unauthorized or inappropriate intervention or manipulation.

What are other adjustments? [ISA | 798.13378]

Other adjustments are adjustments made to the general ledger accounts outside of the general ledger system to determine the amounts presented on the face of the financial statements. Entities often use a spreadsheet to support other adjustments. Other times, entities may make other adjustments

directly in the financial statements or disclosures themselves. Other adjustments are most often seen in period-end financial reporting through post-closing adjustments.

Similar to manual journal entries, the use of other adjustments can increase the risk of management override of controls because there is more opportunity for manual intervention in the process and procedures.

How do we evaluate the design and implementation of process control activities over journal entries and other adjustments? [ISA | 798.1301]

We evaluate the design and implementation of process control activities over journal entries and other adjustments through inquiry in combination with observation and/or inspection, in the same way we evaluate the design and implementation of other relevant process control activities (refer to activity '[Evaluate the design and implementation of relevant process control activities](#)' for more information).

In what circumstances do we evaluate the design and implementation of process control activities over journal entries and other adjustments? [ISA | 798.157909]

We identify and evaluate the design and implementation of process control activities over journal entries and other adjustments that are relied on by management that sufficiently address:

- the risk of management override of controls; and, if identified,
- the risk that journal entries are susceptible to unauthorized or inappropriate intervention or manipulation due to error.

How do we address the risk that journal entries are susceptible to unauthorized or inappropriate intervention or manipulation due to fraud? [ISA | 798.157910]

The risk that journal entries are susceptible to unauthorized or inappropriate intervention or manipulation due to fraud is addressed as part of our response to the risk of management override of controls.

What is the difference between the risk of management override of controls through journal entries and the risk of unauthorized or inappropriate intervention or manipulation of journal entries and how we address these risks? [ISA | 798.157911]

The difference between the risk of management override of controls through journal entries and the risk of unauthorized or inappropriate intervention or manipulation of journal entries and how we address these risks is shown in the table below:

Risk	Characteristics	Risk addressed by
Management override of controls through journal entries	Fraud risk (i.e., significant risk) present in all entities, although the level of risk may vary from entity to entity	Testing the appropriateness of journal entries and other adjustments, which includes evaluating the design and implementation of process control activities over journal entries and other adjustments

Unauthorized or inappropriate intervention or manipulation of journal entries	<p>Presumed to be a fraud risk since the unauthorized or inappropriate intervention or manipulation of journal entries will derive from an intentional act in most cases.</p> <p>However, in certain cases, we may determine that the risk also derives from an unintentional act and therefore be considered a risk due to error.</p>	<p>Addressing the fraud risk as part of our response to the risk of management override of controls.</p> <p>If we determine there is also a risk due to error, we:</p> <ul style="list-style-type: none"> • determine whether there is a risk of material misstatement at the assertion level and, if there is, we • identify and evaluate the design and implementation of process control activities over journal entries that address the risk due to error. <p>We also take this into account in our substantive procedures to select and test high-risk journal entries that address both the risk of management override of controls and the risk that journal entries are susceptible to unauthorized or inappropriate intervention or manipulation due to error, for example, we may consider unusual account combinations when determining the high-risk criteria.</p>
---	--	---

What journal entries may be susceptible to unauthorized or inappropriate intervention or manipulation?

[ISA | 798.157922]

These journal entries include:

- non-standard journal entries, where the journal entries are automated or manual and are used to record non-recurring, unusual transactions or adjustments;
- standard journal entries, where the journal entries are automated or manual and are susceptible to unauthorized or inappropriate intervention or manipulation.

Due to their nature, non-standard journal entries are typically manual journal entries and, therefore, more likely to be susceptible to unauthorized or inappropriate intervention or manipulation.

Standard journal entries can be used to record:

- recurring transactions (e.g., daily routine sales)

In this case, in today's environment where there are significant automated processes, these standard journal entries are typically automated journal entries and therefore less likely to be susceptible to unauthorized or inappropriate intervention or manipulation.

In particular, for system-generated journal entries that are directly and routinely processed to the general ledger, we may judgmentally determine that there is little or no susceptibility to unauthorized or inappropriate intervention or manipulation and therefore would not give rise to a risk of material misstatement and we would not identify controls over those journal entries to evaluate their D&I.

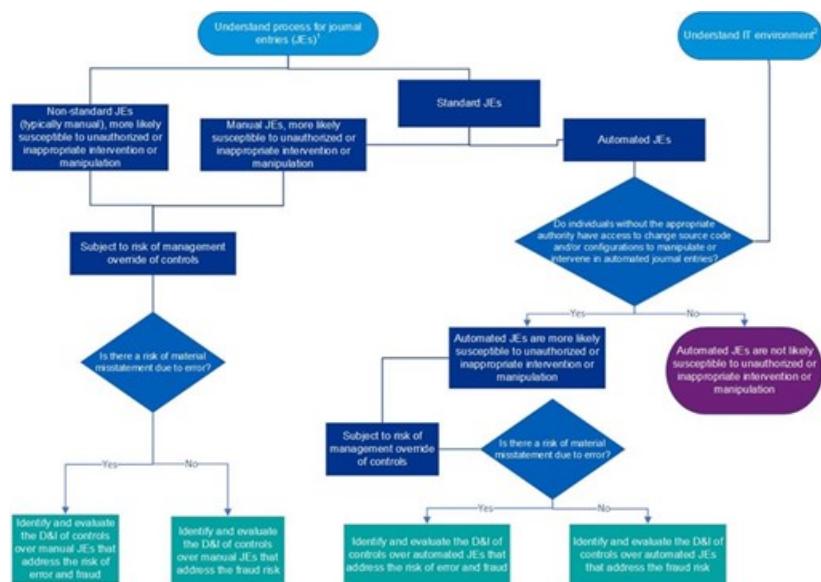
However, there could be other scenarios where a journal entry, although automated, could be manipulated. For example, if individuals without the appropriate authority have access to the source code or are able to make inappropriate changes to configurations.

See questions "[What is an example scenario that indicates likely susceptibility versus little to no susceptibility to unauthorized or inappropriate intervention or manipulation of automated journal entries?](#)" and "[What do we do when it is not clear whether automated journal entries are susceptible to unauthorized or inappropriate intervention or manipulation?](#)" for more information on automated journal entries that could be susceptible to unauthorized or inappropriate intervention or manipulation.

- recurring adjustments (e.g., adjustments related to accounting estimates that are made at each period-end such as changes in the estimate of uncollectible accounts receivable).

In this case, these standard journal entries are more likely to be manual journal entries and therefore more likely to be susceptible to unauthorized or inappropriate intervention or manipulation

The following diagram depicts the process we follow to determine the journal entries that could be susceptible to unauthorized or inappropriate intervention or manipulation and how we address any related risk of material misstatement identified:



¹ This includes understanding the types of journal entries, i.e. standard and non-standard, manual and automated. See activity "Understand processes and procedures for journal entries and other adjustments" [797] for further guidance.

² This includes understanding the IT process to manage changes. See activity "Understand IT processes" [7842] for further guidance.

For guidance on the decisions to be made regarding what controls over journal entries to identify when we do not plan to test their operating effectiveness, refer to the decision tree in the question "[How do we identify process control activities over journal entries and other adjustments over which to evaluate their design and implementation?](#)".

[What is an example scenario that indicates likely susceptibility versus little to no susceptibility to unauthorized or inappropriate intervention or manipulation of automated journal entries?](#) [ISA | 798.157942]

The table below shows an example scenario that indicates likely susceptibility versus little to no susceptibility to unauthorized or inappropriate intervention or manipulation of automated journal entries:

Factor	Likely susceptibility	Little to no susceptibility
Type of general ledger IT system	Entity uses a custom in-house built system or a highly customized ERP system.	Entity uses a standard off the shelf general ledger IT system.
Access to source code/system configuration	Individuals within the entity without the appropriate authority have access to the general ledger IT system's source code.	Individuals within the entity do not have access to the general ledger IT system source code and the entity does not have the ability to change system configurations related to how journal entries are posted to general ledger IT system (i.e., access to configurations or source code to change how journal entry general ledger accounts, dates, amounts, journal entry type are recorded in the general ledger).

When there is likely susceptibility to unauthorized or inappropriate intervention or manipulation of automated journal entries, we identify and evaluate the design and implementation of process control activities over those automated journal entries. If the process control activities are automated, we also identify the relevant layers of technology, RAFITs and GITCs, and evaluate the D&I of GITCs that support the continued effective operation of those automated process control activities.

What do we do when it is not clear whether automated journal entries are susceptible to unauthorized or inappropriate intervention or manipulation? [ISA | 798.157943]

When it's not clear whether automated journal entries are susceptible to unauthorized or inappropriate intervention or manipulation, we take into account our understanding of the IT environment and business processes. We also think about the following questions to help us determine if automated journal entries are susceptible to unauthorized or inappropriate intervention or manipulation and therefore whether to identify and evaluate the design and implementation of process control activities over automated journal entries as well as relevant GITCs, if the process control activities identified are automated.

1. Does management have access to the general ledger IT system's source code? If yes:

- Who has access?

- Is access restricted to authorized personnel (e.g., only IT personnel have access and there is segregation of duties between IT and accounting)?
- Can the entity provide evidence of who has access to the source code?
- If those in the accounting department have access to the general ledger IT system source code, what are the controls in place to detect unauthorized changes to source code impacting journal entries?

2. Are there any system configurations that impact how journal entries are posted (i.e., how journal entry general ledger accounts, dates, amounts, journal entry type are recorded in the general ledger)? If yes:

- What are the configurations related to journal entries?
- Who has access to change the system configurations?
- Is access restricted to authorized personnel (e.g., only IT personnel have access and there is segregation of duties between IT and accounting)?
- Can the entity provide evidence of who has access to the system configurations?
- What controls over system configurations related to journal entries are in place?

For examples as to how these questions we think about would impact our audit approach, refer to the question "[How might an entity's responses to the questions we think about to identify when automated journal entries may be susceptible to unauthorized or inappropriate intervention or manipulation, impact our audit approach?](#)".

[How do we identify process control activities over journal entries and other adjustments over which to evaluate their design and implementation? \[ISA | 798.9409\]](#)

When understanding the entity's financial reporting process, we use the knowledge obtained to identify, at a minimum, process risk points (PRPs) where management override of controls could occur through the recording of journal entries and other adjustments. Additionally, we consider whether there are any additional PRPs related to the risk associated with journal entries that could be susceptible to unauthorized or inappropriate intervention or manipulation.

When understanding the entity's business processes, we specifically understand how the transactions are initiated, and how information about them is recorded, processed, corrected as necessary, incorporated in the general ledger and reported in the financial statements. In obtaining this understanding, we obtain knowledge about how transactions and events are processed, and therefore we may identify journal entries that could be susceptible to unauthorized or inappropriate intervention or manipulation and PRPs related to those journal entries. Additionally, when we take a controls-based approach to respond to RMMs related to the recording of transactions and events in the business process, we may identify PRPs related to the recording of those transactions in the general ledger through journal entries.

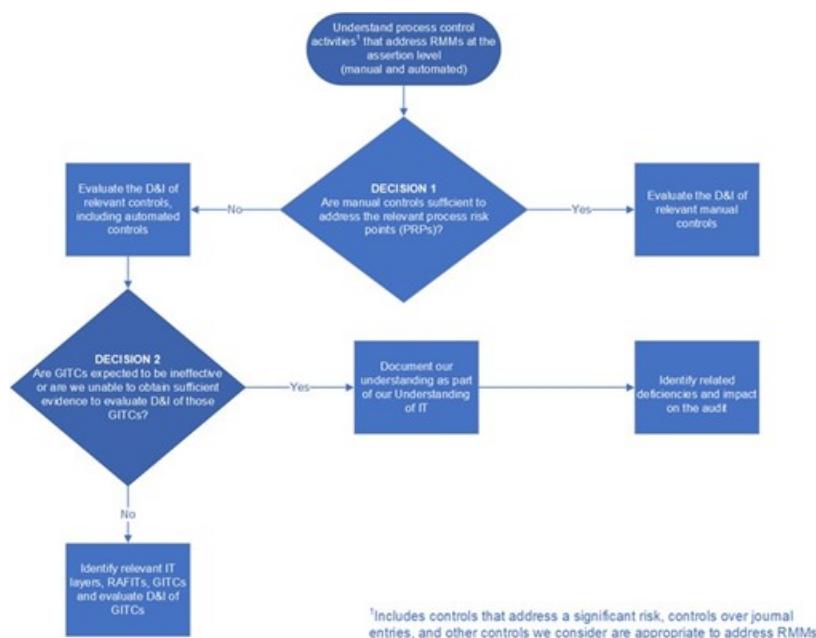
For each PRP identified, we obtain an understanding of the process control activities that are relied on by management to address the PRP.

Most entities maintain their general ledger in an application and posting of journal entries is at least in part performed automatically, so it is likely that control activities over journal entries will include automated controls over the posting of journal entries to the general ledger. However, that does not mean we identify those automated controls as process control activities over journal entries that we will evaluate design and implementation of to address the risk of management override of controls

and/or to address the risk associated with journal entries that could be susceptible to unauthorized or inappropriate intervention or manipulation. For example, entity management may implement manual controls over the automated posting of journal entries or a review process over manual journal entries such that they do not rely on the automated processing of journal entries to address the risk of management override of controls and/or to address the risk associated with journal entries that could be susceptible to unauthorized or inappropriate intervention or manipulation due to error.

In cases where management relies on automated controls to address the risk of management override of controls through journal entries or the risk associated with journal entries that could be susceptible to unauthorized or inappropriate intervention or manipulation, we evaluate the design and implementation of those automated controls, we also identify relevant IT layers, RAFITs and evaluate the design and implementation of general IT controls that support the continued effective operation of those automated controls.

The following decision tree provides an illustration of the decisions to be made and the implications when we evaluate the design and implementation of process control activities but we do not plan to test their operating effectiveness, including controls over journal entries and other adjustments (see question "[Under what circumstances do we evaluate the design and implementation of GITCs](#)" for more information on decision 2 of the decision tree below):



[What are some examples of process control activities over journal entries and other adjustments?](#) [ISA | 798.13524]

Examples of process control activities that may reduce the risk of management override of controls or the risk that journal entries are susceptible to unauthorized or inappropriate intervention or manipulation are:

- the CFO or CEO are prevented from initiating, processing or authorizing journal entries within the IT system;
- objective oversight by personnel independent from the journal entry process reviewing journal entries and supporting documentation;

- all journal entries and supporting documentation are reviewed and approved by an individual separate from the individual posting the journal entry;
- a control exists that prevents the reviewer of a journal entry from posting it.
- accounting manager that neither prepares, reviews nor posts journal entries reviews all manual journal entries posted during the period to the general ledger. If a threshold is applied to this review, the magnitude of those entries not subject to review does not have a risk of material misstatement.
- reconciliation of balance sheet and income statement accounts by an accounting manager that neither prepares, reviews nor posts journal entries by comparing two or more data elements and investigates reconciling items at an appropriate level of precision;
- automated process control activities over journal entries that limit privileged user access to the system to one or two senior IT staff. Only staff with privileged access have the ability to change automated journal entries based on the design of the IT systems or no staff have the ability to change automated journal entries;
- automated control activities that prevent changes in relevant information after a journal entry has been posted, such as preventing management from changing the identity of the person posting a journal entry.

The last two bullets are examples of effective control activities that could suggest that automated journal entries are not a characteristic of high risk journal entries.

[Core and Less Complex | What is an additional example of process control activities over journal entries and other adjustments in a less-complex entity? \[ISA | 798.8909\]](#)

An additional example of process control activities that may reduce the risk of management override of controls or the risk that journal entries are susceptible to unauthorized or inappropriate intervention or manipulation in a less-complex entity is:

- Where senior management are closely involved in the day to day operations, senior management review of financial information on a periodic basis to assess if it is in line with expectations, may be relied on and precise enough to identify material misstatements caused by incorrect journal entries.

[Do we evaluate the design and implementation of controls over journal entries and other adjustments for all audit engagements? \[ISA | 798.13525\]](#)

Yes, for all audit engagements we evaluate the design and implementation of process control activities over journal entries and other adjustments that sufficiently address the risk of management override of controls through the recording of journal entries and other adjustments, which is a fraud risk and thus, a significant risk. Therefore, we evaluate the design and implementation of an entity's process control activities over journal entries and other adjustments as part of our audit that respond to that risk even when we have not identified other controls relevant to our audit.

Additionally, we may identify process control activities that address the risk associated with journal entries that are susceptible to unauthorized or inappropriate intervention or manipulation.

For example, in an audit of a less complex entity, the entity's information system may not be complex and we may not plan to rely on the operating effectiveness of controls. Further, we may not have identified any significant risks or any other risks of material misstatement for which it is necessary for us to evaluate the design and implementation of controls. In such an audit, we may only evaluate the

design and implementation of control activities over journal entries and other adjustments that address the risk of management override of controls and, when relevant, the risk that journal entries could be susceptible to unauthorized or inappropriate intervention or manipulation due to error.

At what point in the audit do we evaluate the design and implementation of process control activities over journal entries and other adjustments? [ISA | 798.1700]

We evaluate the design and implementation of the entity's process control activities over journal entries and other adjustments as part of our risk assessment procedures - i.e., as part of the planning phase of the audit.

Do we test the operating effectiveness of process control activities over journal entries and other adjustments when we perform a financial statement audit? [ISA | 798.1800]

Not necessarily. We test the operating effectiveness of process control activities over journal entries and other adjustments when we plan to rely on the operating effectiveness of those controls as part of our response to a particular risk of material misstatement, including our approach to identifying and testing high risk journal entries

We may plan to rely on the operating effectiveness of process control activities over journal entries and other adjustments in order to reduce the extent of our testing of journal entries and other adjustments (e.g., when excluding automated journal entries from the population of journal entries that we apply high risk criteria to).

Examples

How might an entity's responses to the questions we think about to identify when automated journal entries may be susceptible to unauthorized or inappropriate intervention or manipulation, impact our audit approach? [ISA | 798.157925]

Fact pattern 1

Consider an entity that responds as follows:

Question	Example response
Is the general ledger IT system a custom in-house built system or a highly customized purchased general ledger IT system?	No. The general ledger IT system is a standard off the shelf system
Does management have access to the general ledger IT system's source code?	No. The entity uses an off-the-shelf accounting software. Source code is compiled, and management does not have access to it.
Are there any system configurations (i.e., access to configurations or source code to change how journal entry general ledger	No.

accounts, dates, amounts, journal entry type are recorded in the general ledger) that impact how journal entries are posted?

Analysis

Given:

- The entity uses a standard off the shelf general ledger IT system;
- Management does not have access to the source code, and
- There are no system configurations (i.e., access to configurations or source code to change how journal entry general ledger accounts, dates, amounts, journal entry type are recorded in the general ledger) that impact how the journal entries are posted,

the engagement team determines that automated journal entries are not likely susceptible to unauthorized or inappropriate intervention or manipulation and therefore the engagement team does not identify or evaluate the design and implementation of process control activities over automated journal entries.

Fact pattern 2

Consider an entity that responds as follows:

Question	Example response
Is the general ledger IT system a custom in-house built system or a highly customized purchased general ledger IT system?	Yes. The general ledger IT system is a custom in-house built system.
Does management have access to the general ledger IT system's source code?	Yes. IT management has access to the source code.
Is access restricted to authorized personnel (e.g., only IT personnel have access and there is segregation of duties between IT and accounting)?	Yes. Only personnel in the IT department with the appropriate authority in accordance with the entity's policies has access to the source code.
If those in the accounting department have access to the general ledger IT system, are there controls in place to detect unauthorized changes to source code impacting journal entries? If yes, describe the controls	N/A. The accounting department does not have access to the source code
Are there any system configurations (i.e., access to configurations or source code to change how journal entry general ledger	Yes. The system allows the ability to override how journal entry general ledger accounts and

accounts, dates, amounts, journal entry type are recorded in the general ledger) that impact how journal entries are posted?	journal entry type are recorded in the general ledger.
Who has access to change the system configurations?	Only personnel in the IT department with the appropriate authority in accordance with the entity's policies has access to change the system configurations.
Can the entity provide evidence of who has access to source code and system configurations?	Yes. Management provided a system generated report of users that have access to update source code and system configurations of the general ledger IT system. The engagement team confirmed the controller does not have access to modify source code or system configurations of the general ledger IT system.

Analysis

Given:

- The entity uses a custom in-house built general ledger IT system,
- Only personnel in the IT department with the appropriate authority in accordance with the entity's policies has access to the source code,
- Although the system allows the ability to override how journal entry general ledger accounts and journal entry type are recorded in the general ledger, only personnel in the IT department with the appropriate authority in accordance with the entity's policies has access to change the system configurations, and
- The engagement team obtained and inspected a system-generated report confirming that the controller did not have access to modify source code, system configurations, or journal entries,

the engagement team determines that automated journal entries are not likely susceptible to unauthorized or inappropriate intervention or manipulation and therefore the engagement team does not identify or evaluate the design and implementation of process control activities over automated journal entries.

Fact pattern 3

Consider an entity that responds as follows:

Question	Example response
Is the general ledger IT system a custom in-house built system or a highly customized purchased general ledger IT system?	Yes. The general ledger IT system is a custom in-house built system.

Does management have access to the general ledger IT system's source code?	Yes. IT management has access to the source code.
Is access restricted to authorized personnel (e.g., only IT personnel have access and there is segregation of duties between IT and accounting)?	Yes. Only personnel in the IT department with the appropriate authority in accordance with the entity's policies has access to the source code
If those in the accounting department have access to the general ledger IT system, are there controls in place to detect unauthorized changes to source code impacting journal entries? If yes, describe the controls	N/A. The accounting department does not have access to the source code
Are there any system configurations (i.e., access to configurations or source code to change how journal entry general ledger accounts, dates, amounts, journal entry type are recorded in the general ledger) that impact how journal entries are posted?	Yes. The system allows the ability to override how journal entry general ledger accounts and journal entry type are recorded in the general ledger
Who has access to change the system configurations?	An Accounting Analyst.
Is access restricted to authorized personnel (e.g., only IT personnel have access and there is segregation of duties between IT and accounting)?	No, since an Accounting Analyst has access.
Can the entity provide evidence of who has access to source code and system configurations?	Yes. Management provided a system generated report of users that have access to update source code and system configurations of the general ledger IT system. The engagement team confirmed the controller does not have access to modify source code or system configurations of the general ledger IT system
Are there manual controls in place over journal entries?	Yes. On a monthly basis, the controller reviews a report of journal entries.

<p>What automated process control activities does the entity have in place over journal entries?</p>	<p>The following automated process control activities are in place over the general ledger IT system:</p> <ul style="list-style-type: none"> - AC-1: The system is configured to appropriately post journal entries
--	--

Analysis

Given:

- The entity uses a custom in-house built general ledger IT system,
- Entity Management has access to the source code,
- The general ledger IT system has a system configuration that impacts how journal entries are posted (i.e., access to configurations or source code to change how journal entry general ledger accounts, dates, amounts, journal entry type are recorded in the general ledger) and the Accounting Analyst has access to change the configuration, and
- The engagement team obtained and inspected a system-generated report confirming that the controller did not have access to modify source code, system configurations, or journal entries,

the engagement team determines that journal entries are likely susceptible to unauthorized or inappropriate intervention or manipulation. Additionally, the engagement team determines that the manual process control activity of the controller reviewing a report of journal entries monthly relied on by management is performed at a sufficient level of precision to address the risk of journal entries being subject to unauthorized or inappropriate intervention or manipulation, even though there are also automated process control activities addressing such risk. Therefore, the engagement team evaluates the design and implementation of the manual process control activity only.

Fact pattern 4

Consider an entity that responds in the same way to the questions in Fact pattern 3 above, except that the response to the question "Are there manual controls in place over journal entries?" is that there are no manual controls.

Analysis

Given:

- The entity uses a custom in-house built general ledger IT system,
- The general ledger IT system has a system configuration (i.e., access to configurations or source code to change how journal entry general ledger accounts, dates, amounts, journal entry type are recorded in the general ledger) that impacts how journal entries are posted and the Accounting Analyst has access to change the configuration,
- There are no manual controls in place over journal entries, and
- The engagement team identified automated process control activities over journal entries,

the engagement team determines that journal entries are likely susceptible to unauthorized or inappropriate intervention or manipulation and there is no manual control in place over journal entries. Therefore, the engagement team identifies and evaluates the design and implementation of automated process control activities over journal entries and the relevant GITCs.

The engagement team identifies the following RAFITs relevant to the above automated process control activities and evaluates the design and implementation of the GITCs listed below.

RAFIT	GITC
1.4 APD - Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	Privileged-level access (e.g., configuration, data and security administrators) in the IT system is authorized and appropriately restricted.
2.1 PC - Changes to IT programs were inappropriate (i.e., unapproved or do not function as intended).	Changes to IT system programs are approved prior to implementation into the production environment.
2.2 PC - Changes to IT configurations were inappropriate (i.e., unapproved or do not function as intended).	Changes to IT system configurations are approved prior to implementation into the production environment.
2.3 PC - Logical access to implement changes to IT system program or configurations into the production environment is inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	Changes into the production environment, including configuration changes, are reviewed by IT management personnel to determine if they are appropriately authorized, restricted and segregated from the development environment.

1.7 Design procedures to test the application of control activities [ISA | 1356]

What do we do?

Understand how the entity deploys control activities and design procedures to test the application of control activities that we plan to rely on as part of our response to risks of material misstatement.

Why do we do this?

In order to address the risks of material misstatements (RMM), we design and perform audit procedures to obtain persuasive (sufficient and appropriate) audit evidence. Our planned audit procedures can consist of a substantive testing approach, which does not include tests of controls, or a controls approach, which includes both tests of controls and substantive tests. Although we may not always take a controls

approach in a financial statement audit, there will be situations where we may either choose to or be required to test controls.

Execute the Audit

What does deployment of control activities mean? [ISA | 1356.1500]

Deployment of control activities refers to the policies and procedures management has in place to consistently apply control activities.

Under what circumstances do we understand how the entity deploys control activities? [ISA | 1356.1600]

We understand how the entity deploys control activities only when we intend to test and rely on control activities to alter our substantive procedures or when we are performing an audit of internal control over financial reporting (ICFR).

What is a controls approach? [ISA | 1356.1700]

When we intend to test and rely on control activities to alter our substantive procedures, we obtain evidence that those control activities are operating effectively for the period we intend to rely on them. This is commonly referred to a controls approach. When we take a controls approach, we perform both the evaluation of design and implementation and the test of operating effectiveness to place reliance on the control activities.

We do not use the term 'controls approach' when we only evaluate the design and implementation of a control (e.g., when we are required to evaluate the design and implementation of controls over a significant risk.)

How do we understand how the entity deploys control activities? [ISA | 1356.1800]

We understand how the entity deploys control activities by testing the operating effectiveness of control activities.

What do we consider when we plan to test manual control activities? [ISA | 1356.12152]

When we plan to test the operating effectiveness of manual control activities, we design specific procedures to test the consistency in the application of those manual control activities each and every time the manual control activity is performed. Our sample tested for purposes of our evaluation of D&I may also be utilized as a sample for purposes of our test of operating effectiveness. For example, for a Base RAWTC manual control that occurs at a monthly frequency, one of the two required TOE samples may be the same sample utilized in our evaluation of D&I of that control.

What do we consider when we plan to test automated control activities? [ISA | 1356.12154]

When we plan to test the operating effectiveness of automated control activities, we have the following options:

- If we plan to test the operating effectiveness of related general IT controls, because of the inherent consistency of IT processing, we may use the same evidence obtained for evaluating the D&I of each relevant control attribute to conclude on the operating effectiveness of the automated control at a point in time. Note that the operating effectiveness of related general IT controls provides evidence that the automated control continues to operate effectively throughout the period; or

- If the GITCs are not effective or we choose not to test their operating effectiveness, in limited circumstances, we may be able to gain evidence over the effectiveness of automated process control activities by testing them at multiple points throughout the period in order to still have control reliance for the period (see activity '[Test automated controls throughout the period, if appropriate](#)' for further information including the circumstance when this is appropriate).

When we evaluate the design and implementation of an automated control activities, we identify relevant layers and RAFITs, and the GITCs that address those RAFITs. We evaluate the design and implementation of those GITCs that we identify regardless of whether we plan to test and rely on operating effectiveness of the automated control activities.

2 Test control activities when substantive procedures alone cannot provide sufficient audit evidence [ISA | 597]

What do we do?

IF substantive procedures alone cannot provide sufficient appropriate audit evidence, THEN test the operating effectiveness of control activities over those assessed risks of material misstatement

Why do we do this?

We test the operating effectiveness of controls over a risk of material misstatement (RMM) when we can't design substantive procedures capable of obtaining sufficient appropriate audit evidence on their own.

Execute the Audit

[When may we be unable to obtain sufficient appropriate audit evidence from substantive procedures alone?](#) [ISA | 597.1300]

We may not be able to obtain sufficient appropriate audit evidence from substantive procedures alone when a significant amount of information or data elements are electronically initiated, recorded, processed or reported. In this case, our ability to obtain sufficient appropriate audit evidence may depend on the entity's controls.

However, it is not necessary to test controls for every process with automated control activities or evidence in electronic form, except when the sufficiency and appropriateness of the substantive audit evidence depends on the entity's controls.

[What are examples of when substantive procedures alone may not provide sufficient appropriate audit evidence?](#) [ISA | 597.1400]

The following table sets out examples of situations in which performing substantive procedures alone may not provide sufficient appropriate audit evidence.

Scenario	Examples

<p>The entity's financial reporting and accounting information systems rely heavily on IT, with little or no manual intervention. The entity also relies on embedded, automated process control activities to prevent or detect and correct misstatements that may occur during the activities to initiate, process and record financial transactions, and to create its financial statements.</p>	<ul style="list-style-type: none"> • Customer orders are placed directly on the entity's system via the web, without a customer purchase order, contract or data file. • Customer agreements are signed online and maintained electronically in the entity's systems. • Approvals or document matching are performed online by the IT system with little or no manual intervention. • The entity runs an internet-based consumer marketplace that aggregates data about consumers and bills suppliers on a per click basis. It relies heavily on IT to deliver products and bill customers. • We have identified financial statement-level RMMs or significant risks arising from the use of IT.
<p>Important information may exist solely in electronic form. The entity uses an IT system to provide summarized information from many different IT systems to business process owners or management, and management rely on database information and/or system-generated reports to generate the financial statements.</p>	<ul style="list-style-type: none"> • Each day, a retail entity's IT systems gather store sales data from multiple IT systems. Only automated process control activities exist to ensure management receives complete store sales data and aggregated sales data by region. There is no manual intervention, and there are no manual controls. Data transferred between IT systems does not include individual transactions to allow management (or us) to trace back to the source transactions. • We seek to use the history of price markdowns to audit a retail entity's markdowns reserve. We can only get this information at a sufficiently granular level through reports from the entity's enterprise resource planning or point-of-sale system. Therefore, we test controls to obtain evidence over the accuracy of markdown information and the completeness and accuracy of the entity's report for use in our substantive procedures.
<p>The entity transacts electronically with third parties. Sales and purchases are automatically recorded between the entity and third parties, with little or no manual intervention.</p>	<ul style="list-style-type: none"> • An entity's customers buy software services direct from its website, with little or no manual intervention. The entity's recorded revenues are generated directly through these website sales. It receives daily sales summary reports but cannot trace individual transactions to their source. • An entity conducts much of its business with vendors or customers over the web — e.g. when the entity places an order, its IT system

	automatically sends the order information to the vendor. The IT system then automatically matches the receipt and makes payment without manual intervention.
The entity uses a model to develop complex accounting estimates using data comprised of many small balances resulting from a high volume of transactions.	<ul style="list-style-type: none"> • Data used in developing a complex expected credit loss provision for a financial institution or a utility entity.

What do we do if substantive procedures alone cannot provide sufficient appropriate audit evidence and the control activities related to the RMM are ineffective? [ISA | 597.8596]

If we assess control risk as no controls reliance for an RMM where we are unable to obtain sufficient appropriate audit evidence from substantive procedures alone, then we have a scope limitation for that RMM. We perform procedures in accordance with '[Modify the audit opinion for specific circumstances](#)'.

Example

When might substantive procedures alone not provide sufficient appropriate audit evidence? [ISA | 597.1500]

[Example 1 | Manufacturing entity](#) [ISA | 597.10976]

Fact pattern:

Entity A issues electronic purchase orders to its suppliers, and receives the related supplier invoices electronically. Entity A records the receipt of goods by scanning a supplier barcode on the received parcel. This initiates an automated process to match the purchase order price and quantity against the invoice price, quantity and barcode reference number.

The receipt is recorded in the inventory system, and the payable in the payables system. Both amounts are transferred to the general ledger. Given the automated nature of its process, Entity A does not retain hard copy receiving documents.

Analysis:

The process is highly automated and relies on evidence that only exists in electronic form — i.e. electronic invoices and purchase orders. Therefore, substantive procedures alone may not provide sufficient appropriate audit evidence.

As a result, the engagement team identify and test those automated process control activities and general IT controls that support the effective operation of these automated control activities. Otherwise, they may not obtain sufficient appropriate evidence in response to the identified risk.

[Example 2 | Bank](#) [ISA | 597.10977]

Fact pattern:

Bank J relies heavily on IT systems to process deposit transactions. These transactions are captured through various means, including branch tellers, automated clearing house (ACH) transactions, wire transfers, automated teller machines (ATMs), telephone, online banking and correspondent banks.

We have identified the following RMM:

Deposits are not recorded as liabilities at the time they are received by the entity.

As part of our substantive procedures to address this RMM, we plan to perform procedures over the daily deposit suspense/transit account reconciliations at period end.

Analysis:

The process is highly automated, and relies on evidence that only exists in electronic form — i.e. checks deposited in the bank, wire transfers, ACH transactions, ATMs, branch tellers. Therefore, substantive procedures alone may not provide sufficient appropriate audit evidence.

As a result, the engagement team identify and test those automated process control activities and general IT controls that support the effective operation of these automated control activities. Otherwise, they may not obtain sufficient appropriate evidence in response to the identified risk.

Control Deficiencies Within the Entity's System of Internal Control

International Standards on Auditing: ISA 315.27

Control Deficiencies Within the Entity's System of Internal Control

27. Based on the auditor's evaluation of each of the components of the entity's system of internal control, the auditor shall determine whether one or more control deficiencies have been identified. (Ref: Para. A182-A183)

ISA Application and Other Explanatory Material: ISA 315.A182-A183

Control Deficiencies Within the Entity's System of Internal Control (Ref: Para. 27)

A182. In performing the evaluations of each of the components of the entity's system of internal control,⁴⁶ the auditor may determine that certain of the entity's policies in a component are not appropriate to the nature and circumstances of the entity. Such a determination may be an indicator that assists the auditor in identifying control deficiencies. If the auditor has identified one or more control deficiencies, the auditor may consider the effect of those control deficiencies on the design of further audit procedures in accordance with ISA 330.

⁴⁶ Paragraphs 21(b), 22(b), 24(c), 25(c) and 26(d)

A183. If the auditor has identified one or more control deficiencies, ISA 265⁴⁷ requires the auditor to determine whether, individually or in combination, the deficiencies constitute a significant deficiency. The auditor uses professional judgment in determining whether a deficiency represents a significant control deficiency.⁴⁸

Examples:

Circumstances that may indicate a significant control deficiency exists include matters such as:

- The identification of fraud of any magnitude that involves senior management;
- Identified internal processes that are inadequate relating to the reporting and communication of deficiencies noted by internal audit;
- Previously communicated deficiencies that are not corrected by management in a timely manner;
- Failure by management to respond to significant risks, for example, by not implementing controls over significant risks; and
- The restatement of previously issued financial statements.

47 ISA 265, Communicating Deficiencies in Internal Control to Those Charged with Governance and Management, paragraph 8

48 ISA 265, paragraphs A6.A7 set out indicators of significant deficiencies, and matters to be considered in determining whether a deficiency, or a combination of deficiencies, in internal control constitute a significant deficiency.

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Determine whether a deficiency in ICFR exists and describe it [ISA | 1408]

What do we do?

Determine whether, based on the audit work performed, one or more deficiencies in internal control over financial reporting have been identified AND if so, describe it correctly.

Why do we do this?

During our audit, we may identify one or more deficiencies in internal control. If we ignore the identified deficiencies or improperly evaluate them, we may not achieve our audit objectives. This starts with correctly identifying and describing the control deficiencies so we can understand their true impact and consider any other relevant matters that can factor into their severity or impact on the audit.

Execute the Audit

What is a deficiency in internal control? [ISA | 1408.1300]

A deficiency in internal control (also referred to as a 'control deficiency') exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.

When a control deficiency exists, a control is either missing, designed inappropriately or not operating effectively.

What are the possible sources where we may identify control deficiencies? [ISA | 1408.13273]

The table below sets out the possible sources where we may identify control deficiencies and how we may identify a deficiency from each possible source.

Possible source	How we may identify a deficiency from the possible source
Information we become aware of during our planning and risk assessment procedures, including our walkthrough and evaluation of the design and implementation of controls.	<p>As part of understanding the business process, process risk points, and internal controls during risk assessment, we may identify deficiencies in the design of controls, including missing controls.</p> <p>For example, we may identify that a process risk point is not addressed by a properly designed, implemented and effective control.</p>
A cybersecurity incident occurred during the period	<p>When obtaining an understanding of management's cybersecurity risk assessment, we evaluate the impact of a cybersecurity incident, if one occurs, on our audit approach. As part of that evaluation, we may identify control deficiencies related to the cybersecurity incident.</p> <p>Refer to activity 'Understand cybersecurity risks and incidents' for additional guidance.</p>
Our tests of operating effectiveness	<p>We may identify control deviations when we test the operating effectiveness of the controls. Once we identify a control deviation, we determine whether a control deficiency exists.</p> <p>See activity 'Perform relevant procedures when control deviations are identified' and its sub-activities for further information on what we do when we identify control deviations.</p>
Our substantive procedures	<p>Misstatements identified during our substantive procedures may be the result of control deficiencies.</p> <p>See activity 'Evaluate the nature of and reasons for the misstatements' for further information about evaluating misstatements identified to determine whether they are the result of a control deficiency.</p> <p>Further, there may be instances where a transaction we are testing evidences a deviation from our understanding of the entity's process. Regardless of whether a misstatement has occurred, we consider deviations from the process, as they may indicate that we either have</p>

	<p>not sufficiently understood the process or that a control deficiency exists.</p> <p>For example, we may select a revenue transaction as part of our control testing and identify a deviation because it is recorded outside the normal process. This may prompt us to update our understanding of the revenue process, identify process risk points and identify and test the controls that address the process risk points related to these revenue transaction types.</p>
Other auditors involved in the audit	<p>In a group audit, the other auditors involved in the audit may report deficiencies that they identified at the components.</p> <p>See activity 'Obtain, review and retain documentation of work performed by component auditors' for further information.</p>
Management's risk assessment or monitoring processes	<p>We obtain all deficiencies in ICFR identified by management during the period under audit.</p> <p>There are many ways in which management identifies internal control deficiencies, including the entity's monitoring of controls, applicable examinations of controls at a service organization relevant to the entity's ICFR and external parties that provide input about the presence and functioning of internal control components.</p>
Management's assessment of ICFR (integrated audits)	<p>We obtain all deficiencies in ICFR that management identified during the period through its assessment of ICFR.</p>
Internal auditors or other internal entity sources	<p>Internal auditor's reports or other internal entity sources may identify a deficiency in a control that is relevant to the audit.</p>
Service organization reports	<p>Service organization reports can identify a deficiency in a control at the service provider on which the entity is relying for financial reporting. Since service organizations may be a part of the entity's internal controls, these can be relevant to our audit.</p>

External sources including regulatory reports (i.e. SEC comment letters)	<p>Regulatory inspections and communications may indicate deficiencies in internal control.</p> <p>For instance, the entity may receive a comment letter from a regulatory body questioning whether the entity properly accounted for or presented certain transactions. Even if no change results from the comment letter, management's response to the comment letter could indicate that there are possible control deficiencies.</p>
Prior period misstatements identified in the current period, regardless of whether they result in a restatement	<p>Misstatements identified, even if they relate to prior periods, may be caused by control deficiencies. See activity 'Evaluate the nature of and reasons for the misstatements' for further information about evaluating misstatements identified to determine whether they are the result of a control deficiency.</p> <p>Prior period misstatements usually indicate a deficiency in internal controls that existed during that period, but we also consider whether the deficiency continues to exist in the current period as well.</p>
Operational or compliance deficiencies	<p>Weaknesses in operations or compliance with laws and regulations that come to our attention may indicate a related deficiency in internal control over financial reporting. We carefully consider whether there is a potential effect on ICFR and are mindful that we do not quickly dismiss them as "operational or compliance" only.</p>
Work performed by specific team members or employed KPMG specialists	<p>Specific team members or employed KPMG specialists may identify issues with or recommended improvements to management's process or controls.</p> <p>Discussing potential deficiencies with specific team members and/or employed KPMG specialists, can be helpful in determining whether a deficiency exists and correctly identifying and describing the deficiency.</p>
Management's failure to remediate a deficiency for an extended period	<p>Failure to remediate a deficiency in ICFR for an extended period may indicate a broader issue, such as a control deficiency in one or more CERAMIC components. We can usually determine whether a broader issue exists by considering the reasons why the entity has failed to remediate a control deficiency.</p>

For example:

- management may not have the right attitude or a philosophy or operating style that promotes effective internal controls, or
- the entity may not communicate control deficiencies in a timely manner to those responsible for taking corrective action.

However, there may be some situations when a longer remediation period is not an indicator of a broader issue.

For example, when a control deficiency relates to an IT system that is being upgraded or replaced, management may decide to rely on compensating controls instead of making changes in the current IT system to remediate the deficiency.

[What types of deficiencies may we identify?](#) [ISA | 1408.13275]

We may identify the following types of deficiencies:

- process control activities
- general IT controls (GITCs), or
- CERAMIC.

[How do we correctly describe a control deficiency?](#) [ISA | 1408.13276]

We correctly describe a control deficiency by identifying:

- the situation where we found the deficiency;
- the deficient control, including the type of control;
- type of deficiency - i.e. control is missing, not designed correctly or not operating effectively;
- significant account or disclosure affected;
- relevant assertion affected;
- component(s) of internal control affected (and principle of the component, when COSO 2013 is used and considered); and
- the component of the group affected by the deficiency (in group audits).

For example:

Situation	Control	Deficiency	Component of internal control	Component in the group audit

The entity does not have a formal code of conduct.	Management has a formal code of conduct against which it can evaluate employee actions.	Control is missing	Control Environment	Parent entity
Analysis and review of significant unusual transactions is not performed.	Significant unusual transactions are reviewed by management.	Control is missing	Control Activities or Monitoring	Parent entity
Although designed appropriately, bank reconciliations are not performed timely.	Bank reconciliations are performed timely.	Control is not operating effectively	Control Activities	Mexico
There does not appear to be communication between in-house counsel and the accounting department to properly accrue for and disclose legal contingencies.	Key information is provided from in-house counsel to the accounting department so that the accrual and disclosure of legal contingencies can be made based on appropriate information.	Control is missing or designed inappropriately	Information and Communication	Parent entity

Examples

[Does a control deficiency exist?](#) [ISA | 1408.1800]

Scenario 1: Deficiency in ICFR identified through an operational or compliance deficiency

Fact pattern

An entity's internal auditor detects a manufacturing defect in recently produced products, which may increase the number of units returned during the manufacturer's warranty period. The report

indicates an operational deficiency in the manufacturing process, which will be addressed so that future products do not contain the same defect.

Analysis

Although this appears operational in nature, it may indicate a potential deficiency related to the processes and controls that enable the personnel responsible for recording the entity's warranty reserve to have accurate and up-to-date information to properly calculate and record the warranty reserve.

Scenario 2: Business combinations

Fact pattern

An entity with a calendar year-end acquires a business in early December. Management has initiated its processes to estimate the fair value of acquired assets and assumed liabilities in the business combination and has designed and documented relevant internal controls over process risk points identified in the process. Management's specialists performed a reasonable preliminary analysis given the information available from the date of acquisition to the date of the report.

Analysis

In this example, the engagement team may conclude that there is not a deficiency. It is not reasonable to expect that management's controls over the fair value estimates are designed and operating at a higher level of precision than the relevant accounting framework requires of the estimates themselves.

Nonetheless, management must have some controls operating at an adequate precision over the preliminary purchase price allocation disclosed. Because the engagement team concluded that those are in place for this year, there is no control deficiency.

Scenario 3: Internal audit findings

Fact pattern

We find that the entity's inventory cycle count program excludes certain categories of inventory from the counts.

Analysis

The finding indicates a control deficiency in ICFR because it has an impact on the entity's controls related to the existence, completeness and accuracy of inventory.

[What is an appropriate and inappropriate description of a control deficiency?](#) [ISA | 1408.13277]

Fact pattern

We identify a misstatement in the entity's tax provision calculation.

The description of the control deficiency is: "There was an error in the operating effectiveness of controls related to the income tax provision."

Analysis

This description is insufficient because it does not identify the specific control or controls that are deficient (missing, designed inappropriately or operating ineffectively). It only describes that the control relates to the income tax provision.

2 Evaluate the severity and assess the impact of CERAMIC control deficiencies [ISA | 7628]

What do we do?

IF we identify a control deficiency in a CERAMIC component, THEN evaluate the severity of the CERAMIC control deficiency and assess the impact on our audit.

Why do we do this?

CERAMIC is an important part of an entity's ICFR and we consider our understanding of these components when planning and performing our audit. Given the broad nature of CERAMIC, deficiencies in CERAMIC could have a more pervasive impact to our audit approach. As a result, when we identify deficiencies in CERAMIC, we evaluate the severity of the control deficiency and determine the impact on our audit.

Execute the audit

[Not Integrated Audit | When do we identify a CERAMIC control deficiency?](#) [ISA | 7628.8573]

We identify a CERAMIC control deficiency if:

- there are unaddressed principles/elements or
- the entity's set of controls, processes and structures do not appropriately address the principle/element considering the nature and complexity of the entity

[Not Integrated Audit | How do we determine the impact of a CERAMIC control deficiency on our audit?](#)

[ISA | 7628.8575]

When we have identified at least one deficiency in a CERAMIC component, we determine that the CERAMIC component is not appropriate based on the nature and complexity of the entity.

When we conclude that a component is not appropriate based on the nature and complexity of the entity, we identify a financial statement level risk (see activity '[Evaluate RMs at the financial statement level](#)' for additional information) and respond to the risk in line with activity '[Design and implement overall responses](#)'.

[Group Audit | Not Integrated Audit | How do we determine the impact of a CERAMIC control deficiency differently for a group audit?](#) [ISA | 7628.8922]

If a component auditor identifies a financial statement level risk as a result of a CERAMIC control deficiency identified at a component, we assess if there is a financial statement level risk in the context of the group financial statements.

[How does a financial statement level risk related to a CERAMIC component impact our audit?](#) [ISA | 7628.8576]

A financial statement level risk related to a CERAMIC component can result in:

- designing general overall responses (e.g. assigning significant engagement responsibilities appropriately, selecting audit procedures with elements of unpredictability, etc.)

- identifying an assertion level RMM(s);
- identifying a fraud risk factor(s), which could impact our assessment of fraud risks;
- revising our assessment of the inherent risk of an RMM(s); and/or
- deciding not rely on control activities in response to some or all RMMs.

When the financial statement level risk impacts an assertion level RMM, we design or adjust our planned audit procedures in response, such as:

- changing our planned testwork over process control activities, including a revision in RAWTC and/or to the nature, timing, extent of our procedures; and/or
- changing the nature, timing, extent of our planned substantive audit procedures - e.g., performing substantive procedures at the period end instead of at an interim date; modifying the nature of audit procedures to obtain more persuasive audit evidence.

[How can a financial statement level risk related to a CERAMIC component affect our testing of control activities? \[ISA | 7628.8578\]](#)

Where there is a financial statement level risk (FSLR) related to a CERAMIC component, there may be an increase in the risk that the control activities at the process level are not properly designed or do not operate effectively and that there are deficiencies in other CERAMIC components.

We consider this increased risk when evaluating the design and implementation of process control activities, specifically whether the process control activity is appropriately designed to achieve the objective and address the process risk point.

When testing the operating effectiveness of control activities, we factor this increased risk into our assessment of the risk associated with the control (RAWTC). We may also seek to obtain more persuasive audit evidence when we plan the nature, timing and extent of our control testing procedures.

Response to RMMs - testing of controls	Impact of FSLR
Mix of tests of controls and substantive audit procedures	Less likely to design an audit response that uses tests of controls to modify the nature, timing, and extent substantive audit procedures.
Nature of control testing procedures	Increases the RAWTC. We may design our control testing procedures to obtain more persuasive evidence – e.g. reperformance rather than inspection or observation.
Timing of control testing procedures	Increases the RATWC. Control testing procedures are performed closer to or at period-end rather than performing at an interim date with appropriate procedures to roll-forward our interim conclusions.

Extent of control testing procedures	Increases the RAWTC. We may increase the extent of our control testing procedures - e.g. increase the instances that a control that is tested.
--------------------------------------	--

How can a financial statement level risk related to a CERAMIC component affect our substantive audit procedures? [\[ISA | 7628.8579\]](#)

A financial statement level risk (FLSR) related to CERAMIC component may impact our evaluation of CAR for an RMM(s) through (i) a revision to our assessment of the inherent risk of the RMM(s) and/or (ii) a change in our assessment of control risk - i.e., whether we can take a controls approach for an RMM(s).

An increase in CAR will increase the persuasiveness of the audit evidence we seek to obtain when we design the nature, timing and extent of our substantive audit procedures.

Response to RMMs - substantive audit procedures	Impact of FLSR
Nature of substantive audit procedures	May increase CAR and we may design the nature of our substantive procedures to obtain more persuasive evidence - e.g. test of details procedures rather than substantive analytical procedures.
Timing of substantive audit procedures	May increase CAR and certain substantive procedures are performed closer to or at period-end rather than at an interim date and rolling forward the conclusion to period-end.
Extent of substantive audit procedures	May increase CAR and the extent of our substantive procedures - e.g. increase the number of items that are tested when substantive sampling is used.

Examples

[Not Integrated Audit | How might a deficiency in the Control Environment affect how we identify and assess risks?](#) [\[ISA | 7628.8583\]](#)

Fact pattern

When we obtain an understanding an entity's Control Environment, we identify a deficiency, because the entity does not have established competence requirements, training, or a process for evaluating the performance of people in key financial reporting roles, which we would expect to exist based on the circumstances of the entity (a large entity with complex products and revenue arrangements). In the current year, the entity hired a new CFO and controller.

Analysis

After considering the nature and severity of the deficiency, we determine that the entity has not appropriately addressed Principle/Element 4, and we conclude the following and identify a related financial statement level risk:

- The control deficiency identified undermines the other components of the entity's system of internal control.
- The control environment does not provide an appropriate foundation for the other components of ICFR considering the nature and complexity of the entity.

Due to the new CFO and controller and the lack of training and performance evaluations for existing financial reporting personnel, we identify a financial statement level risk and in response, we:

- design general overall responses (refer to activity '[Design and implement overall responses](#)' for additional information) and
- make pervasive changes to our audit procedures.

Given the pervasiveness of the FSLR, we may determine pervasive changes to our audit procedures such as:

- deciding to place limited or no reliance on control activities and obtain more extensive audit evidence from substantive procedures,
- assessing the inherent risk of RMMs as greater than Base, particularly those that require significant judgement and are more susceptible to error and/or
- conducting more audit procedures as of the period end rather than at an interim date.

We also consider the impact of the deficiency on our assessment of aggregation risk when determining performance materiality, component materiality, and group audit scoping.

Refer to the question '[How do we identify and respond to risks that results in pervasive changes to our audit procedures?](#)' for an alternative example of a deficiency identified in the control environment and related response.

[Not Integrated Audit | How might a deficiency in risk assessment affect the identification and assessment of risks?](#) [ISA | 7628.12615]

Fact pattern

When we obtain an understanding of an entity's risk assessment process, we determine that the entity has a deficiency in ICFR because it doesn't have an established risk assessment process to identify business and related financial reporting risks when we would expect that to exist based on the circumstances of the entity (a large entity with complex products and revenue arrangements).

Further, the lack of an established risk assessment process resulted in management's failure to appropriately analyze the business risks related to financial reporting for a significant acquisition that occurred during the year. The acquisition was in a country in which the entity did not previously have operations.

Analysis

After considering the nature and severity of the deficiency - in particular, the lack of an established risk assessment process and the entity's failure to identify business risks - we determine that the entity has not appropriately addressed Principle/Elements 6-8. We conclude that the entity's risk assessment

process is not appropriate to the entity's circumstances considering the nature and complexity of the entity and identify a financial statement-level risk.

In response, we:

- design general overall responses (refer to activity 'Design and implement overall responses' [782] for additional information), in particular increasing involvement of senior members in executing risk assessment procedures and more extensive engagement partner review of the engagement team's risk assessment procedures, and
- make pervasive changes to our audit procedures.

We may determine pervasive changes to our audit procedures such as:

- increasing RAWTC for any controls that we plan to rely on;
- deciding to place very limited or no reliance on controls in the audit areas affected by the acquisition and obtain more extensive audit evidence from substantive procedures and/or
- re-assessing the inherent risk of RMMs related to the audit areas affected by the acquisition

We also consider the impact of the deficiency on our assessment of aggregation risk when determining performance materiality, component materiality, and group audit scoping.

[Not Integrated Audit | How might a deficiency in information and communication affect the identification and assessment of risks?](#) [ISA | 7628.12617]

Fact pattern

Fact pattern

When we obtained an understanding of an entity's information and communication processes, based upon consideration of the factors in activity '[Perform procedures to obtain an understanding of the CERAMIC components](#)', we determined that it was necessary to perform procedures other than inquiry. We planned to inspect minutes from the December monthly Finance Group meeting and noted that it was not held in December due to time pressures associated with the period-end close process. These monthly Finance Group meetings are the primary means through which information is communicated to enable financial reporting personnel to carry out their responsibilities.

As a result, the Income Tax Director did not become aware of new related-party transactions that affected the income tax provision for foreign entities. The income tax provision for foreign entities was subject to a set of controls whereby the Income Tax Director reviews various aspects of the provision, including permanent and temporary differences associated with related-party transactions and transfer pricing.

As a result of the exception and the related misstatement in the entity's financial statements, we identify a related control deficiency in the entity's ICFR.

In particular, we note that a number of matters that should have been discussed during December's Executive Committee meeting that could potentially affect financial reporting and ICFR, including new product launches, new geographic markets, related-party transactions and changes in tax laws in foreign jurisdictions.

Although some of these items were communicated through other informal channels and did not result in a misstatement to the entity's financial statements, a reasonable possibility exists that the

deficiency in the entity's Information and Communication component of ICFR could result in a material misstatement to its financial statements.

Analysis

As a result of the deficiency, we determine that the entity has not appropriately addressed Principle 14/Element 10 and conclude that the entity's communication component does not appropriately support the preparation of the entity's financial statements in accordance with the applicable financial reporting framework considering the nature and complexity of the entity. We identify a financial statement level risk (FSLR) related to the entity's failure to internally communicate important information related to financial reporting and ICFR.

In response, we:

- design general overall responses (refer to activity '[Design and implement overall responses](#)' for additional information) and
- make pervasive changes to our audit procedures.

We may determine pervasive changes to our audit procedures such as:

- re-assessing RAWTC for the controls for which we planned to place reliance and perform more than inquiry for those controls during the rollforward period
- re-assessing the inherent risk of RMMs related to the audit areas where events occurred and were not properly communicated and/or
- conducting more audit procedures as of the period end rather than at an interim date.

We also consider the impact of the deficiency on our assessment of aggregation risk when determining performance materiality, component materiality, and group audit scoping.

[Not Integrated Audit | How might a deficiency in monitoring activities affect our identification and assessment of risks?](#) [ISA | 7628.12619]

Fact pattern

When we obtain an understanding of how the entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, we determine that a number of deficiencies have not been remediated in a timely manner.

Analysis

As a result of the exception, we identify a related control deficiency.

In particular, when we evaluate the severity of the deficiency, we note that:

- the nature and frequency of the deficiencies that remain unremediated could have resulted in a material misstatement to the entity's financial statements; and
- as a result, those charged with the entity's governance have not exercised appropriate oversight over ICFR (Element 2 of the Control Environment).

After considering the nature and severity of the deficiency, we conclude that the entity has not appropriately addressed Principle 17 and 2/Element 14 and 2. We conclude that the entity's process for monitoring the system of internal control is not appropriate to the entity's circumstances considering the nature and complexity of the entity and identify a financial statement level risk (FSLR) related to:

- the entity's failure to take corrective actions to respond to identified deficiencies; and
- ineffective oversight of ICFR by those charged with the entity's governance.

In response, we:

- design general overall responses (refer to activity '[Design and implement overall responses](#)' for additional information) and
- make pervasive changes to our audit procedures, such as taking a fully substantive approach to respond to RMMs related to the unremediated deficiencies - i.e. assess control risk as non-reliance.

Additionally, as the FSLR is related to both the Monitoring and Control Environment components of ICFR, we consider it [when identifying fraud risk factors and related fraud risks](#).

In particular, the ineffective oversight of ICFR by those charged with the entity's governance provides opportunities to commit fraud that we consider to be a fraud risk factor as part of our identification and assessment of fraud risks.

We also consider the impact of the deficiency on our assessment of aggregation risk when determining performance materiality, component materiality, and group audit scoping.

Identifying and Assessing the Risks of Material Misstatement

International Standards on Auditing: ISA 315.28-34

Identifying and Assessing the Risks of Material Misstatement (Ref: Para. A184.A185)

Identifying Risks of Material Misstatement

28. The auditor shall identify the risks of material misstatement and determine whether they exist at: (Ref: Para. A186-A192)

- (a) The financial statement level; (Ref: Para. A193-A200) or
- (b) The assertion level for classes of transactions, account balances and disclosures. (Ref: Para. A201)

29. The auditor shall determine the relevant assertions and the related significant classes of transactions, account balances and disclosures. (Ref: Para. A202-A204)

Assessing Risks of Material Misstatement at the Financial Statement Level

30. For identified risks of material misstatement at the financial statement level, the auditor shall assess the risks and: (Ref: Para. A193-A200)

- (a) Determine whether such risks affect the assessment of risks at the assertion level; and
- (b) Evaluate the nature and extent of their pervasive effect on the financial statements.

Assessing Risks of Material Misstatement at the Assertion Level

Assessing Inherent Risk (Ref: Para. A205-A217)

31. For identified risks of material misstatement at the assertion level, the auditor shall assess inherent risk by assessing the likelihood and magnitude of misstatement. In doing so, the auditor shall take into account how, and the degree to which:

- (a) Inherent risk factors affect the susceptibility of relevant assertions to misstatement; and
- (b) The risks of material misstatement at the financial statement level affect the assessment of inherent risk for risks of material misstatement at the assertion level. (Ref: Para. A215.A216)

32. The auditor shall determine whether any of the assessed risks of material misstatement are significant risks. (Ref: Para. A218-A221)

33. The auditor shall determine whether substantive procedures alone cannot provide sufficient appropriate audit evidence for any of the risks of material misstatement at the assertion level. (Ref: Para. A222-A225)

Assessing Control Risk

34. If the auditor plans to test the operating effectiveness of controls, the auditor shall assess control risk. If the auditor does not plan to test the operating effectiveness of controls, the auditor's assessment of control risk shall be such that the assessment of the risk of material misstatement is the same as the assessment of inherent risk. (Ref: Para. A226-A229)

ISA Application and Other Explanatory Material: ISA 315.A184-A229

Identifying and Assessing the Risks of Material Misstatement (Ref: Para. 28.37)

Why the Auditor Identifies and Assesses the Risks of Material Misstatement

A184. Risks of material misstatement are identified and assessed by the auditor in order to determine the nature, timing and extent of further audit procedures necessary to obtain sufficient appropriate audit evidence. This evidence enables the auditor to express an opinion on the financial statements at an acceptably low level of audit risk.

A185. Information gathered by performing risk assessment procedures is used as audit evidence to provide the basis for the identification and assessment of the risks of material misstatement. For example, the audit evidence obtained when evaluating the design of identified controls and determining whether those controls have been implemented in the control activities component, is used as audit evidence to support the risk assessment. Such evidence also provides a basis for the auditor to design overall responses to address the assessed risks of material misstatement at the financial statement level, as well as designing and performing further audit procedures whose nature, timing and extent are responsive to the assessed risks of material misstatement at the assertion level, in accordance with ISA 330.

Identifying Risks of Material Misstatement (Ref: Para. 28)

A186. The identification of risks of material misstatement is performed before consideration of any related controls (i.e., the inherent risk), and is based on the auditor's preliminary consideration of misstatements that have a reasonable possibility of both occurring, and being material if they were to occur.⁴⁹

⁴⁹ ISA 200, paragraph A15a

A187. Identifying the risks of material misstatement also provides the basis for the auditor's determination of relevant assertions, which assists the auditor's determination of the significant classes of transactions, account balances and disclosures.

Assertions

Why the Auditor Uses Assertions

A188. In identifying and assessing the risks of material misstatement, the auditor uses assertions to consider the different types of potential misstatements that may occur. Assertions for which the auditor has identified related risks of material misstatement are relevant assertions.

The Use of Assertions

A189. In identifying and assessing the risks of material misstatement, the auditor may use the categories of assertions as described in paragraph A190(a).(b) below or may express them differently provided all aspects described below have been covered. The auditor may choose to combine the assertions about classes of transactions and events, and related disclosures, with the assertions about account balances, and related disclosures.

A190. Assertions used by the auditor in considering the different types of potential misstatements that may occur may fall into the following categories:

- (a) Assertions about classes of transactions and events, and related disclosures, for the period under audit:
 - (i) Occurrence-transactions and events that have been recorded or disclosed have occurred, and such transactions and events pertain to the entity.
 - (ii) Completeness-all transactions and events that should have been recorded have been recorded, and all related disclosures that should have been included in the financial statements have been included.
 - (iii) Accuracy-amounts and other data relating to recorded transactions and events have been recorded appropriately, and related disclosures have been appropriately measured and described.
 - (iv) Cutoff-transactions and events have been recorded in the correct accounting period.
 - (v) Classification-transactions and events have been recorded in the proper accounts.
 - (vi) Presentation-transactions and events are appropriately aggregated or disaggregated and clearly described, and related disclosures are relevant and understandable in the context of the requirements of the applicable financial reporting framework.

(b) Assertions about account balances, and related disclosures, at the period end:

- (i) Existence-assets, liabilities and equity interests exist.
- (ii) Rights and obligations-the entity holds or controls the rights to assets, and liabilities are the obligations of the entity.
- (iii) Completeness-all assets, liabilities and equity interests that should have been recorded have been recorded, and all related disclosures that should have been included in the financial statements have been included.
- (iv) Accuracy, valuation and allocation-assets, liabilities and equity interests have been included in the financial statements at appropriate amounts and any resulting valuation or allocation adjustments have been appropriately recorded, and related disclosures have been appropriately measured and described.
- (v) Classification-assets, liabilities and equity interests have been recorded in the proper accounts.
- (vi) Presentation-assets, liabilities and equity interests are appropriately aggregated or disaggregated and clearly described, and related disclosures are relevant and understandable in the context of the requirements of the applicable financial reporting framework.

A191. The assertions described in paragraph A190(a).(b) above, adapted as appropriate, may also be used by the auditor in considering the different types of misstatements that may occur in disclosures not directly related to recorded classes of transactions, events or account balances.

Example:

An example of such a disclosure includes where the entity may be required by the applicable financial reporting framework to describe its exposure to risks arising from financial instruments, including how the risks arise; the objectives, policies and processes for managing the risks; and the methods used to measure the risks.

Considerations Specific to Public Sector Entities

A192. When making assertions about the financial statements of public sector entities, in addition to those assertions set out in paragraph A190(a).(b), management may often assert that transactions and events have been carried out in accordance with law, regulation or other authority. Such assertions may fall within the scope of the financial statement audit.

Risks of Material Misstatement at the Financial Statement Level (Ref: Para. 28(a) and 30)

Why the Auditor Identifies and Assesses Risks of Material Misstatement at the Financial Statement Level

A193. The auditor identifies risks of material misstatement at the financial statement level to determine whether the risks have a pervasive effect on the financial statements, and would therefore require an overall response in accordance with ISA 330.⁵⁰

50 ISA 330, paragraph 5

A194. In addition, risks of material misstatement at the financial statement level may also affect individual assertions, and identifying these risks may assist the auditor in assessing risks of material misstatement at the assertion level, and in designing further audit procedures to address the identified risks.

Identifying and Assessing Risks of Material Misstatement at the Financial Statement Level

A195. Risks of material misstatement at the financial statement level refer to risks that relate pervasively to the financial statements as a whole, and potentially affect many assertions. Risks of this nature are not necessarily risks identifiable with specific assertions at the class of transactions, account balance or disclosure level (e.g., risk of management override of controls). Rather, they represent circumstances that may pervasively increase the risks of material misstatement at the assertion level. The auditor's evaluation of whether risks identified relate pervasively to the financial statements supports the auditor's assessment of the risks of material misstatement at the financial statement level. In other cases, a number of assertions may also be identified as susceptible to the risk, and may therefore affect the auditor's risk identification and assessment of risks of material misstatement at the assertion level.

Example:

The entity faces operating losses and liquidity issues and is reliant on funding that has not yet been secured. In such a circumstance, the auditor may determine that the going concern basis of accounting gives rise to a risk of material misstatement at the financial statement level. In this situation, the accounting framework may need to be applied using a liquidation basis, which would likely affect all assertions pervasively.

A196. The auditor's identification and assessment of risks of material misstatement at the financial statement level is influenced by the auditor's understanding of the entity's system of internal control, in particular the auditor's understanding of the control environment, the entity's risk assessment process and the entity's process to monitor the system of internal control, and:

- The outcome of the related evaluations required by paragraphs 21(b), 22(b), 24(c) and 25(c); and
- Any control deficiencies identified in accordance with paragraph 27.

In particular, risks at the financial statement level may arise from deficiencies in the control environment or from external events or conditions such as declining economic conditions.

A197. Risks of material misstatement due to fraud may be particularly relevant to the auditor's consideration of the risks of material misstatement at the financial statement level.

Example:

The auditor understands from inquiries of management that the entity's financial statements are to be used in discussions with lenders in order to secure further financing to maintain working capital. The auditor may therefore determine that there is a greater susceptibility to misstatement due to fraud risk factors that affect inherent risk (i.e., the susceptibility of the financial statements to material misstatement because of the risk of fraudulent financial reporting, such as overstatement of

assets and revenue and under-statement of liabilities and expenses to ensure that financing will be obtained).

A198. The auditor's understanding, including the related evaluations, of the control environment and other components of the system of internal control may raise doubts about the auditor's ability to obtain audit evidence on which to base the audit opinion or be cause for withdrawal from the engagement where withdrawal is possible under applicable law or regulation.

Examples:

- As a result of evaluating the entity's control environment, the auditor has concerns about the integrity of the entity's management, which may be so serious as to cause the auditor to conclude that the risk of intentional misrepresentation by management in the financial statements is such that an audit cannot be conducted.
- As a result of evaluating the entity's information system and communication, the auditor determines that significant changes in the IT environment have been poorly managed, with little oversight from management and those charged with governance. The auditor concludes that there are significant concerns about the condition and reliability of the entity's accounting records. In such circumstances, the auditor may determine that it is unlikely that sufficient appropriate audit evidence will be available to support an unmodified opinion on the financial statements.

A199. ISA 705 (Revised)⁵¹ establishes requirements and provides guidance in determining whether there is a need for the auditor to express a qualified opinion or disclaim an opinion or, as may be required in some cases, to withdraw from the engagement where withdrawal is possible under applicable law or regulation.

51 ISA 705 (Revised), Modifications to the Opinion in the Independent Auditor's Report

Considerations Specific to Public Sector Entities

A200. For public sector entities, the identification of risks at the financial statement level may include consideration of matters related to the political climate, public interest and program sensitivity.

Risks of Material Misstatement at the Assertion Level (Ref: Para. 28(b))

Appendix 2 sets out examples, in the context of inherent risk factors, of events or conditions that may indicate susceptibility to misstatement that may be material.

A201. Risks of material misstatements that do not relate pervasively to the financial statements are risks of material misstatement at the assertion level.

Relevant Assertions and Significant Classes of Transactions, Account Balances and Disclosures (Ref: Para. 29)

Why Relevant Assertions and Significant Classes of Transactions, Account Balances and Disclosures Are Determined

A202. Determining relevant assertions and the significant classes of transactions, account balances and disclosures provides the basis for the scope of the auditor's understanding of the entity's information system required to be obtained in accordance with paragraph 25(a). This understanding may further assist the auditor in identifying and assessing risks of material misstatement (see A86).

Automated Tools and Techniques

A203. The auditor may use automated techniques to assist in the identification of significant classes of transactions, account balances and disclosures.

Examples:

- An entire population of transactions may be analyzed using automated tools and techniques to understand their nature, source, size and volume. By applying automated techniques, the auditor may, for example, identify that an account with a zero balance at period end was comprised of numerous offsetting transactions and journal entries occurring during the period, indicating that the account balance or class of transactions may be significant (e.g., a payroll clearing account). This same payroll clearing account may also identify expense reimbursements to management (and other employees), which could be a significant disclosure due to these payments being made to related parties.
- By analyzing the flows of an entire population of revenue transactions, the auditor may more easily identify a significant class of transactions that had not previously been identified.

Disclosures that May Be Significant

A204. Significant disclosures include both quantitative and qualitative disclosures for which there is one or more relevant assertions. Examples of disclosures that have qualitative aspects and that may have relevant assertions and may therefore be considered significant by the auditor include disclosures about:

- Liquidity and debt covenants of an entity in financial distress.
- Events or circumstances that have led to the recognition of an impairment loss.
- Key sources of estimation uncertainty, including assumptions about the future.
- The nature of a change in accounting policy, and other relevant disclosures required by the applicable financial reporting framework, where, for example, new financial reporting requirements are expected to have a significant impact on the financial position and financial performance of the entity.
- Share-based payment arrangements, including information about how any amounts recognized were determined, and other relevant disclosures.
- Related parties, and related party transactions.

- Sensitivity analysis, including the effects of changes in assumptions used in the entity's valuation techniques intended to enable users to understand the underlying measurement uncertainty of a recorded or disclosed amount.

Assessing Risks of Material Misstatement at the Assertion Level

Assessing Inherent Risk (Ref: Para. 31.33)

Assessing the likelihood and magnitude of misstatement (Ref: Para: 31)

Why the auditor assesses likelihood and magnitude of misstatement

A205. The auditor assesses the likelihood and magnitude of misstatement for identified risks of material misstatement because the significance of the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement were the misstatement to occur determines where on the spectrum of inherent risk the identified risk is assessed, which informs the auditor's design of further audit procedures to address the risk.

A206. Assessing the inherent risk of identified risks of material misstatement also assists the auditor in determining significant risks. The auditor determines significant risks because specific responses to significant risks are required in accordance with ISA 330 and other ISAs.

A207. Inherent risk factors influence the auditor's assessment of the likelihood and magnitude of misstatement for the identified risks of material misstatement at the assertion level. The greater the degree to which a class of transactions, account balance or disclosure is susceptible to material misstatement, the higher the inherent risk assessment is likely to be. Considering the degree to which inherent risk factors affect the susceptibility of an assertion to misstatement assists the auditor in appropriately assessing inherent risk for risks of material misstatement at the assertion level and in designing a more precise response to such a risk.

Spectrum of inherent risk

A208. In assessing inherent risk, the auditor uses professional judgment in determining the significance of the combination of the likelihood and magnitude of a misstatement.

A209. The assessed inherent risk relating to a particular risk of material misstatement at the assertion level represents a judgment within a range, from lower to higher, on the spectrum of inherent risk. The judgment about where in the range inherent risk is assessed may vary based on the nature, size and complexity of the entity, and takes into account the assessed likelihood and magnitude of the misstatement and inherent risk factors.

A210. In considering the likelihood of a misstatement, the auditor considers the possibility that a misstatement may occur, based on consideration of the inherent risk factors.

A211. In considering the magnitude of a misstatement, the auditor considers the qualitative and quantitative aspects of the possible misstatement (i.e., misstatements in assertions about classes of transactions, account balances or disclosures may be judged to be material due to size, nature or circumstances).

A212. The auditor uses the significance of the combination of the likelihood and magnitude of a possible misstatement in determining where on the spectrum of inherent risk (i.e., the range) inherent risk is assessed. The higher the combination of likelihood and magnitude, the higher the assessment of inherent risk; the lower the combination of likelihood and magnitude, the lower the assessment of inherent risk.

A213. For a risk to be assessed as higher on the spectrum of inherent risk, it does not mean that both the magnitude and likelihood need to be assessed as high. Rather, it is the intersection of the magnitude and likelihood of the material misstatement on the spectrum of inherent risk that will determine whether the assessed inherent risk is higher or lower on the spectrum of inherent risk. A higher inherent risk assessment may also arise from different combinations of likelihood and magnitude, for example a higher inherent risk assessment could result from a lower likelihood but a very high magnitude.

A214. In order to develop appropriate strategies for responding to risks of material misstatement, the auditor may designate risks of material misstatement within categories along the spectrum of inherent risk, based on their assessment of inherent risk. These categories may be described in different ways. Regardless of the method of categorization used, the auditor's assessment of inherent risk is appropriate when the design and implementation of further audit procedures to address the identified risks of material misstatement at the assertion level is appropriately responsive to the assessment of inherent risk and the reasons for that assessment.

Pervasive Risks of Material Misstatement at the Assertion Level (Ref: Para 31(b))

A215. In assessing the identified risks of material misstatement at the assertion level, the auditor may conclude that some risks of material misstatement relate more pervasively to the financial statements as a whole and potentially affect many assertions, in which case the auditor may update the identification of risks of material misstatement at the financial statement level.

A216. In circumstances in which risks of material misstatement are identified as financial statement level risks due to their pervasive effect on a number of assertions, and are identifiable with specific assertions, the auditor is required to take into account those risks when assessing inherent risk for risks of material misstatement at the assertion level.

Considerations Specific to Public Sector Entities

A217. In exercising professional judgment as to the assessment of the risk of material misstatement, public sector auditors may consider the complexity of the regulations and directives, and the risks of non-compliance with authorities.

Significant Risks (Ref: Para. 32)

Why significant risks are determined and the implications for the audit

A218. The determination of significant risks allows for the auditor to focus more attention on those risks that are on the upper end of the spectrum of inherent risk, through the performance of certain required responses, including:

- Controls that address significant risks are required to be identified in accordance with paragraph 26(a)(i), with a requirement to evaluate whether the control has been designed effectively and implemented in accordance with paragraph 26(d).
- ISA 330 requires controls that address significant risks to be tested in the current period (when the auditor intends to rely on the operating effectiveness of such controls) and substantive procedures to be planned and performed that are specifically responsive to the identified significant risk.⁵²
- ISA 330 requires the auditor to obtain more persuasive audit evidence the higher the auditor's assessment of risk.⁵³

- ISA 260 (Revised) requires communicating with those charged with governance about the significant risks identified by the auditor.⁵⁴
- ISA 701 requires the auditor to take into account significant risks when determining those matters that required significant auditor attention, which are matters that may be key audit matters.⁵⁵
- Timely review of audit documentation by the engagement partner at the appropriate stages during the audit allows significant matters, including significant risks, to be resolved on a timely basis to the engagement partner's satisfaction on or before the date of the auditor's report.⁵⁶
- ISA 600 (Revised) requires the group auditor to evaluate the appropriateness of the design and performance of further audit procedures for areas of higher assessed risks of material misstatement of the group financial statements, or significant risks, on which a component auditor is determining the further audit procedures to be performed.⁵⁷

52 ISA 330, paragraphs 15 and 21

53 ISA 330, paragraph 7(b)

54 ISA 260 (Revised), paragraph 15

55 ISA 701, Communicating Key Audit Matters in the Independent Auditor's Report, paragraph 9

56 ISA 220 (Revised), paragraphs 32 and A87-A89

57 ISA 600, paragraphs 30 and 31

Determining significant risks

A219. In determining significant risks, the auditor may first identify those assessed risks of material misstatement that have been assessed higher on the spectrum of inherent risk to form the basis for considering which risks may be close to the upper end. Being close to the upper end of the spectrum of inherent risk will differ from entity to entity, and will not necessarily be the same for an entity period on period. It may depend on the nature and circumstances of the entity for which the risk is being assessed.

A220. The determination of which of the assessed risks of material misstatement are close to the upper end of the spectrum of inherent risk, and are therefore significant risks, is a matter of professional judgment, unless the risk is of a type specified to be treated as a significant risk in accordance with the requirements of another ISA. ISA 240 provides further requirements and guidance in relation to the identification and assessment of the risks of material misstatement due to fraud.⁵⁸

Example:

- Cash at a supermarket retailer would ordinarily be determined to be a high likelihood of possible misstatement (due to the risk of cash being misappropriated), however the magnitude would typically be very low (due to the low levels of physical cash handled in the stores). The combination of these two factors on the spectrum of inherent risk would be unlikely to result in the existence of cash being determined to be a significant risk.
- An entity is in negotiations to sell a business segment. The auditor considers the effect on goodwill impairment, and may determine there is a higher likelihood of possible misstatement and a higher magnitude due to the impact of inherent risk factors of subjectivity, uncertainty and susceptibility to management bias or other fraud risk factors. This may result in goodwill impairment being determined to be a significant risk.

58 ISA 240, paragraphs 26-28

A221. The auditor also takes into the account the relative effects of inherent risk factors when assessing inherent risk. The lower the effect of inherent risk factors, the lower the assessed risk is likely to be. Risks of material misstatement that may be assessed as having higher inherent risk and may therefore be determined to be a significant risk, may arise from matters such as the following:

- Transactions for which there are multiple acceptable accounting treatments such that subjectivity is involved.
- Accounting estimates that have high estimation uncertainty or complex models.
- Complexity in data collection and processing to support account balances.
- Account balances or quantitative disclosures that involve complex calculations.
- Accounting principles that may be subject to differing interpretation.
- Changes in the entity's business that involve changes in accounting, for example, mergers and acquisitions.

Risks for Which Substantive Procedures Alone Do Not Provide Sufficient Appropriate Audit Evidence (Ref: Para. 33)

Why risks for which substantive procedures alone do not provide sufficient appropriate audit evidence are required to be identified

A222. Due to the nature of a risk of material misstatement, and the control activities that address that risk, in some circumstances the only way to obtain sufficient appropriate audit evidence is to test the operating effectiveness of controls. Accordingly, there is a requirement for the auditor to identify any such risks because of the implications for the design and performance of further audit procedures in accordance with ISA 330 to address risks of material misstatement at the assertion level.

A223. Paragraph 26(a)(iii) also requires the identification of controls that address risks for which substantive procedures alone cannot provide sufficient appropriate audit evidence because the auditor is required, in accordance with ISA 330,⁵⁹ to design and perform tests of such controls.

59 ISA 330, paragraph 8

Determining risks for which substantive procedures alone do not provide sufficient appropriate audit evidence

A224. Where routine business transactions are subject to highly automated processing with little or no manual intervention, it may not be possible to perform only substantive procedures in relation to the risk. This may be the case in circumstances where a significant amount of an entity's information is initiated, recorded, processed, or reported only in electronic form such as in an information system that involves a high degree of integration across its IT applications. In such cases:

- Audit evidence may be available only in electronic form, and its sufficiency and appropriateness usually depend on the effectiveness of controls over its accuracy and completeness.
- The potential for improper initiation or alteration of information to occur and not be detected may be greater if appropriate controls are not operating effectively.

Example:

It is typically not possible to obtain sufficient appropriate audit evidence relating to revenue for a telecommunications entity based on substantive procedures alone. This is because the evidence of call or data activity does not exist in a form that is observable. Instead, substantial controls testing is typically performed to determine that the origination and completion of calls, and data activity is correctly captured (e.g., minutes of a call or volume of a download) and recorded correctly in the entity's billing system.

A225. ISA 540 (Revised) provides further guidance related to accounting estimates about risks for which substantive procedures alone do not provide sufficient appropriate audit evidence.⁶⁰ In relation to accounting estimates this may not be limited to automated processing, but may also be applicable to complex models.

⁶⁰ ISA 540 (Revised), paragraphs A87-A89

Assessing Control Risk (Ref: Para. 34)

A226. The auditor's plans to test the operating effectiveness of controls is based on the expectation that controls are operating effectively, and this will form the basis of the auditor's assessment of control risk. The initial expectation of the operating effectiveness of controls is based on the auditor's evaluation of the design, and the determination of implementation, of the identified controls in the control activities component. Once the auditor has tested the operating effectiveness of the controls in accordance with ISA 330, the auditor will be able to confirm the initial expectation about the operating effectiveness of controls. If the controls are not operating effectively as expected, then the auditor will need to revise the control risk assessment in accordance with paragraph 37.

A227. The auditor's assessment of control risk may be performed in different ways depending on preferred audit techniques or methodologies, and may be expressed in different ways.

A228. If the auditor plans to test the operating effectiveness of controls, it may be necessary to test a combination of controls to confirm the auditor's expectation that the controls are operating effectively. The auditor may plan to test both direct and indirect controls, including general IT controls, and, if so, take into account the combined expected effect of the controls when assessing control risk. To the extent that the control to be tested does not fully address the assessed inherent risk, the auditor determines the implications on the design of further audit procedures to reduce audit risk to an acceptably low level.

A229. When the auditor plans to test the operating effectiveness of an automated control, the auditor may also plan to test the operating effectiveness of the relevant general IT controls that support the continued functioning of that automated control to address the risks arising from the use of IT, and to provide a basis for the auditor's expectation that the automated control operated effectively throughout the period. When the auditor expects related general IT controls to be ineffective, this determination may affect the auditor's assessment of control risk at the assertion level and the auditor's further audit procedures may need to include substantive procedures to address the applicable risks arising from the use of IT. Further guidance about the procedures that the auditor may perform in these circumstances is provided in ISA 330.⁶¹

61 ISA 330, paragraphs A29-A30

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Identify and assess RMMs [ISA | 561]

What do we do?

Identify and assess the risks of material misstatement at the financial statement level and the assertion level

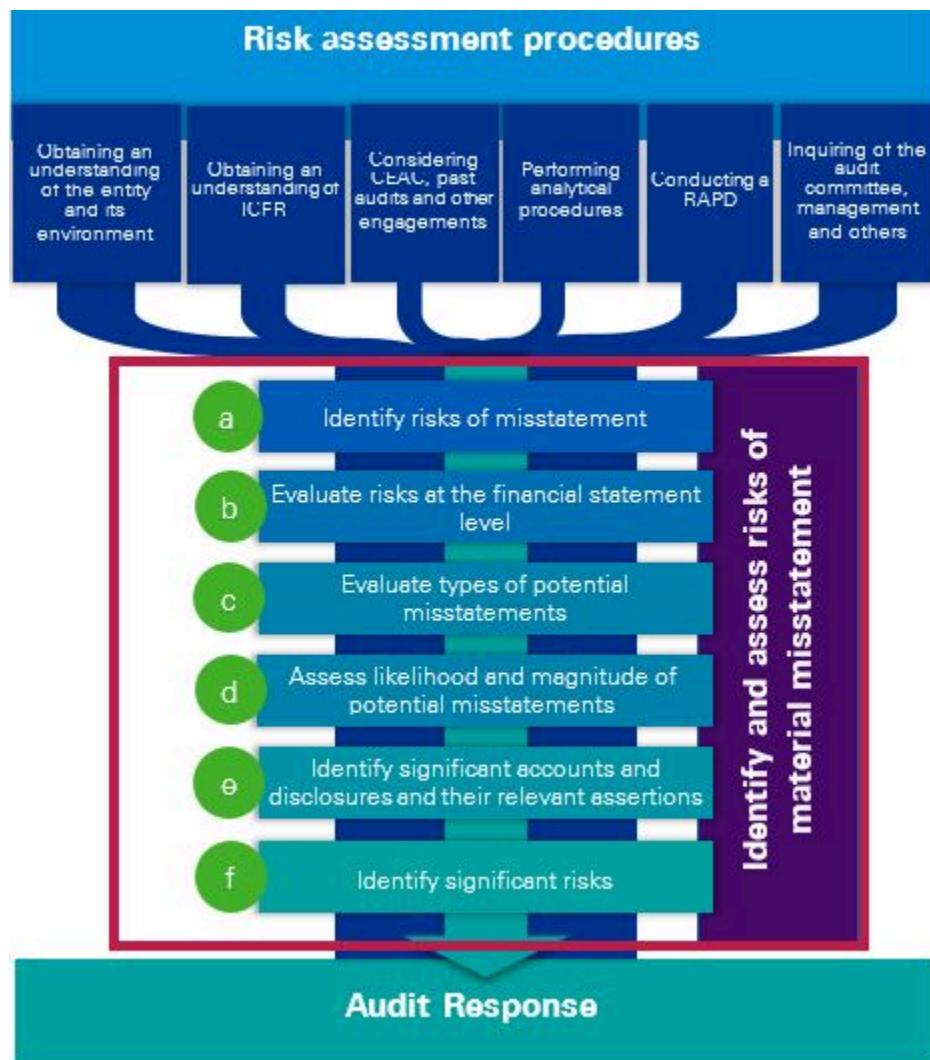
Why do we do this?

Identifying and assessing the risks of material misstatement (RMMs) provides the basis for the determination of relevant assertions, significant accounts and disclosures and to provide a basis for designing and performing further audit procedures.

Execute the Audit

Where does this activity fit into our risk assessment? [ISA | 561.1300]

We perform our risk assessment procedures with a specific purpose in mind: to collect information to identify and assess RMMs. These RMMs will then drive our audit responses. Visually, we may think of the process as follows.



What are the different types of risks, and how are they interrelated? [ISA | 561.1400]

There are three types of risk.

Risks of misstatement (RMs)	Risks that could result in a misstatement to the financial statements. These can be either assertion-level RMs or financial statement-level RMs . This is the population of risks we assess further.
Risks of material misstatement (RMMs)	Risks that could result in a <i>material</i> misstatement to the financial statements. These can be either assertion-level RMMs or financial statement-level RMMs .
<u>Significant risks</u>	Risks that are closer to the upper end of the spectrum of inherent risk.

	Special audit consideration is given for these RMMs because of the nature of the risk or the potential likelihood and magnitude of misstatement related to the risk. These include fraud risks and significant unusual transactions with related parties.
--	---

These are subsets of one another, representing an increasingly narrow focus. As such, we identify the different types of risk in this order.

The graphic below shows one way to visualize the relationship between these different types of risks.



What are assertion level and financial-statement level RMMs? [ISA | 561.8552]

The following table explains the differences between assertion-level and financial statement level risks:

Type of risks	What are they?
Assertion-level RMMs	Risks of material misstatement that: <ul style="list-style-type: none"> relate to specific assertions for classes of transactions, account balances, or disclosures; and relate to misstatements that can arise when the financial reporting framework (e.g. IFRS, US GAAP), is not applied appropriately.
Financial statement-level RMMs	Risks of material misstatement that: <ul style="list-style-type: none"> relate pervasively to the financial statements as a whole may affect many accounts and/or assertions don't necessarily relate to applying particular accounting policies or principles

- may arise from the entity and its environment, including business risks and broad internal control issues

How do we identify and assess RMMs? [ISA | 561.1500]

We follow a six-step process to identify and assess RMMs. This process uses the information we have obtained during our risk assessment procedures, as well as any other relevant knowledge we may have.



Step a	Identify RMs using information from risk assessment procedures and considering the characteristics of the accounts and disclosures
Step b	Evaluate whether the identified RMs relate pervasively to the financial statements as a whole and potentially affect many assertions
Step c	Evaluate the types of potential misstatements that could result from the identified risks and the accounts, disclosures and assertions that could be affected
Step d	Assess the likelihood and magnitude of potential misstatements, including the possibility of multiple misstatements to determine RMMs and assess inherent risk

Step e	Identify significant accounts and disclosures and their relevant assertions
Step f	Determine whether any of the identified and assessed RMMs are significant risks

As part of this six-step process we also document our rationale for significant judgements made regarding the identification and assessment of RMMs.

1.1 Identify risks of misstatement [ISA | 562]

What do we do?

Identify risks of misstatement using information from risk assessment procedures and considering the characteristics of the accounts and disclosures

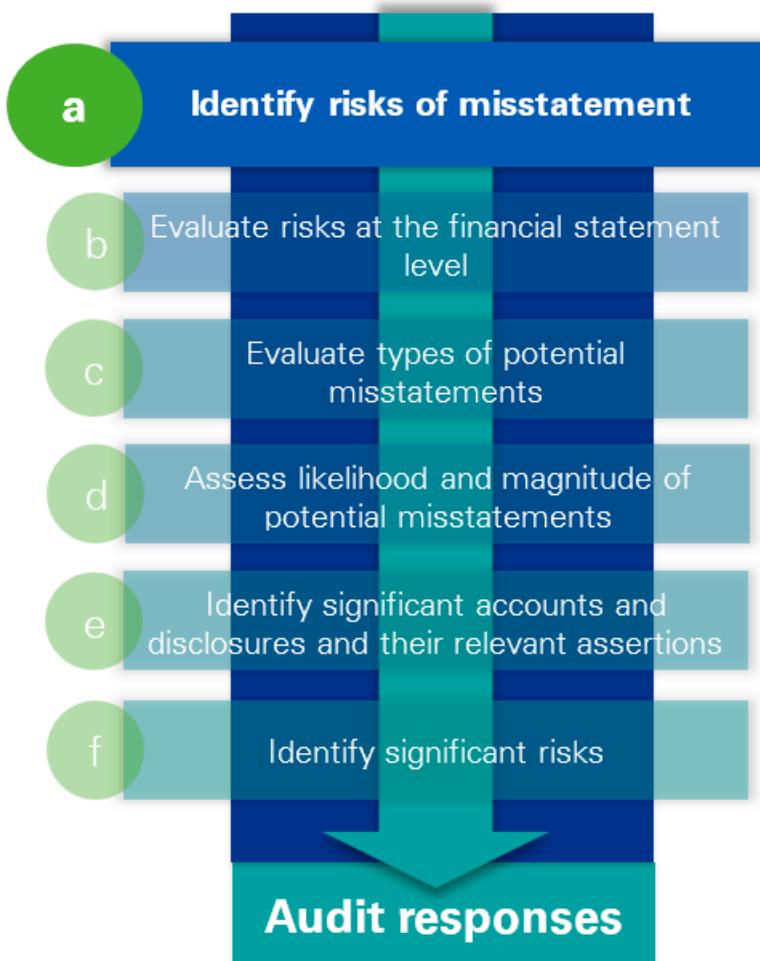
Why do we do this?

Understanding the population of risks of misstatement, allows us to narrow the population down to those risks that are risks of material misstatements (RMMs) to provide a basis for designing and performing further audit procedures.



Execute the Audit

Where are we in our risk assessment? [ISA | 562.1300]



What are risks of misstatement? [ISA | 562.1400]

Risks of misstatement (RMs) are risks that could result in a misstatement to the financial statements. There are two types of RMs.

Type of risks	What are they?	Example
Assertion-level RMs	<p>Risks that:</p> <ul style="list-style-type: none"> • relate to specific assertions for classes of transactions, account balances, or disclosures; and • relate to misstatements that can 	We expect assertion-level RMs to be similar across entities with similar types of transactions Additions to property, plant and equipment are not completely identified and recorded.

	arise when the financial reporting framework (e.g. IFRS, US GAAP), is not applied appropriately		
Financial statement-level RMs	<p>Risks that:</p> <ul style="list-style-type: none"> • relate pervasively to the financial statements as a whole • may affect many accounts and/or assertions • don't necessarily relate to applying particular accounting policies or principles • may arise from the entity and its environment, including business risks and broad internal control issues 	We expect financial statement-level RMs to be distinct to a particular entity or industry, and more dependent on the entity and its environment	Weakening economic conditions that negatively affect the value of many of the entity's assets

How do we identify RMs? [ISA | 562.8601]

To identify an RM, we consider all information gathered during audit planning and our risk assessment procedures.

When we learn something during the audit, it helps to ask ourselves:



What risks or problems could arise, resulting in a misstatement to one or more accounts or disclosures?

We draw on both our knowledge from risk assessment and our general knowledge about the nature of the accounts and disclosures and how they work — e.g. specific industry knowledge and general accounting knowledge.

Identification of an RM is based on whether it applies to the entity during the current period (e.g. did the entity have this type of transactions in the audit period?) and not based on hypothetical situations (e.g. could it happen to the entity?). For example, if the risk applies to other entities within the industry but the entity under audit does not have that type of transaction, we do not identify it as an RM.

The table below sets out examples of the types of information we may obtain during risk assessment and one instance of an RM that we might identify. However, our risk assessment will help us to identify many RMs, including those that relate to error or fraud.

Information gained during risk assessment	Example RM
One of the entity's external analysts recently reduced their stock price target for the entity's stock to 30% below the current price because the entity is not meeting the analyst's quarterly sales forecasts	For performance obligations satisfied at a point in time, revenue is not recognized when control is transferred to the customer, resulting in revenue not being recognized in the correct period (this may also be a fraud risk).
The entity has certain revenue streams with significant variable consideration that is difficult to determine	
We notice significant swings in revenue between quarters	
Sales have decreased and accounts receivable increased, when we expect the two metrics to move in the same direction	Receivables are not accurately recorded.
Rapid technological changes in the industry render certain products that the entity sells obsolete	An inappropriate amount is estimated for the net realizable value (NRV) of inventory, or an inaccurate amount is recorded for the lower of cost or NRV.
There is unfavorable change in the inventory turnover ratio from the prior period	

A significant lawsuit threatens the entity	Loss contingencies are not completely identified and/or accurately recorded.
A new accounting standard is being adopted in the current period	Disclosures of significant accounting policies or principles that are an integral part of the financial statements are incomplete, inaccurate, or not fairly presented.

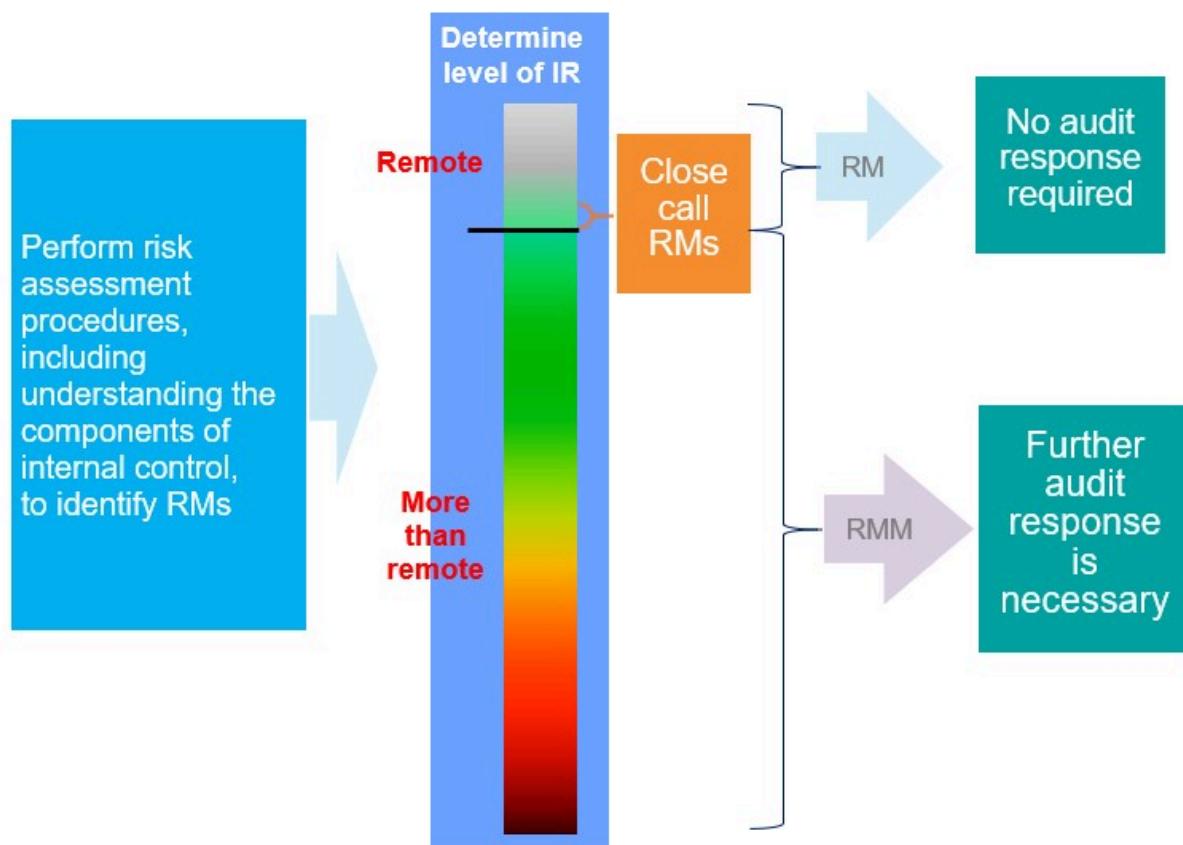
Do we document every RM we identify? [ISA | 562.8602]

No. We only document those RMs that we identify and assess as RMMs or close call RMs.

We evidence our considerations for close call RMs so that it helps support our thought process and gives a reviewer insight into why we concluded that a particular RM is not a RMM. It also helps demonstrate how we apply professional scepticism in our audit.

What are close call RMs? [ISA | 562.8604]

We think about inherent risk as a continuum - different RMs may fall at different points along that continuum. There is a point along the continuum where an RM becomes an RMM. Close call RMs are RMs where we assess the risk as being on the threshold or close to the threshold between RMs and RMMs.



If we are struggling to decide whether an RM is an RMM, or there is a debate on it within the engagement team (e.g. during our [RAPD meeting](#)), those are indicators of a close call RM.

In order to decide whether an RM is an RMM or not, refer to the factors discussed in the question '[What factors do we consider in assessing likelihood and magnitude and level of inherent risk?](#)'.

Not assessing a risk as an RMM has ramifications — it means we don't address it further in our audit*.

* There are certain areas within the financial reporting process where procedures are always performed even if there is no RMM (e.g. disclosures: agree/reconcile information in the disclosure to the underlying accounting records).

[Group Audit | Do we identify different risks in a group audit? \[ISA | 562.10975\]](#)

Yes. As the group auditor, we also identify RMMs related to the consolidation process, including on sub-consolidations, which are not linked to any specific significant accounts. However, we respond to consolidation RMMs similar to assertion-level RMMs (i.e., design substantive procedures and when applicable, identify PRPs and relevant control activities), rather than designing overall responses like we do for financial statement-level RMMs.

[How do we identify risks related to disclosures? \[ISA | 562.1700\]](#)

Information obtained during our risk assessment procedures may indicate the existence of RMs related to disclosures, which may include omissions, presentation of inaccurate or incomplete disclosures and obscuring financial information.

Obtaining that information may involve, for example:

- identifying possible constraints on the availability of capital and credit;
- determining that there are certain entities or business segments to be sold;
- learning about inquiries into the entity's operations or financial results by regulatory or government bodies;
- identifying new or evolving legal matters affecting the entity;
- identifying transactions that are recorded based on management's intent — e.g. a bond investment where management intends to hold the assets until their scheduled maturity (held-to-maturity) versus one where management are willing to sell (available-for-sale);
- identifying new accounting pronouncements that could apply to the entity;
- identifying events or circumstances that could lead to recognizing an impairment loss;
- learning about changes in assumptions about the future;
- identifying additional related parties and related party transactions;
- identifying new share-based payment arrangements; or
- identifying changes in assumptions used in the entity's valuation techniques.

[Group Audit or Component Audit | How do we identify RMMs of the group financial statements? \[ISA | 562.2100\]](#)

It is an iterative process. We follow the same process for identifying RMMs as in the stand-alone audit.

However, since most assertion-level RMMs of the group financial statements, or group RMMs, will arise in components, we, as the group auditor, will often involve component auditors when identifying the group RMMs.

As the group auditor, based upon our understanding of the group and its environment, the applicable reporting framework and the consistency of accounting policies and practices across the group, and the [group's system of internal control](#), we develop an initial expectation of accounts and disclosures that have potential group RMMs (i.e. potential significant accounts and disclosures).

Based on the initial expectations, we may involve component auditors in risk assessment procedures to identify and assess RMMs in those potential significant accounts and disclosures, because they may have direct knowledge and experience with the components that may be helpful in understanding the activities and related risks, and where RMMs of the group financial statements may arise in relation to those components.

[Group Audit | Who is responsible for identifying risks of material misstatement in a group audit?](#) [ISA | 562.160252]

The lead group auditor takes responsibility for identifying the risks of material misstatement of the group financial statements in a group audit.

[Group Audit | What does 'take responsibility for' mean?](#) [ISA | 562.160253]

'Take responsibility for' means the lead group auditor may either design and/or perform procedures, tasks, or actions themselves or are permitted to assign the design and/or performance of procedures, tasks or actions to other appropriately skilled or suitably experienced members of the engagement team, including component auditors.

Assigning the design and/or performance of procedures to another member of the engagement team, however, does not relieve the lead group auditor of their responsibility for the overall design and performance of the audit

[Group Audit or Component Audit | Do we document every RMM of the group financial statements in the group engagement file?](#) [ISA | 562.1900]

No. As the group auditor, we identify RMMs of the group financial statements, or group RMMs, in the group engagement file to the extent that they relate to:

- the consolidation process and the preparation of the consolidated financial statements
- those RMMs that arise at the group level due to the activities performed by group management. For example, RMMs related to deferred tax assets not being recoverable and goodwill not being appropriately valued may be addressed by group management.
- Elevated RMMs and significant risks of the group financial statements

Component auditors document group RMMs that arise at the component in their engagement file when:

- performing risk assessment procedures to help the group auditor identify and assess group RMMs and/or
- performing further audit procedures over group RMMs

Where we, as the group auditor, also perform work at a component, we document the group RMMs arising from processes occurring at the component level in the group or component engagement file.

[At what level do we identify our RMs?](#) [ISA | 562.6461]

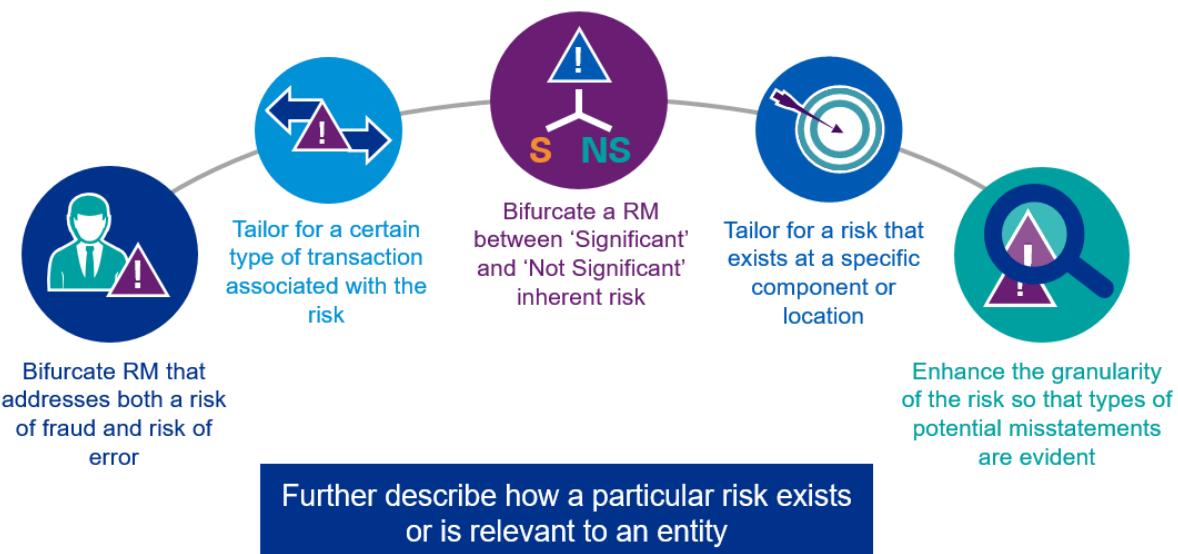
We identify risks at a granular enough level to design our audit procedures to address the specific risks we identify and assess — so failing to identify risks at the right level can lead us to perform the wrong procedures.

The risks captured in the Library are at an appropriately granular level. However, the description from the Library can be enhanced with an additional risk description where appropriate.

[When might we include an 'additional risk description'? \[ISA | 562.11016\]](#)

We may include an 'additional risk description' to enhance the granularity of our risks, which can be particularly helpful in the following circumstances:

Additional risk descriptions



Additional risk descriptions may not be necessary for every risk. However, they can help us further describe the specific risk and its relevance to an entity, as well as help support how our assessment and planned audit response is responsive to the specific risk.

[When would we identify a custom risk? \[ISA | 562.6462\]](#)

We may identify risks that are unique to an entity and are not in the Library, from our risk assessment procedures. However, because most risks are closely tied to the accounting standards and the risks in the Library are derived from evaluating the risks from the accounting standards, you may not identify any custom risks.

But before we decide to identify custom risks, we think about:

- whether we can use the additional risk description functionality to tailor an existing risk from the library (e.g. rather than identifying a custom risk, we start with the existing risk and tailor it, but retain the meta tagging of the library core account / risk, etc.)
- whether we may have confused a process risk point as a risk; and
- that certain required content, minimum expected substantive procedures, etc. may not be delivered in the workflow.

When it is appropriate to add a custom risk, we describe the custom risk with appropriate granularity such that the risk is not too broad, not too narrow.

For example, when determining whether a custom risk for revenue cut-off is necessary, we consider that:

We can link the risk related to revenue cut-off to the risk of misstatement below from the ASC Topic 606 /IFRS 15:

- Over-time revenue recognition: 'An inappropriate, inconsistent or inaccurate measure of progress is used when revenue is recognized over time.'
- Point-in-time revenue recognition: 'For performance obligations satisfied at a point in time, revenue is not recognized when control is transferred to the customer, resulting in revenue not being recognized in the correct period.'

When our inherent risk assessment is different for revenue cut-off, we duplicate the RM, and use the additional risk description to further describe the risk. Therefore, it is not necessary to create a custom risk for revenue cut-off in this example.

[When might we disaggregate RMs?](#) [ISA | 562.11112]

When performing our risk assessment, we may identify situations when it is appropriate to duplicate an RM to better disaggregate an account/location/fund/component because of differing risk profiles.

For example, we may disaggregate an RM related to the physical existence of inventory at warehouses because the inventory management process at warehouses is different (i.e. some warehouses are subject to cycle counts and use a perpetual inventory system and some warehouses are subject to periodic inventory counts and use a periodic inventory systems).

[Is there anything additional we consider when accounting estimates are involved?](#) [ISA | 562.10984]

Yes. We perform the risk assessment procedures related to accounting estimates in the KAEG chapter on estimates (ISA 540, AU-C 540 or AS 2501).

[Is there anything additional we consider when the financial reporting process is involved?](#) [ISA | 562.6463]

Yes. 'Risk considerations' are used when available, within the financial reporting process screens in KPMG Clara workflow - i.e. financial statements, cash flows, segment information, disclosures - and may assist us in:

- identifying the risks of misstatement (RMs);
- determining whether the RMs are risks of material misstatement (RMMs); and/or
- designing appropriate audit responses for those assessed as RMMs.

[What are 'risk considerations' in the context of the financial reporting process?](#) [ISA | 562.6464]

'Risk considerations' are requirements from the applicable financial reporting framework that provide more detailed information about the RMs within the financial reporting process screens in KPMG Clara workflow, which are more general in nature (i.e. not at a granular level).

1.2 Evaluate RMs at the financial statement level [ISA]

| 563]

What do we do?

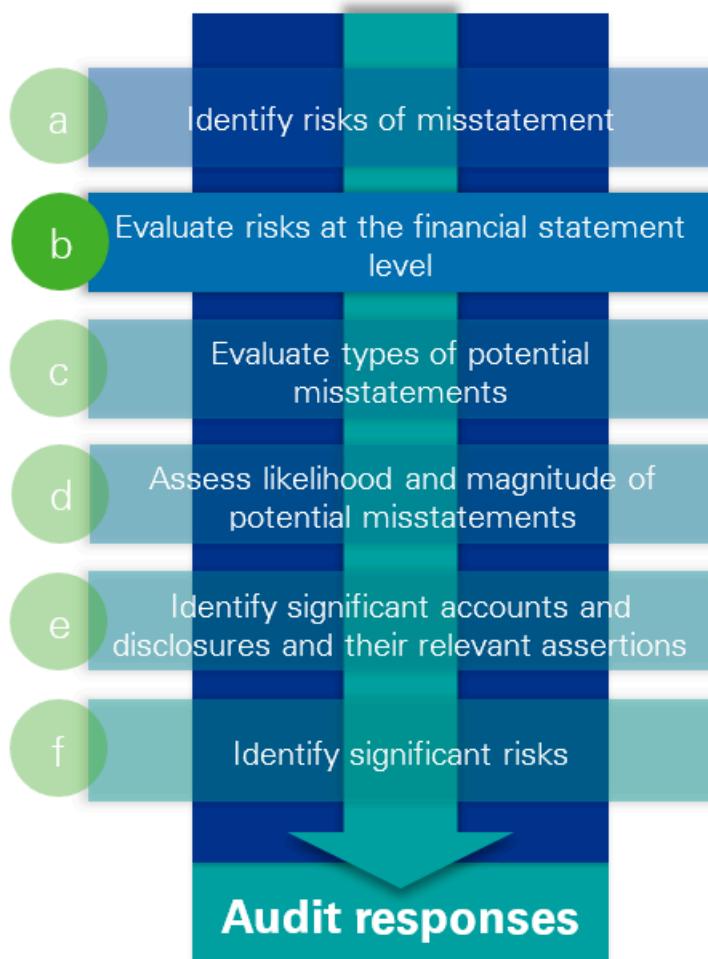
Evaluate whether the identified risks of misstatement are financial statement level risks of misstatement.

Why do we do this?

Understanding the risks that relate pervasively to the financial statements as a whole will help us better think about the types of potential misstatement that could arise and how we design our audit responses.

Execute the Audit

[Where are we in our risk assessment?](#) [ISA | 563.1300]



[What are financial statement level RMs?](#) [ISA | 563.1400]

Financial statement level RMs are risks that have a pervasive effect on the financial statements as a whole and/or relate to many assertions. They may be risks arising from the entity and its environment, including many business risks and broad internal control issues.

[How do financial statement level RMs differ from assertion level RMs?](#) [ISA | 563.11455]

Financial statement level RMs differ from assertion-level RMs because:

- they may not relate to how specific transactions are accounted for under the financial reporting framework; and
- their effects can't be narrowed down to a few specific accounts, disclosures or assertions.

[Why do we evaluate whether an RM relates pervasively to the financial statements?](#) [ISA | 563.1500]

We evaluate whether an RM relates pervasively to the financial statements because it affects how we design our audit response. Our responses to address assertion-level risks are normally narrower in focus - e.g. designing and performing a specific audit procedure - than our responses to address risks that relate to the financial statements as a whole (see activity '- e.g. changing how we conduct our audit, such as increasing the persuasiveness of all our audit procedures.

[How do we identify financial statement-level RMs?](#) [ISA | 563.1600]

We use the information gathered during risk assessment to identify financial statement-level RMs. However, we pay particular attention to those broader business risks arising from the entity and its environment, and the broader internal control issues we have identified. It may be helpful to pose the following question when determining if an RM is at a financial statement level:



Could the RM potentially affect many or all significant accounts, disclosures and relevant assertions in the financial statements?

If our response to that question is 'yes', it may be a financial-statement level RM.

The following table illustrates how information obtained during risk assessment may rise to a financial-statement level risk:

Information gathered during our risk assessment	Translation to risks of misstatement	Is it a risk at the financial statement level?
An entity has no formal hiring policies and practices and does not appropriately evaluate the skills and competency of individuals hired in accounting and financial reporting roles. The entity hires a new Corporate Controller who is responsible	Financial reporting is under the direction of the Corporate Controller, so this risk potentially affects all accounts, disclosures and assertions.	Due to the lack of formal hiring policies and practices, the weakness in the entity's control environment is pervasive, so it is a financial statement-level RM.

for financial reporting during the period.		
A negative tone at the top has created an entity-wide attitude that internal controls and accurate financial reporting are not important, including that management do not hold individuals accountable for their internal control responsibilities.	<p>It may be difficult to associate this risk with any specific financial statement accounts, disclosures or assertions — because it could affect <i>all</i> of them.</p>	Because of the poor tone at the top, there is a weakness in the entity's control environment and the financial reporting process. This is a pervasive risk, so it is a financial statement-level RM.
An entity has been rapidly expanding its business, but there is significant uncertainty about the long-term demand for its products.	<p>We may be able to link this business risk to the valuation assertion of inventory. However, it may also affect many other accounts, disclosures and assertions.</p> <p>Significant uncertainty about demand for the entity's products could also affect the value of several other assets, including:</p> <ul style="list-style-type: none"> • tangible and intangible long-lived assets • goodwill • deferred tax assets, • as well as risks associated with the classification of debt and liquidity/going concern disclosures. 	The entity's business expansion and the uncertainty of demand represent a financial statement-level RM. This is because the risk is pervasive and could affect many accounts, disclosures and assertions.

What if a risk affects many but not all assertions? [ISA | 563.1800]

A financial statement-level risk that affects all accounts differs from a risk that has a pervasive effect and affects many (but not all) accounts, disclosures or assertions.

For example, we identify a risk related to declining economic factors that causes an entity to have significantly reduced or negative margins for the foreseeable future.

On the surface, this may seem like a risk that relates pervasively to the financial statements as a whole. However, we may find that the risk affects a set of specific accounts or disclosures - e.g. long-lived assets, goodwill, intangible assets, deferred tax assets, debt, liquidity/going concern disclosures.

This risk still represents a financial statement-level risk because it potentially affects many different accounts, disclosures and assertions.

In response to this financial statement-level risk, we may not identify any additional assertion-level risks — but we may re-evaluate our inherent risk assessment for the assertion-level risks related to the valuation of the affected accounts.

1.3 Evaluate types of potential misstatements [ISA | 564]

What do we do?

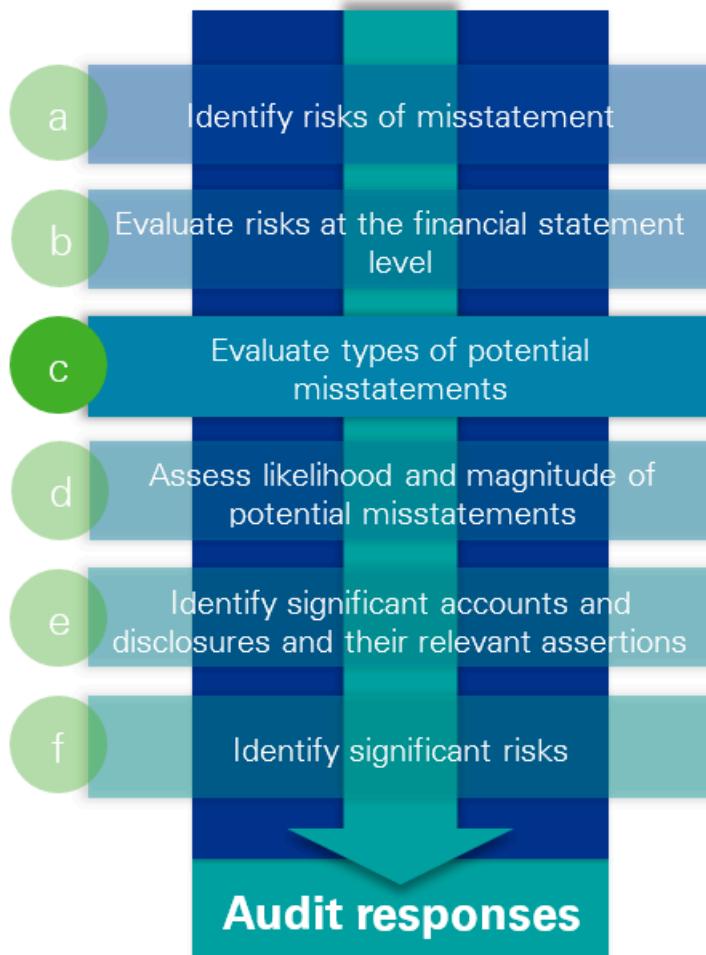
Evaluate the types of potential misstatements that could result from the identified risks and the accounts, disclosures, and assertions that could be affected - i.e. what could go wrong in the accounts and disclosures

Why do we do this?

To determine which risks rise to a risk of *material* misstatement (RMM), we evaluate the types of misstatements that could arise from a risk. This allows us to better assess the risk and clearly link it to the accounts, disclosures and assertions that could be affected.

Execute the Audit

[Where are we in our risk assessment?](#) [ISA | 564.1300]



What is a type of potential misstatement? [ISA | 564.1400]

'Types of potential misstatements' are the various ways an account or disclosure could be affected by a risk of misstatement. Thinking about the types of potential misstatement enables us to identify the risk at a granular level.

First, we think about how the risk could affect the financial statements broadly, by asking ourselves "what could go wrong" because of this risk. Then, once we understand this, we can think about how specific accounts, disclosures and assertions might be affected.

For example, we may first determine that a risk affects how the entity records the inventory it buys and sells. This information might help us better identify potential misstatements and their possible impact on inventory and cost of goods sold.

How might the types of potential misstatements affect accounts, disclosures and assertions? [ISA | 564.1500]

Information gained during risk assessment	Example RM	Example type of potential misstatement	Example account / disclosure and assertion
One of the entity's external analysts recently reduced their stock price target for the entity's stock to 30% below the current price as a result of the entity not meeting the analyst's quarterly sales forecasts	For performance obligations satisfied at a point in time, revenue is not recognized when control is transferred to the customer, resulting in revenue not being recognized in the correct period (this may also be a fraud risk).	The risk could result in an overstatement of revenue	Existence of revenue
The entity has certain revenue streams with significant variable consideration that is difficult to determine			
We notice significant swings in revenue between quarters.			
Sales have decreased and accounts receivable have increased, when we expect the two metrics to move in the same direction	Receivables are not accurately recorded.	The risk could result in an understatement of allowance for doubtful accounts	Valuation of the allowance for doubtful accounts
Rapid technological changes in the industry render certain products	An inappropriate amount is estimated for the net realizable value (NRV) of inventory, or an	The risk could result in an overstatement of inventory	Valuation of inventory

that the entity sells obsolete	inaccurate amount is recorded for the lower of cost or NRV		
There is unfavorable change in the inventory turnover ratio from the prior period			
A significant lawsuit threatens the entity	Loss contingencies are not completely identified and/or accurately recorded.	The risk could result in an omitted disclosure for commitments and contingencies	Presentation and disclosure of commitments and contingencies
A new accounting standard is being adopted in the current period	Disclosures of significant accounting policies or principles that are an integral part of the financial statements are incomplete, inaccurate, or not fairly presented	The risk could result in an omitted disclosure under a new accounting standard	Presentation and disclosure under the new accounting standard

At what level do we identify our RMs and the related types of potential misstatement? [ISA | 564.1600]

We identify risks at a granular enough level to understand what specific types of potential misstatements could result from them. We design our audit procedures to address the specific risks we identify and assess — so failing to identify risks at the right level can lead us to perform the wrong procedures.

The risks captured in the Library are at an appropriately granular level to portray the types of potential misstatement that could occur.

When it is appropriate to add a custom risk, we describe the custom risk with appropriate granularity such that the risk is not too broad, not too narrow, and the type of potential misstatement is evident.

When would we identify a custom risk? [ISA | 564.6462]

We may identify risks that are unique to an entity and are not in the Library, from our risk assessment procedures. However, because most risks are closely tied to the accounting standards and the risks in the Library are derived from evaluating the risks from the accounting standards, you may not identify any custom risks.

But before we decide to identify custom risks, we think about:

- whether we can use the additional risk description functionality to tailor an existing risk from the library (e.g. rather than identifying a custom risk, we start with the existing risk and tailor it, but retain the meta tagging of the library core account / risk, etc.)
- whether we may have confused a process risk point as a risk; and
- that certain required content, minimum expected substantive procedures, etc. may not be delivered in the workflow.

When it is appropriate to add a custom risk, we describe the custom risk with appropriate granularity such that the risk is not too broad, not too narrow.

For example, when determining whether a custom risk for revenue cut-off is necessary, we consider that:

We can link the risk related to revenue cut-off to the risk of misstatement below from the ASC Topic 606 /IFRS 15:

- Over-time revenue recognition: 'An inappropriate, inconsistent or inaccurate measure of progress is used when revenue is recognized over time.'
- Point-in-time revenue recognition: 'For performance obligations satisfied at a point in time, revenue is not recognized when control is transferred to the customer, resulting in revenue not being recognized in the correct period.'

When our inherent risk assessment is different for revenue cut-off, we duplicate the RM, and use the additional risk description to further describe the risk. Therefore, it is not necessary to create a custom risk for revenue cut-off in this example.

[What do we do with financial statement-level RMs?](#) [ISA | 564.1700]

We evaluate how financial statement-level risks could affect assertion-level risks.

[How do we evaluate how financial statement-level risks affect assertion-level risks?](#) [ISA | 564.1800]

We consider the nature of the pervasive effect, and attempt to narrow down the effects to a specific set of accounts, disclosures or specific assertions. We do this by following the same steps that we do for any other risk — by evaluating the types of potential misstatements that could occur from the risk and assessing the likelihood and magnitude of potential misstatements.

For example, suppose we determine that the entity has no consistent hiring policies and practices, and does not appropriately evaluate the skills and competency of individuals hired in accounting and financial reporting roles.

The entity hired only one new individual during the period, an Accounts Payable Team Supervisor.

Given the specific activities under the management of this role, the team conclude that:

- the issue still represents a weakness in the entity's control environment; and
- the effects of this risk may be limited to a specific set of accounts, disclosures and assertions related to accounts payable transactions — as opposed to the financial statements as a whole.

However, we may not always be able to narrow down the effects of a financial statement-level RM to a specific set of accounts, disclosures or specific assertions.

For example, assume the same facts as in the example above, except that during the period the entity hired a Corporate Controller responsible for financial reporting.

We assess that, given the lack of hiring policies and practices, the weakness in the entity's control environment is a financial statement-level risk, due to its more pervasive nature.

In this example, the effects of the weakness could broadly affect all of financial reporting, so it's difficult to narrow down the risk to any specific assertion.

1.4 Assess likelihood and magnitude of potential misstatements to determine RMMs [ISA | 565]

What do we do?

Assess the likelihood and magnitude of potential misstatements, including the possibility of multiple misstatements, to determine RMMs and inherent risk

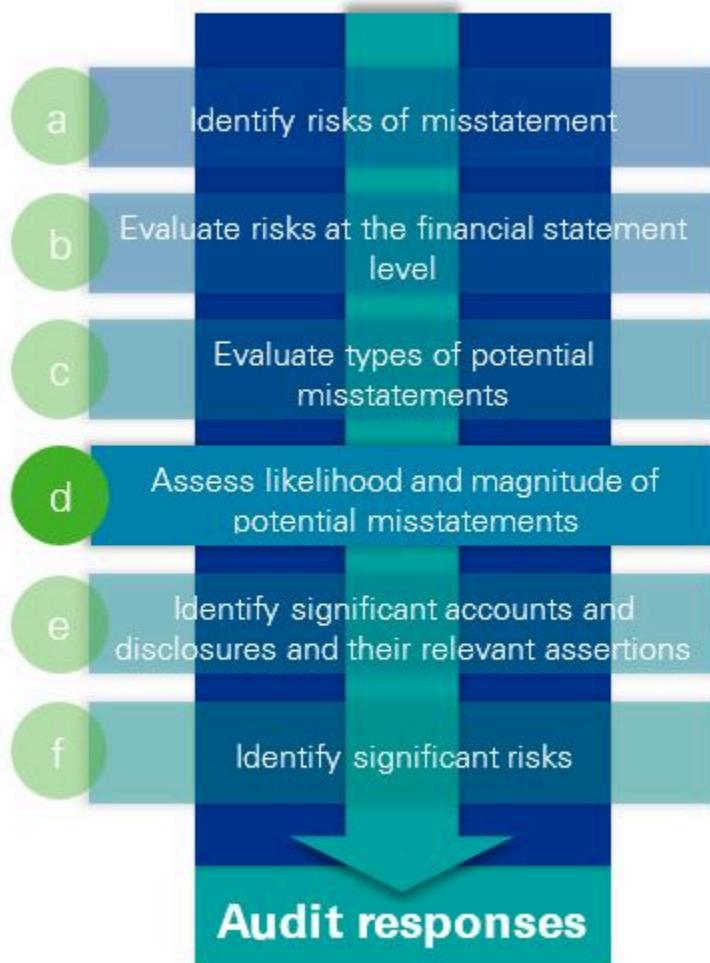
Why do we do this?

We assess the likelihood and magnitude of potential misstatements to:

- Identify risks of material misstatements (RMMs);
- Determine where on the continuum of inherent risk the RMM sits (which informs our design of further audit procedures to respond to the RMM); and
- Assist in the determination of significant risks.

Execute the Audit

Where are we in our risk assessment? [ISA | 565.1300]

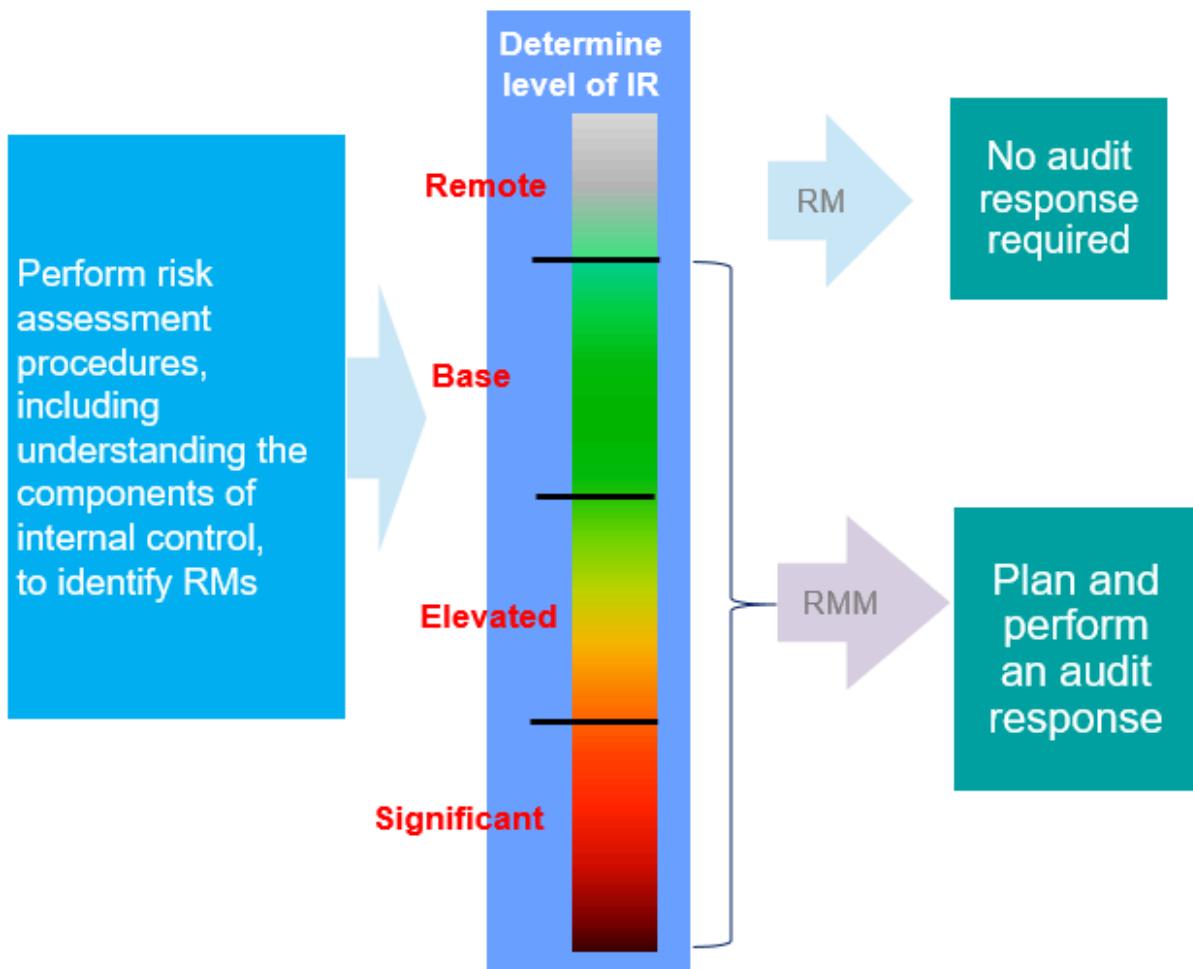


How does assessing likelihood and magnitude of potential misstatements help us determine RMMs and level of inherent risk? [ISA | 565.8701]

Assessing the likelihood and magnitude of potential misstatements helps us gauge where we are on the inherent risk continuum and whether we've reached the level where inherent risk is more than remote for that risk. An RM is simply a risk on the "remote" part of the inherent risk continuum, where no audit response is necessary*.

When the likelihood and magnitude of potential misstatement is more than remote, we assess inherent risk for each RMM at one of three levels - Base, Elevated or Significant, depending on where it is on the continuum (significant risks are closer to the upper end of the continuum).

The following diagram illustrates the inherent risk continuum and how we think about RMs, RMMs and our inherent risk assessment in relation to that continuum:



Not assessing a risk as an RMM has ramifications — it means we don't address it further in our audit*.

* There are certain areas within the financial reporting process where procedures are always performed even if there is no RMM (e.g. disclosures: agree/reconcile information in the disclosure to the underlying accounting records).

How do internal controls affect our assessment of likelihood and magnitude? [ISA | 565.1700]

We don't consider the effects of control activities when we determine which risks are RMMs.

Our understanding of CERAMIC, however, can influence our assessment of inherent risk. When there are deficiencies in CERAMIC, it may highlight an increased chance of material misstatements occurring. For example, when we identify deficiencies related to the entity's ability to attract, develop, and retain competent individuals, there is a higher likelihood of misstatements occurring broadly because unqualified or lower competence individuals are more prone to record transactions incorrectly.

How do we assess likelihood and magnitude? [ISA | 565.8704]

The table below sets out examples of how an engagement team might assess likelihood and magnitude when they determine RMMs and level of inherent risk.

Description of RM and related accounts / disclosures and assertions	Considerations related to likelihood and magnitude of potential misstatement	Assessment of RMM and level of inherent risk
Prepayments are not accurately recorded or do not exist. (Existence of prepaid expenses)	<ul style="list-style-type: none"> • The size of the prepaid expenses account is less than two times performance materiality and has not changed significantly from the prior year, which is consistent with our expectations. • The account comprises a small number of routine prepayments to vendors for materials that the entity expects to consume within 12 months. • The individual balances are homogeneous and not subject to accounting complexities. • There is no risk of aggregation with other non-significant accounts. 	<p>Although the engagement team has identified an RM, they assess that the likelihood and magnitude that a material misstatement may occur is remote given the low number and dollar value of transactions and lack of accounting complexity associated with the risk.</p> <p>The engagement team assess the risk as not an RMM.</p>
Indicators that an asset or cash-generating unit may be impaired are not appropriately identified. (Valuation of PP&E)	<ul style="list-style-type: none"> • The size of the PP&E account is relatively large (40 times performance materiality) and has not changed significantly from the prior year. • All of the PP&E is included within a single long-lived asset group. • The information identified from our inquiries of management indicated no changes in the use of the PP&E. • The favorable interim results of operations reviewed 	<p>Given the more favorable economic conditions and reduced complexity (e.g. not having a significant number of different asset groups), there is a <i>lower</i> likelihood of a material misstatement occurring.</p> <p>However, given the magnitude of the balance of PP&E and susceptibility in recent periods to changes in value, the engagement team concludes that there is still <i>more than a remote</i> chance of a material misstatement occurring.</p>

	<p>in our planning analytical procedures indicate a reduced risk of exposure to losses in this account.</p> <ul style="list-style-type: none"> Asset values have fluctuated in the past and there have been impairments taken in the last three years. 	<p>The engagement team assesses the risk to be an RMM and inherent risk is assessed to be Base.</p>
<p>An inappropriate amount is estimated and recorded for the value of rights of return.</p> <p>Additional risk description: Risk relates to products sold through a new distribution channel. (Existence and Accuracy of revenue and accounts receivable)</p>	<ul style="list-style-type: none"> Based on our risk assessment procedures, we identified that the entity planned to begin selling a new product to resellers in the last quarter of the fiscal year. Previously, the entity had only sold its products directly to end users and these new contracts include unique rights of return. The entity has relatively little experience with product returns and limited data related to these new sales arrangements. Although the product is new, the entity expects its sales volumes to represent approximately 10% of revenue for the year. 	<p>Given the complexity and judgment in determining the estimate for returns, there is an increased chance that a misstatement could occur. Considering the increased likelihood along with the fact that the revenue from the new product is a substantial portion of total revenues, resulting in magnitude of potential misstatement being material, the engagement team concludes that there is more than a remote chance of a material misstatement occurring.</p> <p>The engagement team assesses the risk to be an RMM and considering the degree of complexity in the measurement of the estimate for returns, and the wide range of measurement uncertainty, the inherent risk assessment is Significant.</p>
<p>The disclosure is incomplete, inaccurate, or not fairly presented.</p> <p>Additional risk description: Risk related to the required disclosures of</p>	<ul style="list-style-type: none"> The entity is manufacturer with point-of-sale revenue recognition. Revenue is material to the financial statements and important to its users. There have not been new accounting pronouncements or changes in the entity's accounting policies for 	<p>Given there is no judgment or complexity in the policies, and no changes nor expected changes in the revenue accounting policies disclosures, the engagement team assesses the risk to be an RM.</p>

revenue accounting policies	revenue in the past two years.	
The disclosure is incomplete, inaccurate, or not fairly presented. Additional risk description: Risk relates to the required disclosure of disaggregated revenue amounts. (Presentation of revenue)	<ul style="list-style-type: none"> Revenue is material to the financial statements and important to users of the financial statements. The entity completed an acquisition in the current reporting period, adding a new business line in a geographic region in which the entity has not previously operated. 	<p>Given the magnitude of the balance of revenue and changes in the disclosure from the prior period given the entity's acquisition, the engagement team assesses the risk to be an RMM.</p> <p>As disaggregating revenue amounts does not require judgment, inherent risk is assessed to be Base.</p>

Group Audit | How do we assess RMMs of the group financial statements? [ISA | 565.2200]

As the group auditor, we assess the risks of material misstatement of the group financial statements, whether due to fraud or error, including with respect to the consolidation process by applying the same guidance for assessing RMMs in a stand-alone audit. However, since most assertion-level RMMs of the group financial statements, or group RMMs, will arise in components, we, as the group auditor, will often involve component auditors in risk assessment procedures to assess group RMMs.

Group Audit | Who is responsible for assessing the RMMs of the group financial statements? [ISA | 565.160255]

The lead group auditor takes responsibility for assessing the RMMs of the group financial statements in a group audit.

Group Audit | What does 'take responsibility for' mean? [ISA | 565.160253]

'Take responsibility for' means the lead group auditor may either design and/or perform procedures, tasks, or actions themselves or are permitted to assign the design and/or performance of procedures, tasks or actions to other appropriately skilled or suitably experienced members of the engagement team, including component auditors.

Assigning the design and/or performance of procedures to another member of the engagement team, however, does not relieve the lead group auditor of their responsibility for the overall design and performance of the audit.

Group Audit | Do we assess different RMMs in a group audit? [ISA | 565.11097]

Yes. As the group auditor, we also assess RMMs related to the consolidation process, including sub-consolidations, which are not linked to any specific significant accounts or disclosures. However, we respond to consolidation RMMs similar to assertion-level RMMs (i.e., design substantive procedures and when applicable, identify PRPs and relevant control activities) rather than designing overall responses like we do for financial statement-level RMMs.

Group Audit | Why may RMMs of the group financial statements be assessed differently at components? [ISA | 565.160257]

Examples of when an RMM at the component may be assessed differently than the RMMs of the group financial statements include:

- the component auditor assesses the magnitude of potential misstatements associated with an RMM considering the component performance materiality for the component; however, the potential misstatement to the group financial statements is not considered material or at a magnitude that warrants the same assessment as that at the component; or
- RMMs at the component are identified based on an RMMs that relates to local financial reporting framework which are not RMMs under the financial reporting framework used by the group.

In circumstances where a component auditor has assessed an RMM as either Elevated or Significant that we as the group auditor have not assessed at the same inherent risk level, we document why we consider those RMMs not to be at the same inherent risk level.

For example, suppose that the group auditor has assessed RMMs associated with capitalized software costs as Base because the magnitude to the group financial statements is 2x group performance materiality.

However, a component auditor has assessed RMMs associated with capitalized software costs as Elevated due to the magnitude at the component and the judgment involved in determining the amounts to capitalize. The component auditor communicates this assessment to the group auditor.

The group auditor documents why the RMM is not assessed as Elevated for the group financial statements.

How do we determine whether our assessment of inherent risk for an RMM is Base, Elevated or Significant? [ISA | 565.8705]

In addition to our consideration of inherent risk factors (see question '[What are the inherent risk factors?](#)'), it may be helpful to:

- first determine which risks are closer to the upper end of the inherent risk continuum and are significant risks (see activity '[Determine significant risks](#)'); and
- then assess the remaining risks by evaluating whether they are relatively lower or higher on the inherent risk continuum — i.e. Base or Elevated.

When we are trying to determine whether a risk is Base or Elevated, it may be useful to compare our assessments across non-significant risks.

For example, suppose that:

- the engagement team have assessed risks associated with several smaller and less complex accounts — e.g. prepaid expenses — as Base; and
- they are trying to determine whether a risk associated with a higher-volume, more complex account is Base or Elevated.

The team may find it helpful to consider whether they really believe the lowest level of inherent risk — i.e. Base — makes sense for both types of risks.

Questioning this can help us better determine where the RMM falls on the continuum.

[What factors do we consider in assessing likelihood and magnitude and level of inherent risk?](#) [ISA | 565.2000]

We consider:

- Inherent risk factors;
- Significant risk factors (see question '[How do we determine whether any of the identified and assessed RMM are significant risks?](#)'); and
- Estimates risk factors, if applicable (see question '[What are the additional risk factors that we evaluate when identifying significant accounts and disclosures involving accounting estimates?](#)').

We consider each factor for each RM, to gauge whether it is an RMM, and if so where it sits on the inherent risk continuum. When considering these factors, a key consideration is the degree to which the inherent risk factors affect the combination of likelihood of misstatement occurring and magnitude of misstatement. The higher the combination of likelihood and magnitude, the higher the assessment of inherent risk; the lower the combination of likelihood and magnitude, the lower the assessment of inherent risk.

[What are the inherent risk factors?](#) [ISA | 565.8706]

The following table describes the inherent risk factors:

Inherent risk factors	Additional description and examples
Factors that affect the susceptibility to misstatement of an assertion about a class of transactions, account balance or disclosure	
<p>Quantitative or qualitative significance, including:</p> <ul style="list-style-type: none"> • Size and composition of the account • Nature of the account or disclosure • Existence of related party transactions in the account • Possibility of significant contingent liabilities arising from the activities reflected in the account or disclosure • Exposure to losses in the account 	<p>Size and composition: As the size of an account increases, so does the potential magnitude of a misstatement in that account or disclosure. Often, this is because in larger account balances, errors that represent a small percentage of the account balance may still exceed materiality. For example, a 2% misstatement in an account that is 60 times materiality exceeds materiality.</p> <p>Understanding the composition of an account helps us evaluate the other factors and determine whether relevant assertions exist for a particular account and whether there is an RMM we haven't yet identified and assessed.</p> <p>For example, if an entity has domestic sales and international sales, the risk for each type may be different. If there are uncertainties about a foreign countries' economic stability, there may be greater risk in their international operations than their domestic operations.</p>

Nature of accounts and disclosures: When we consider the nature, we think about numerous characteristics of an account, disclosure or assertion, including:

- its importance or prominence in the financial statements
- the way it is recorded or presented
- the basic types of transactions that affect it.

These factors, along with others, can affect how likely a material misstatement is to occur for a specific assertion.

For example:

- accrual balances, by their nature, often have more risk of understatement than overstatement
- assertions related to accounting estimates are more likely to contain a material misstatement related to the valuation assertion
- assertion disclosures related to revenue or significant judgments in applying the related revenue accounting policies or principles are important or prominent in the financial statements
- an accounting estimate often involves management making significant judgments about the assumptions to use. These judgments can involve uncertainty, and introduce more potential for human error.

Existence of related party transactions: Related party transactions involve close relationships between parties, so there is more chance that they might involve fraud or be inappropriate, and lack a clear business purpose and not be appropriately disclosed.

These issues may arise because the entity doesn't account for the transaction properly, or because the substance of a related party transaction might be different from its form.

For example, an entity may structure a related party transaction solely to avoid recording and disclosing a liability in the financial statements. The risk to the financial statements increases because the entity and its related parties control both sides of the transaction.

Given this risk, a material misstatement is more likely in an account that includes related party transactions.

Possibility of significant contingent liabilities: The nature of an entity's transactions and business activities could lead to significant contingencies.

For example, selling goods could lead to sales returns or warranty claims on defective products. Or certain fixed assets may exist (such as underground storage tanks containing gasoline) that could lead to asset retirement obligations or environmental liabilities.

Contingent liabilities may be difficult to identify, and judgment may be involved to determine the amount to be recorded or disclosed in the financial statements. Therefore, they may be more likely to contain a material misstatement.

Exposure to losses in the account: The more exposure an account has to losses, the more chance it may contain an error. Factors in the entity's general environment may expose a particular account to losses. We also think about accounts that may have lower recorded balances but a higher exposure to losses.

For example, an entity may record a small legal accrual, but face several lawsuits with potential unfavorable outcomes that expose it to significant losses. This potential for loss may increase the likelihood of material misstatement over the completeness, valuation and presentation assertions for the legal accrual.

Volume of activity, complexity and homogeneity of the individual transactions processed through the account or reflected in the disclosure

Volume : The more transactions processed through a class of transactions, account balance or reflected in a disclosure, the greater the chance that it contains a material misstatement. There is more risk that multiple items could be misstated that could aggregate to a material misstatement.

We consider the volume of transactions in all accounts and disclosures, but we don't dismiss those with smaller balances without carefully considering the volume of transactions.

For example, a cash account may have a zero balance at the period end, but the entity may process a high volume of cash transactions through it during the period. This may be an account with a reasonable possibility of a material misstatement.

Complexity: More complex transactions can suggest more judgment or present a greater opportunity for errors.

	<p>For example, transactions that result from complex calculations often have multiple inputs, each of which may present a possibility for error. Simple calculations with fewer inputs may have a lower chance of error.</p>
	<p>More complex calculations increase the likelihood of material misstatements related to particular assertions — e.g. valuation — of a particular account or disclosure.</p> <p><i>Homogeneity:</i> In certain cases, when transactions are homogeneous, misstatements in one transaction may indicate additional misstatements in others. As such, multiple errors could occur, which could increase the magnitude of any potential misstatement. In this case, the homogeneity may increase the possibility of a material misstatement. Conversely, when transactions lack uniformity in the composition of the items processed in the account or class of transactions may increase susceptibility to misstatement in the related account or disclosure.</p>
Susceptibility to misstatement due to error	<p>Some accounts, disclosures and assertions, by their nature, are more susceptible to misstatement - including those more likely to be affected by human error.</p> <p>This may be due to the types of transactions processed in an account, the nature of the account or disclosure itself, or many other factors.</p> <p>This higher susceptibility to misstatements increases the likelihood that a material misstatement will occur.</p> <p>For example, when substantial doubt about an entity's ability to continue as a going concern is raised but is alleviated by management's plans, the disclosures could be more susceptible to misstatement whether due to error or fraud.</p>
Factors relating to preparation of the information required by the financial reporting framework	
Complexity, including accounting and reporting complexities associated with the account or disclosure	Complexity arises either from the nature of the information or in the way that the required information is prepared, including when such preparation processes are more inherently difficult to apply.

	<p>For example, complexity may arise in calculating supplier rebate provisions because it may be necessary to take into account different commercial terms with many different suppliers, or many interrelated commercial terms that are all relevant in calculating the rebates due.</p> <p>As another example, complexity may arise in developing disclosures for a business combination because several individuals from different departments may be involved and different sources of information from multiple IT systems may be necessary in preparing the disclosures.</p>
	<p>Complex accounting and reporting can often:</p> <ul style="list-style-type: none"> • be more challenging for an entity to evaluate; • involve a greater degree of judgment; and • necessitate a greater degree of skill, knowledge and experience. <p>For example, accounting for income taxes can be complex, especially when an entity operates in multiple jurisdictions.</p>
	<p>Such complexities can make errors or incorrect judgments more prevalent, and increase the likelihood of material misstatement.</p> <p>Complexity may arise from changes in the applicable financial reporting framework that create new disclosure requirements, or changes in the entity's transactions and activities that result in new accounting policies or principles.</p>
Subjectivity (including judgment in the recognition or measurement of financial information related to the risk)	<p>Subjectivity arises from inherent limitations in the ability to prepare necessary information in an objective manner, due to limitations in the availability of knowledge or information, such that management may need to make an election or subjective judgment about the appropriate approach to take and about the resulting information to include in the financial statements.</p> <p>Because of different approaches to preparing the required information, different outcomes could result from appropriately applying the requirements of the applicable financial reporting framework. As limitations in knowledge or data increase, the subjectivity in the judgments that could be made by reasonably knowledgeable and independent individuals, and the diversity in possible outcomes of those judgments, will also increase.</p>

	<p>For example, management's selection of a valuation technique or model for a non-current asset, such as investment properties.</p> <p>Additionally, subjectivity can arise for disclosures that are subjective in relation to their preparation.</p> <p>For example, disclosures related to a lawsuit and related loss contingency could be more susceptible to misstatement given their subjective nature.</p>
<p>Change(s), including changes from the prior period in account/disclosure characteristics</p> <p>Risk relates to recent significant economic, accounting or other developments</p>	<p>Results from events or conditions that, over time, affect the entity's business or the economic, accounting, regulatory, industry or other aspects of the environment in which it operates, when the effects of those events or conditions are reflected in the required information. Such events or conditions may occur during, or between, financial reporting periods.</p> <p>For example, change may result from developments in the requirements of the applicable financial reporting framework, or in the entity and its business model, or in the environment in which the entity operates. Such change may affect management's assumptions and judgments, including as they relate to management's selection of accounting policies or principles or how accounting estimates are made or related disclosures are determined.</p> <p>As another example, rising interest rates may affect management's projected financial information utilized in the valuation of goodwill, including an impact on the discount rates used and projected revenue and expenses. This change in business environment may also have an impact on management's disclosures of judgments applied in performing the annual impairment test.</p>
	<p>Changes from the prior period may indicate that the risks have changed or that entity has entered into new types of transactions with a different risk profile.</p> <p>The more significant the change, the greater the likelihood that a material misstatement could occur.</p>

	<p>For example, an entity may change its mix of investment securities from government treasury securities to private hedge funds - i.e. from Level 1 investments to Level 3 investments.</p> <p>This change involves a new and potentially more complex valuation model. It may increase the likelihood of a material misstatement related to the valuation and presentation assertions.</p>
Uncertainty	<p>Uncertainty arises when the required information cannot be prepared based only on sufficiently precise and comprehensive data that is verifiable through direct observation (e.g. pending litigation).</p> <p>In these circumstances, an approach may need to be taken that applies the available knowledge to prepare the information using sufficiently precise and comprehensive observable data, to the extent available, and reasonable assumptions supported by the most appropriate available data, when it is not. Constraints on the availability of knowledge or data, which are not within the control of management (subject to cost constraints where applicable) are sources of uncertainty and their effect on the preparation of the necessary information cannot be eliminated.</p> <p>For example, estimation uncertainty arises when the required monetary amount cannot be determined with precision and the outcome of the estimate is not known before the date the financial statements are finalized.</p>
Susceptibility to misstatement due to management bias or other fraud risk factors insofar as they affect inherent risk (including significant unusual transactions)	<p>Results from conditions that create susceptibility to intentional or unintentional failure by management to maintain neutrality in preparing the information.</p> <p>For example:</p> <p>Opportunities for management and employees to engage in fraudulent financial reporting, including omission, or obscuring, of significant information in disclosures.</p> <p>Significant amount of non-routine or non-systematic transactions including intercompany transactions and large revenue transactions at period end.</p>

Transactions that are recorded based on management's intent, for example, debt refinancing, assets to be sold and classification of marketable securities.

Management bias is often associated with certain conditions that have the potential to give rise to management not maintaining neutrality in exercising judgment (indicators of potential management bias), which could lead to a material misstatement of the information that would be fraudulent if intentional.

See activity '[Identify fraud risk factors](#)' for additional considerations when considering other fraud risk factors.

We perform risk assessment procedures to obtain an understanding of how these inherent risk factors affect susceptibility of assertions to misstatement and the degree to which they do so, in the preparation of the financial statements in accordance with the applicable financial reporting framework.

It is not expected that an inherent risk factor is selected in the applicable workflow just because it is "relevant", if it does not impact where the risk sits on the inherent risk continuum. For example, where the RM is associated with the transaction (e.g. PPE additions) we would select volume of activity and homogeneity of the transaction, rather than the size and composition of the account as volume of activity and homogeneity factors impact where the risk sits on the inherent risk continuum.

[Will all inherent risk factors be relevant?](#) [ISA | 565.11100]

No. Depending on the specific risk we are assessing, some inherent risk factors may not be relevant or are not impactful to our assessment.

For example, when there are no related party transactions that are associated with a particular risk, that factor is not relevant or important in our assessment.

We focus on the factors that are most relevant to our assessment of whether the risk rises to an RMM and the related level of inherent risk. We also think about the relative significance of each inherent risk factor during our evaluation.

[Does the number of relevant factors impact the level of inherent risk?](#) [ISA | 565.11102]

No. There is not a specific number of factors that are present before something moves from one inherent risk level to another (e.g. base to elevated), because the factors are considered on a continuum and not in a binary manner.

It is often helpful to take a step back and compare the risks aggregated at an account level against other risks from other accounts.

For example, suppose that:

- We have assessed the risks associated with several smaller and less complex accounts, e.g., prepaid expenses, as Base.

- We are trying to determine whether a risk associated with a higher-volume, more complex account is Base or Elevated.

It may be helpful to think about whether the lowest level of inherent risk, (i.e., Base), makes sense for both types of risks.

Furthermore, for a risk to be assessed as higher on the continuum of inherent risk, it does not mean that both the magnitude and likelihood are assessed as high. Rather, it is the intersection of the magnitude and likelihood of the material misstatement on the continuum of inherent risk that will determine whether the assessed inherent risk is higher or lower on the continuum of inherent risk. A higher inherent risk assessment may also arise from different combinations of likelihood and magnitude, for example a higher inherent risk assessment could result from a lower but still reasonable likelihood but a very high magnitude.

[What if the risk is on the threshold between two levels of inherent risk?](#) [ISA | 565.11103]

If, we assess a risk as being on the threshold between two levels of inherent risk — e.g. Base/Elevated or Elevated/Significant — it may be appropriate to 'round up', or pick the higher risk level, documenting our rationale for the decision as part of our assessment of likelihood and magnitude.

Remember: assessing a risk as too low may result in an insufficient audit response and an unacceptable increase in audit risk.

[What if an RMM includes multiple portions of an account balance with varying levels of inherent risk?](#) [ISA | 565.11104]

If this is the case, we may have defined the RMM too broadly. In this situation, it may be appropriate to disaggregate the RMM into separate components that have varying levels of inherent risk and associate a disaggregated RM/RMM to each component. This may mean we create a duplicate RM/RMM. Adding an additional risk description can clarify how the disaggregated RMMs apply to each component.

We then perform our assessment of likelihood and magnitude of potential misstatements for each of the disaggregated RMs we identified. In performing this assessment, we may determine that one or more of the RMs does not rise to the level of an RMM. This concept applies for both accounts and disclosures.

For example, we identify the following RMM: An inappropriate amount is estimated for the net realizable value (NRV) of inventory, or an inaccurate amount is recorded for the lower of cost and NRV.

Raw materials inventory comprises multiple types of raw materials that are subject to different levels of inherent risk - including steel.

If steel prices are volatile, that may increase the risk of steel-based inventory being overvalued.

We assess inherent risk differently for the steel-based raw materials than for the remaining raw materials inventory.

As a result, we break down the risk into two separate risks - one relating to the steel-based raw materials, and the other relating to the remaining raw materials.

This disaggregation leads us to identify and assess one RMM as Significant (the risk relating to steel-based raw materials) and another as Elevated (the risk relating to the remaining raw materials) based on the relevant inherent risk factors.

As another example, we may disaggregate an RM related to the existence of cash and cash equivalent balances between different cash and cash equivalents accounts because management may use them in varying ways in different locations for different purposes (e.g. payroll, accounts payable and expense disbursement, treasury function for interest and dividend receipts, or revenue receipts) and therefore the related inherent risks may vary based on account/location/component because of differing risk profiles.

[What do we do if we have identified the same RMM due to error and due to fraud?](#) [ISA | 565.8702]

If we have identified the same RMM due to error and due to fraud, then we create 2 separate RMMs within the KPMG Clara workflow, and assess them separately. A fraud risk is always a significant risk, but a risk due to error may have a different inherent risk assessment.

We perform procedures to respond to the fraud risk and demonstrate our special audit consideration in response to the related significant risk. These procedures/responses may differ to our response to the RMM due to error (particularly if our CAR assessment is different). By identifying and assessing these RMMs separately, we can appropriately tailor our response to obtain sufficient appropriate audit evidence for both.

[How do we consider whether there is an RMM in aggregate?](#) [ISA | 565.2100]

We assess for each business process and across all business processes if there are any indications that there is an RMM in aggregate within those assertions, transactions, account balances and disclosures that do not have any RMM associated with them. Signs that might indicate that there are reasonable possibilities of RMM in the aggregate include the following:

- identifying multiple risks that relate to the same accounts/disclosures and assertions;
- determining that the combined magnitude of potential misstatements related to the remaining risks is material; or
- identifying multiple risks with similar characteristics, which may indicate several potential misstatements that could aggregate to a material misstatement.

We assess risks in the aggregate in a manner similar to our risk assessment over each risk on an individual basis. That is, when performing this aggregation assessment, we consider the same inherent risk factors (see question '[What factors do we consider in assessing likelihood and magnitude and level of inherent risk?](#)').

When assessing risks in the aggregate across all business processes, we step back and focus on those accounts and disclosures that were not identified as significant and the assertions were not identified as relevant (see question '[How do we identify significant accounts and disclosures and their relevant assertions?](#)').

[What do we do when we have determined that RMs identified represent an RMM when assessed in the aggregate?](#) [ISA | 565.11107]

When we have identified that RMs aggregate to one or more RMMs, we

- change the assessment of RMs to RMMs until the remaining RMs do not aggregate to an RMM, or
- add a custom RMM that identifies the aggregate risk.

[Is there anything we additionally consider when accounting estimates are involved?](#) [ISA | 565.11116]

Yes. We perform the risk assessment procedures related to accounting estimates in the KAEG chapter on estimates (ISA 540, AU-C 540 or AS 2501). We perform certain risk assessment procedures in order to identify and assess RMMs related to accounting estimates, as outlined in '[Perform risk assessment procedures related to accounting estimates](#)'.

[Is there anything additional we consider when the financial reporting process is involved?](#) [ISA | 565.6463]

Yes. 'Risk considerations' are used when available, within the financial reporting process screens in KPMG Clara workflow - i.e. financial statements, cash flows, segment information, disclosures - and may assist us in:

- identifying the risks of misstatement (RMs);
- determining whether the RMs are risks of material misstatement (RMMs); and/or
- designing appropriate audit responses for those assessed as RMMs.

[How do the 'risk considerations' assist us in determining whether the RMs are RMMs?](#) [ISA | 565.6469]

The 'risk considerations' let us see more clearly the individual items that contribute to the corresponding RMs within the financial reporting process, individually or in combination.

As a result, we can appropriately assess the inherent risk for the RMs, by assessing the likelihood and magnitude of potential misstatements and other relevant factors.

We assess inherent risk at the RM level, not at the risk consideration level.

[How do the 'risk considerations' assist us in designing appropriate audit responses?](#) [ISA | 565.6470]

For each RM we assess as an RMM, we design appropriate audit responses taking into account the more detailed information provided by the 'risk considerations'.

Our response is at the RMM level, not the risk consideration level.

[What do we do with financial statement-level RMs?](#) [ISA | 565.6468]

As with other risks, we assess financial statement-level RMs and determine whether there is a possibility of a material misstatement to the financial statements by considering the likelihood and magnitude of potential misstatements.

When determining whether a financial statement-level RM is an RMM, we also consider whether it affects the assessment of RMMs at the assertion level.

If the financial statement-level RM is an RMM, it affects how we conduct our audit broadly and we design and implement overall responses. See activity '[Design and implement overall responses](#)' for information about overall responses.

[What key success factors might help us in our inherent risk assessment?](#) [ISA | 565.11119]

The table below sets out examples of key success factors that can help us when assessing inherent risk.

Key success factor	How it may help
Timely partner and manager involvement	<p>An effective inherent risk assessment relies on the judgments of the engagement team's most senior members at a sufficiently detailed level early in the audit - especially for risks on the thresholds between Base and Elevated, and Elevated and Significant.</p>
Not being anchored in prior-period inherent risk assessments	<p>We use the information obtained through our risk assessment process to form up-to-date inherent risk assessments based on the current period's factors.</p> <p>Prior-period knowledge is helpful, but we combine it with everything we learn during planning and risk assessment in the current period.</p>
Thinking about inherent risk as a continuum	<p>The inherent risk continuum includes varying levels of risk.</p> <p>Thinking about where each RMM falls on that continuum can help us identify whether an account/disclosure contains components, or groups of transactions, with varying degrees of risk that are subject to different processes and controls.</p> <p>This can help us better identify significant accounts or disclosures.</p>
Paying attention to what's documented in our audit file	<p>Fully capturing how we considered the factors in our inherent risk assessment has several benefits:</p> <p>Our inherent risk assessments involve judgment, and so may warrant more persuasive audit evidence and robust documentation.</p> <p>Documenting the basis for our conclusions demonstrates how we applied professional skepticism.</p> <p>The process of documenting our rationale may lead us to rethink our initial conclusion</p>

	and revisit that assessment when it is not appropriate.
Leveraging management's risk assessment process	Reconciling our inherent risk assessments with management's risk assessments can help us evaluate the effectiveness of management's internal control over financial reporting — i.e. the Risk Assessment component.
Holding risk assessment meetings at the right times	We may hold meetings to discuss risk assessment throughout the audit - not just during planning and before issuing the audit opinion. The best ideas may come when we ask people to invest time thinking about risk assessment before these meetings. Risk Assessment and Planning Discussion (RAPD) meetings provide excellent opportunities to discuss risks holistically - but to be most effective, we plan and conduct these at the right times.
Completion of an Accounting Disclosure Checklist (ADC)	Completion of relevant sections of an ADC during risk assessment in connection with each business process assists in understanding disclosures to be expected for the process. The prior period financial statements and related disclosures, and previously completed ADC combined with current year activity, changes within existing business processes and events and circumstances that may require disclosures, all while being mindful to take a 'fresh lens' approach, assists in assessing inherent risk.

Examples

How do we consider the inherent risk factors when assessing RMs around disclosures? [ISA | 565.159465]

Below are examples of how an engagement team considers the inherent risk factors when assessing RMs around disclosures.

Fact Pattern:

RM	Initial risk assessment to identify and assess RMs
<p>Disclosures of significant accounting policies that are an integral part of the financial statements are incomplete, inaccurate or not fairly presented</p> <p>Additional risk description - goodwill and intangible asset accounting policies</p>	<p>Significant accounting policies related to recognition of goodwill and intangible assets for an acquisition are complex and involve judgment. The entity has not been involved in a significant business combination in several years, and the acquisition is material to the financial statements and intended users.</p> <p>Based on these factors, the engagement team has assessed the risk of the accounting policy disclosures is an RMM.</p>
<p>The disclosures is incomplete, inaccurate, or not fairly presented.</p> <p>Additional risk description - revenue note disclosures.</p>	<p>The entity's revenue streams have significant variable consideration that is difficult to identify and measure.</p> <p>Revenue is significant to the users of the intended users and the recognition policy is complex.</p> <p>Based on these factors, the engagement team has assessed the risk of the revenue note disclosures is an RMM.</p>

[What are additional examples of how we determine the inherent risk level?](#) [ISA | 565.11149]

See some examples below on how we determine the inherent risk levels.

Expected credit losses (ECL) allowance

The engagement team identified the following RMM: An inappropriate amount is estimated and recorded for the expected credit losses (ECL) allowance for financial assets or contracts.

Fact Pattern:

The ECL has several factors that are high on the inherent risk continuum:

- The most complex estimate for the entity (factors *complexity* and *subjectivity* are very high on the risk continuum, and possibly *exposure to losses*, *significant accounting*, or *economic factors*, *susceptibility of error*, etc.)
- The most heavily scrutinized by regulators and investors (factors *nature of the account*, *exposure to losses*).

Analysis:

Based on these factors alone, the engagement team assesses the inherent risk as Significant for related RMMs.

Deposits

The engagement team identified the following RMM: Deposits are recorded inappropriately when:

- they are not accurately recorded
- they do not meet the recognition requirements or
- they do not exist.

Fact Pattern:

The only factor that is higher on the risk continuum is volume/amount. All other factors are quite low on the risk continuum (low complexity even on a relative basis to other processes, no judgment, no exposure to losses, no SUTs or related parties, etc.).

Analysis:

Based on this fact pattern, the engagement team assesses the inherent risk of RMMs associated with deposits as Base.

Product Returns

The engagement team identified an RMM related to the rights of return estimate, including the related disclosures.

Fact Pattern:

While volume/amount are lower on the risk continuum, exposure to losses and changes from the prior period are higher on the risk continuum (given certain changes in the entity's revenue contracts and uncertainty in the economic environment).

Analysis:

Based on this fact pattern, the engagement team assesses the inherent risk for both the account and related disclosures as Elevated.

1.5 Identify significant accounts and disclosures and their relevant assertions [ISA | 566]

What do we do?

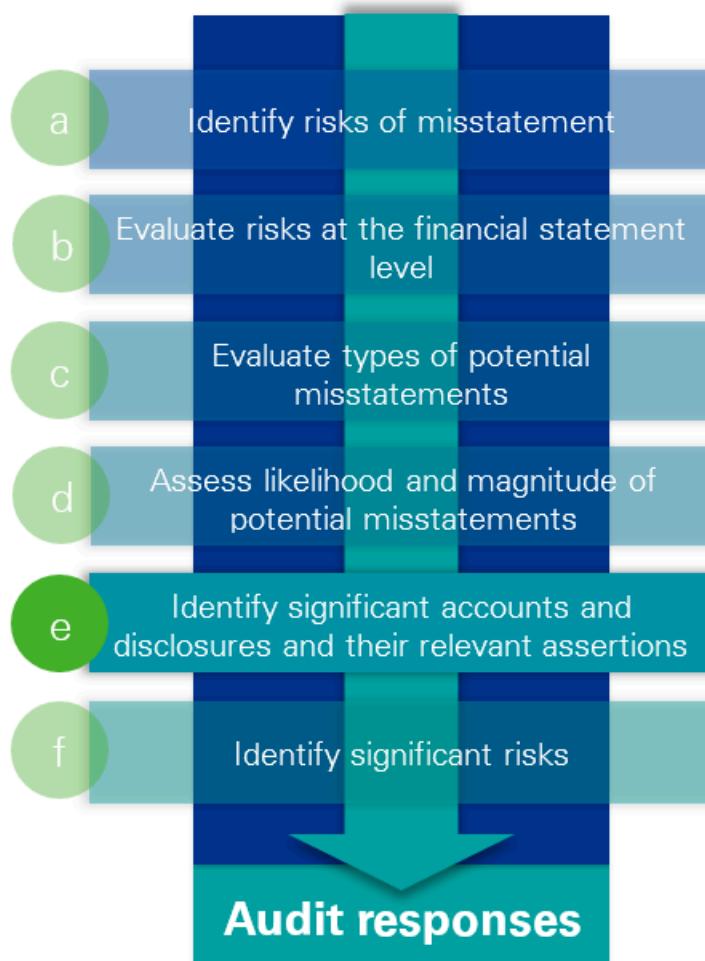
Identify significant accounts and disclosures and their relevant assertions

Why do we do this?

Determining relevant assertions and significant accounts and disclosures helps us identify the specific elements of the financial statements to focus on in our audit and design procedures in response to the identified risks of material misstatements (RMMs).

Execute the Audit

Where are we in our risk assessment? [ISA | 566.1300]



What is a significant account or disclosure, and what is a relevant assertion? [ISA | 566.1400]

Significant accounts and disclosures and their relevant assertions are those with a reasonable possibility of containing a material misstatement. In other words, they relate to an RMM.

Relevant assertion	Each assertion that has one or more RMM
Significant account or significant disclosure	Each account or disclosure that has one or more relevant assertion (and therefore one or more RMM)

Following that logic, if we *don't* identify an assertion as relevant, or an account or disclosure as significant, then we've concluded that there is a remote chance of a material misstatement arising, both individually and when aggregated with others.

In other words, it doesn't relate to an RMM — so we may perform *no* specific audit procedures over that assertion, financial statement line item or disclosure.*

* There are certain areas within the financial reporting process where procedures are always performed even if there is no RMM (e.g. disclosures: agree/reconcile information in the disclosure to the underlying accounting records).

How do we identify significant accounts and disclosures and their relevant assertions? [ISA | 566.8693]

We have already associated each RMM with the specific accounts, disclosures and assertions it affects. This means we've essentially identified our initial population of significant accounts, disclosures and relevant assertions.

After identifying our initial population, we perform three additional activities that help validate the population of significant accounts, disclosures and relevant assertions.

1	Evaluate inherent risk factors	<p>Evaluate the inherent risk factors (see question 'What factors do we consider in assessing likelihood and magnitude and level of inherent risk?') related to each financial statement line item and disclosure and their assertions.</p> <p>This helps us consider whether we missed any significant accounts, disclosures and relevant assertions through our initial analysis.</p>
2	Step back and assess accounts and disclosures we did not identify as significant, and assertions we did not identify as relevant	<p>Consider the accounts and disclosures we did not identify as significant and the assertions we did not identify as relevant.</p> <p>Step back and assess whether those accounts, disclosures and assertions — both individually and in the aggregate — have a reasonable possibility of containing a material misstatement.</p> <p>This aggregate assessment includes considering possible similarities in the accounts and disclosures. This acts as an additional check on our population of significant accounts, disclosures and relevant assertions.</p> <p>We perform the individual assessment on an assertion-by-assertion basis for each account and disclosure. This aggregate assessment includes thinking about:</p> <ul style="list-style-type: none"> • similarities that may exist in these accounts, disclosures and assertions; and • other factors that may increase the chances of multiple misstatements aggregating to a material misstatement. <div style="background-color: #D3D3D3; padding: 10px; margin-top: 10px;"> <p>For example, we may look at the total impact these accounts have on:</p> <ul style="list-style-type: none"> • total current assets/liabilities; </div>

		<ul style="list-style-type: none"> • total assets/liabilities; • total revenue/expenses; or • net income.
		<p>When we evaluate these accounts, disclosures and assertions in the aggregate, we think about the same inherent risk factors we evaluated in step 1.</p>
3	Step back and evaluate whether for material classes of transactions, account balances or disclosures, that have not been determined to be significant classes of transactions, account balances or disclosures, this remains appropriate	<p>As a final step, we consider those material accounts that we did not identify as significant accounts and evaluate whether this remains appropriate.</p> <p>This helps us to challenge and properly analyse our initial conclusions before we plan and perform audit procedures.</p>

Do we perform substantive procedures for material accounts and disclosures we have not identified as significant? [\[ISA | 566.8879\]](#)

Yes. See activity '[Design and perform substantive procedures for accounts and disclosures with no RMMs](#)'.

What accounts are considered 'material accounts'? [\[ISA | 566.11297\]](#)

Material accounts are accounts that are equal to or greater than materiality.

What if we identify an RMM after our initial assessment? [\[ISA | 566.11216\]](#)

If we determine there is a reasonable possibility of a material misstatement arising in:

- the accounts and disclosures we did not initially identify as significant; or
- the assertions we did not initially identify as relevant,

then we revisit our risk assessment decisions and identify additional RMMs. This may indicate that we didn't obtain a sufficient understanding of the entity's processes during risk assessment and may prompts us to reassess our understanding of the entity, including the flow of information for transactions, events and conditions.

When we identify additional significant accounts and relevant assertions, we also think about why we selected those accounts as opposed to the other accounts. We then identify the RMMs that led us to this conclusion.

Group Audit | How do we identify the significant accounts and disclosures and their relevant assertions in a group audit? [\[ISA | 566.1510\]](#)

As the lead group auditor, we take responsibility for the identification of all significant accounts and disclosures and their relevant assertions based on the group financial statements.

It is an iterative process. Since most assertion-level RMMs of the group financial statements will arise in components, we in practice, as the lead group auditor, may perform the following:

- (1) perform initial risk assessment procedures at the group level and evaluate qualitative and quantitative risk factors to identify those accounts, disclosures and assertions that have indicators that they are likely significant accounts or disclosures and relevant assertions
- (2) identify components for which more granular risk assessment procedures will be performed based upon the likely significant accounts and disclosures and their relevant assertions
- (3) use our knowledge from the risk assessment procedures we perform at the group level or component level
- (4) communicate with component auditors (i.e. RAPD or other two way communication) regarding their knowledge from the risk assessment procedures that they perform at the component level, including their identification of significant accounts and disclosures and their relevant assertions.

[Group Audit | What does 'take responsibility for' mean?](#) [ISA | 566.160253]

'Take responsibility for' means the lead group auditor may either design and/or perform procedures, tasks, or actions themselves or are permitted to assign the design and/or performance of procedures, tasks or actions to other appropriately skilled or suitably experienced members of the engagement team, including component auditors.

Assigning the design and/or performance of procedures to another member of the engagement team, however, does not relieve the lead group auditor of their responsibility for the overall design and performance of the audit

[At what level do we identify accounts and disclosures?](#) [ISA | 566.1600]

Our goal is to find the highest level of accounts and disclosures where similar risks exist. Therefore, we may start by capturing each financial statement line item. If the financial statement line item contains general ledger accounts or groups of general ledger accounts with different inherent risks of error, inherent risk of fraud, control risks, or controls in place, we may disaggregate them further to the level of general ledger accounts or a group of such accounts.

For example, within trade receivables there may be general ledger accounts for domestic and foreign receivables with different inherent risks that warrant disaggregating into separate accounts.

We may also disaggregate a general ledger account if that is appropriate for our purposes.

For example, the audited entity records all provisions in one general ledger account but for the purpose of our audit we disaggregate this general ledger account into separate provisions because each provision is subject to sufficiently different inherent risks of error, risks of fraud, control risks, or controls in place.

Similarly, for disclosures we may start by capturing each distinct note in the financial statements. Then we may look at the underlying source of the disclosed information to determine if each disclosure is supported by general ledger accounts, subledger accounts, documents prepared by the entity, or

external documents (e.g. laws and regulations, group accounting instructions) or a combination of different sources. We may consider whether these sources have different inherent risk characteristics that warrant disaggregating a disclosure. We may consider how the accounts related to the disclosure have been disaggregated in the business process(es). Additionally, it may be helpful to associate the significant accounting policies (often from Note 1 in financial statements) with each distinct disclosure in the financial statements.

For example, the property and equipment significant accounting policies in Note 1 and the property disclosures in Note 5 have similar inherent risks and relate to the PP&E business process. We may aggregate these into a distinct disclosure in the PP&E business process.

[What if a certain financial statement line item or disclosure contains different types of transactions?](#) [ISA | 566.1700]

Some of an entity's financial statement line items or disclosures will contain several different types of transactions. This is often the case for accounts that contain several different components — e.g. miscellaneous, other and general accounts.

In order to consider all possible risks affecting the account, we understand the different types of transactions included in the accounts and the types of misstatements that could arise. This can help us disaggregate the account risks and properly identify all the RMs and RMMs related to those different types of transactions.

Our audit response addresses each RMM we identify, so we design procedures that consider these different types of potential misstatements.

[Do we perform substantive audit procedures for accounts or disclosures that don't have an RMM?](#) [ISA | 566.8695]

Yes. We perform substantive audit procedures for accounts or disclosures that don't have an RMM, but those instances are limited to:

- when we perform procedures related to material non-significant accounts (MNSAs) (see activity '[Design and perform substantive procedures for accounts and disclosures with no RMMs](#)' for additional information);
- when we perform procedures specifically to incorporate an element of unpredictability in our audits (see activity '[Incorporate elements of unpredictability](#)' for additional information);
- when we perform additional substantive procedures in response to possible undetected misstatements that could make the financial statements materially misstated (see activity '[Consider the possibility of undetected misstatements and its implications](#)' for additional information);
- certain areas within the financial reporting process where procedures are always performed even if there is no RMM (e.g. disclosures: agree/reconcile information in the disclosure to the underlying accounting records).

[What are financial statement assertions?](#) [ISA | 566.11274]

Financial statement assertions are representations by management, explicit or otherwise, that are embodied in the financial statements, as used by us to consider the different types of potential misstatements that may occur.

In representing that the financial statements are in accordance with the applicable financial reporting framework, management implicitly or explicitly makes assertions regarding recognition, measurement and presentation of classes of transactions and events, account balances and disclosures.

For example, when management provides us with a draft of the financial statements, they are implicitly asserting that accounts payable is complete. We relate these assertions associated with significant accounts to the potential types of RMs when identifying RMMs and ultimately designing our planned audit procedures to gather audit evidence that is responsive to those RMMs.

[What financial statement assertions do we use?](#) [ISA | 566.11276]

The following table describes the relevant assertions for classes of transactions, account balances and their related disclosures, which is derived from the standards:

KPMG Assertion	Income Statement Classes of Transactions	Balance Sheet Account balances
C Completeness	All transactions and events have been recorded. These transactions and events have been recorded in the correct accounting period (i.e. no understatement due to cut-off).	All assets, liabilities and equity interests have been recorded.
E Existence (account balances) and Occurrence (class of transaction)	Transactions and events that have been recorded have occurred. These transactions and events have been recorded in the correct accounting period (i.e. no overstatement due to cut-off).	Assets, liabilities and equity interests exist.
A Accuracy	Amounts and other data relating to recorded transactions and events have been recorded correctly.	Amounts and other data relating to recorded assets, liabilities and equity interests

		have been recorded correctly.
V Valuation	Transactions and events have been recorded at appropriate amounts (i.e. are appropriately valued).	Assets, liabilities and equity interests have been recorded at appropriate amounts and any resulting valuation or allocation adjustments are appropriately recorded
O Obligations and Rights	The entity has the rights and obligations to transactions and events that it has recorded (i.e. transactions and events pertain to the entity).	The entity holds or controls the rights to assets. Liabilities and equity interests are the obligations of the entity.
P Presentation	<p>Financial information is appropriately presented and disclosed in the financial statements.</p> <p>Classes of transactions and events or assets, liabilities and equity interests:</p> <ul style="list-style-type: none"> • have been recorded in the proper accounts and are classified to the appropriate financial statement line item; • are appropriately aggregated or disaggregated and clearly described; • have occurred and/or are relevant to the accounting period; and • pertain to the entity. <p>Disclosures related to classes of transactions and events or assets, liabilities and equity interests:</p> <ul style="list-style-type: none"> • are relevant and understandable in the context of the requirements of the applicable financial reporting framework; • are complete (i.e. all disclosures related to classes of transaction, account balances and other matters have been included in the financial statements); and • are disclosed at appropriate amounts (i.e. are appropriately measured and described). 	

Other matters disclosed in the financial statements are disclosures not directly related to recorded classes of transaction or account balances.

For example, the entity may describe its exposure to risks arising from financial instruments, including:

- how the risks arise;
- the objectives, policies and processes for managing the risks; and
- the methods used to measure the risks.

Examples

How do we consider accounts, disclosures and assertions not identified as significant in the aggregate?

[ISA | 566.11279]

Fact pattern:

Entity X records operating expenses in multiple accounts.

Account	Balance (\$)
Payroll expense	37,000
Depreciation expense	29,000
Rent expense	8,500
Advertising expense	7,600
Utilities expense	750
Amortization expense	250
Total operating expenses	\$83,100

First, the engagement team identify RMMs related to payroll expense and depreciation expense, making these significant accounts. The relevant assertions for those identified RMMs are Completeness, Existence and Accuracy.

Analysis:

Stepping back, the team analyze the remaining accounts, disclosures and assertions that they did not identify as significant or relevant.

Their initial decision to identify no RMMs over the completeness of each remaining expense account remains appropriate. But they reach a different conclusion when they step back and consider these accounts in combination — i.e. that an RMM exists in the aggregate relating to the Completeness of these expense accounts.

In this case, they identify that the performance of procedures over the Completeness assertion of the other expense accounts are necessary. They identify RMMs relating to the Completeness of rent expenses (\$8,500) and advertising expenses (\$7,600). They then step back and conclude that there is no longer a reasonable possibility of material misstatement in the remaining expense accounts.

If the team hadn't been able to identify specific accounts for which Completeness was relevant, they might instead have identified Completeness as a relevant assertion for *all* the remaining expense accounts, and included them as significant accounts.

1.5.1 Identify accounting estimates in significant accounts and disclosures [ISA | 7706]

What do we do?

Identify accounting estimates in significant accounts and disclosures with a reasonable possibility of containing a risk of material misstatement

Why do we do this?

Once we understand the entity and its environment, within each account and disclosure we identify accounting estimates with a reasonable possibility of containing a risk of material misstatement.

Execute the Audit

How do we identify estimates in significant accounts and disclosures? [ISA | 7706.15271]

We identify estimates in significant accounts and disclosures as we perform our risk assessment procedures. See activity '[Perform risk assessment procedures related to accounting estimates](#)'.

How do we identify significant accounts and disclosures? [ISA | 7706.15272]

We perform the activity '[Identify significant accounts and disclosures and their relevant assertions](#)'. However, we consider additional risk factors when identifying significant accounts and disclosures involving accounting estimates.

Do we identify all estimates that may exist in a business process? [ISA | 7706.8801]

No. Within each business process, we only identify the accounting estimates with a reasonable possibility of containing a risk of material misstatement. For example, the estimate may be clearly inconsequential to the financial statements such that it is clear to us that there is not a risk of material misstatement associated with it.

In some cases, our general risk assessment procedures, previous client or audit experience and other walkthroughs within the business process, may be sufficient for us to initially conclude about whether there is an RMM related to an estimate. For example, an estimate may be complex and material enough that it is clear to us that there is a risk of material misstatement associated with it. In other situations, we may not have enough information to reach an initial conclusion and may obtain an understanding of the process to develop an estimate, as well as think about the risks related to each of the elements of the estimate - i.e., the selection and application of methods, assumptions, and data - to help us identify and assess the RMMs related to an accounting estimate.

What are the additional risk factors that we evaluate when identifying significant accounts and disclosures involving accounting estimates? [ISA | 7706.15273]

We evaluate additional risk factors when identifying significant accounts and disclosures involving accounting estimates with a reasonable possibility of containing a risk of material misstatement, which include:

- the degree of uncertainty associated with the future occurrence or outcome of events and conditions underlying the relevant assumptions;
- the complexity of the process for developing the accounting estimate;
- the number and complexity of methods and relevant assumptions associated with the process;
- the degree of subjectivity associated with the methods, relevant assumptions, and data;
- if forecasts are important to the estimate, the length of the forecast period and degree of uncertainty regarding trends affecting the forecast; and
- the degree of subjectivity associated with the selection of management's point estimate and related disclosures for inclusion in the financial statements.

These are the same risk factors we evaluate to assess which RMs related to an accounting estimate are RMMs. See activity '[Identify and assess which RMs related to an accounting estimate are RMMs](#)' for further information.

2 Determine significant risks [ISA | 573]

What do we do?

Determine whether any of the identified and assessed risks of material misstatement are significant risks

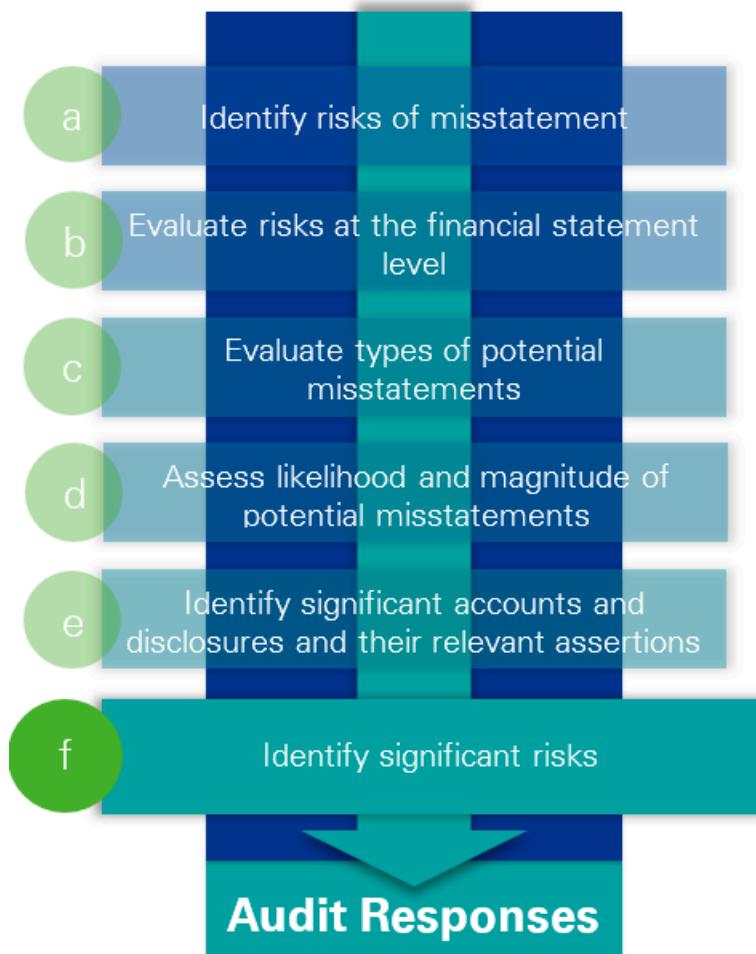
Why do we do this?

The determination of significant risks allows for the auditor to focus more attention on those risks that are on the upper end of the continuum of inherent risk. If we fail to assess the inherent risk as Significant, we could perform the wrong audit procedures to address the risk.



Execute the Audit

[Where are we in our risk assessment? \[ISA | 573.1300\]](#)



What is a significant risk? [ISA | 573.1400]

A significant risk is a risk of material misstatement (RMM) which is:

- close to the upper end of the continuum of inherent risk due to the degree to which inherent risk factors affect the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement should that misstatement occur; or
- fraud risks; or
- significant unusual transactions with related parties.

We document special audit considerations in response to significant risks.

What does 'special audit consideration' mean? [ISA | 573.8652]

'Special audit consideration' means focusing more attention on those risks that are on the upper end of the continuum of inherent risk, through the performance of certain procedures including:

- Evaluating design and implementation of control activities that address the RMM (see '[Evaluate the design and implementation of relevant control activities](#)');
- Designing and performing substantive procedures that specifically respond to the significant risk (see '[Perform substantive procedures that respond to significant risks](#)');
- Obtaining more persuasive audit evidence as our assessment of inherent risk increases (see '[Design and perform substantive procedures whose nature is responsive to CAR](#)');

- Communicating with those charged with governance about the significant risks we identified (see '[Communicate planned scope and timing of the audit](#)')
- Taking into account significant risks when determining those matters that required significant auditor attention, which are matters that may be key audit matters (see '[Determine if there are any KAMs in the current audit period](#)')
- Required review of audit documentation related to significant risks and our audit response thereto by the engagement partner (see '[Perform minimum required review](#)')
- For group audits, increased involvement by the group engagement partner if the significant risk relates to a component in a group audit and for the group engagement team to direct the necessary work at the component by the component auditor (see '[Group Audit | Be involved in the component auditor's risk assessment when they perform an audit of a significant component](#)' and '[Group Audit | Evaluate the appropriateness of, and determine whether to be involved in, the component auditor's planned audit procedures over group significant risks](#)').
- In addition, where we plan to rely on the operating effectiveness of control activities that address significant risks, we cannot rely on prior period testing of such controls.

We think carefully about how we identify and describe significant risks and include the 'what, where, why and how' associated with each significant risk.

Being specific helps us to better tailor our responses to these risks and apply 'special audit consideration'. With this in mind, it may be useful to take a second look at the population of significant risks, and carefully think about whether we've identified them with enough specificity.

[How do we determine whether any of the identified and assessed RMMs are significant risks?](#) [ISA |

573.11802]

In addition to considering those risks that are closer to the upper end of the continuum of inherent risk noted in question '[What are the inherent risk factors?](#)' the following table shows the factors we consider to determine whether any identified and assessed RMMs are significant risks:

Factors	Example of being lower on the inherent risk continuum	Example of being higher on the inherent risk continuum
Whether the risk is a fraud risk	A risk that is not a fraud risk.	An identified fraud risk. Remember: a fraud risk is a significant risk.
Whether the risk relates to recent significant economic, accounting or other developments	Risks related to the valuation of certain assets, when: <ul style="list-style-type: none"> • a commodity price is a primary input in the valuation model; and • the commodity's prices have been relatively 	Risks related to the valuation of certain assets, when: <ul style="list-style-type: none"> • a commodity price is a primary input in the valuation model; and • there has been significant volatility in

	<p>stable in the current period.</p>	<p>the commodity's prices in the current period.</p> <p>Changes in the entity's business that involve changes in accounting, for example, mergers and acquisitions.</p>
The complexity of transactions	<p>Risks associated with the issuance of new debt when the debt instrument is simple and does not have unique or complex features.</p>	<p>Risks associated with the issuance of new debt when the debt instrument has multiple conversion features and embedded derivatives.</p> <p>Complexity in data collection and processing to support account balances.</p> <p>Accounting policies or principles that may be subject to differing interpretation.</p> <p>Accounting for unusual or complex transactions, including those in controversial or emerging areas (for example, accounting for revenue with multiple performance obligations that are difficult to value).</p>
Whether the risk involves significant transactions with related parties	<p>Risks associated with accounting for and disclosing a transaction between an entity and an unrelated third party for the purchase of land to be used to build a new corporate headquarters.</p>	<p>Risks associated with accounting for and disclosing a transaction between an entity and a board member, to buy land to build a new corporate headquarters.</p> <p>Remember: significant unusual transactions with related parties are assessed as a significant risk. (see activity 'Identify and assess RMMs, including significant risks, associated with</p>

		related parties' for additional considerations)
The degree of complexity or judgment in recognizing or measuring financial information related to the risk	Risks related to the valuation of investment securities that are exchange-traded, and for which published prices are available in active markets — i.e. Level 1.	Risks related to the valuation of investment securities that are valued using multiple unobservable inputs — i.e. Level 3. Accounting policies or principles that may be subject to differing interpretation. Transactions for which there are multiple acceptable accounting treatments such that subjectivity is involved.
Whether the risk involves significant unusual transactions	Risks related to a transaction that is routine and in the normal course of business — e.g. processing monthly payroll transactions.	Risks related to a transaction that is (or could be) many times greater than materiality and outside of the normal course of business — e.g. a large, speculative investment in a business unrelated to the entity's core operations. Not <i>all</i> risks related to significant unusual transactions will be significant risks, however, these risks may be higher on the inherent risk continuum because they may involve one or more of the following: <ul style="list-style-type: none"> • greater management intervention to specify the accounting treatment • greater manual intervention for data collection and processing • more complex calculations or

		<ul style="list-style-type: none"> accounting policies or principles • non-routine transactions, whose nature may make it difficult for the entity to implement effective processes to account for the transactions <p>Remember: significant unusual transactions with related parties are assessed as a significant risk. (see activity 'Identify and assess RMMs, including significant risks, associated with related parties' for additional considerations)</p>
--	--	--

We consider these factors as a whole, which means that no individual factor determines where a risk falls on the inherent risk continuum. We identify significant risks based on inherent risk, without regard to control activities.

3 Conclude on our assessment of control risk [ISA | 1283]

What do we do?

Conclude on our assessment of control risk

Why do we do this?

We make a preliminary assessment of control risk as an input to our combined assessed risk (CAR) when planning our audit.

After performing procedures over the relevant controls, we either confirm or revise — i.e. reassess — our preliminary control risk assessment.

We confirm our preliminary assessment of control risk by considering all of the evidence we gather in evaluating the design and testing the operating effectiveness of relevant controls.

Execute the Audit

How do we assess control risk? [ISA | 1283.8519]

We assess control risk based on our understanding of controls and whether we plan to test the operating effectiveness of controls.

How do we make a preliminary assessment of control risk? [ISA | 1283.8522]

Our preliminary assessment of control risk is based on whether:

- we expect to rely on controls by testing the operating effectiveness of relevant controls to reduce our substantive procedures (Controls Reliance); or
- we will not rely on controls to reduce our substantive procedures (No Controls Reliance) because the controls are missing, we do not expect them to be effective or because we will not test their operating effectiveness.

Refer to activity '[Make a preliminary CAR assessment for each RMM](#)' for additional information on the impact of our preliminary control risk assessment on CAR.

[How do we conclude on our control risk assessment?](#) [ISA | 1283.1400]

To conclude on our assessment of control risk:

- [if we identified control deficiencies, we determine whether we can or want to test different controls that address the same RMM and process risk points,](#)
- [if we identified general IT control \(GITC\) deficiencies, we determine whether to test other GITCs or perform additional procedures,](#)
- [we evaluate the evidence we obtained from all sources, including our tests of controls, misstatements detected and any identified control deficiencies, and](#)
- [we confirm control risk assessment.](#)

4 Test control activities when substantive procedures alone cannot provide sufficient audit evidence

[ISA | 597]

What do we do?

IF substantive procedures alone cannot provide sufficient appropriate audit evidence, THEN test the operating effectiveness of control activities over those assessed risks of material misstatement

Why do we do this?

We test the operating effectiveness of controls over a risk of material misstatement (RMM) when we can't design substantive procedures capable of obtaining sufficient appropriate audit evidence on their own.

Execute the Audit

[When may we be unable to obtain sufficient appropriate audit evidence from substantive procedures alone?](#) [ISA | 597.1300]

We may not be able to obtain sufficient appropriate audit evidence from substantive procedures alone when a significant amount of information or data elements are electronically initiated, recorded, processed or reported. In this case, our ability to obtain sufficient appropriate audit evidence may depend on the entity's controls.

However, it is not necessary to test controls for every process with automated control activities or evidence in electronic form, except when the sufficiency and appropriateness of the substantive audit evidence depends on the entity's controls.

What are examples of when substantive procedures alone may not provide sufficient appropriate audit evidence? [ISA | 597.1400]

The following table sets out examples of situations in which performing substantive procedures alone may not provide sufficient appropriate audit evidence.

Scenario	Examples
<p>The entity's financial reporting and accounting information systems rely heavily on IT, with little or no manual intervention. The entity also relies on embedded, automated process control activities to prevent or detect and correct misstatements that may occur during the activities to initiate, process and record financial transactions, and to create its financial statements.</p>	<ul style="list-style-type: none"> • Customer orders are placed directly on the entity's system via the web, without a customer purchase order, contract or data file. • Customer agreements are signed online and maintained electronically in the entity's systems. • Approvals or document matching are performed online by the IT system with little or no manual intervention. • The entity runs an internet-based consumer marketplace that aggregates data about consumers and bills suppliers on a per click basis. It relies heavily on IT to deliver products and bill customers. • We have identified financial statement-level RMMs or significant risks arising from the use of IT.
<p>Important information may exist solely in electronic form. The entity uses an IT system to provide summarized information from many different IT systems to business process owners or management, and management rely on database information and/or system-generated reports to generate the financial statements.</p>	<ul style="list-style-type: none"> • Each day, a retail entity's IT systems gather store sales data from multiple IT systems. Only automated process control activities exist to ensure management receives complete store sales data and aggregated sales data by region. There is no manual intervention, and there are no manual controls. Data transferred between IT systems does not include individual transactions to allow management (or us) to trace back to the source transactions. • We seek to use the history of price markdowns to audit a retail entity's markdowns reserve. We can only get this information at a sufficiently granular level through reports from the entity's enterprise resource planning or point-of-sale system. Therefore, we test controls to obtain evidence over the accuracy of markdown information and the

	completeness and accuracy of the entity's report for use in our substantive procedures.
The entity transacts electronically with third parties. Sales and purchases are automatically recorded between the entity and third parties, with little or no manual intervention.	<ul style="list-style-type: none"> An entity's customers buy software services direct from its website, with little or no manual intervention. The entity's recorded revenues are generated directly through these website sales. It receives daily sales summary reports but cannot trace individual transactions to their source. An entity conducts much of its business with vendors or customers over the web — e.g. when the entity places an order, its IT system automatically sends the order information to the vendor. The IT system then automatically matches the receipt and makes payment without manual intervention.
The entity uses a model to develop complex accounting estimates using data comprised of many small balances resulting from a high volume of transactions.	<ul style="list-style-type: none"> Data used in developing a complex expected credit loss provision for a financial institution or a utility entity.

What do we do if substantive procedures alone cannot provide sufficient appropriate audit evidence and the control activities related to the RMM are ineffective? [ISA | 597.8596]

If we assess control risk as no controls reliance for an RMM where we are unable to obtain sufficient appropriate audit evidence from substantive procedures alone, then we have a scope limitation for that RMM. We perform procedures in accordance with '[Modify the audit opinion for specific circumstances](#)'.

Example

When might substantive procedures alone not provide sufficient appropriate audit evidence? [ISA | 597.1500]

Example 1 | Manufacturing entity [ISA | 597.10976]

Fact pattern:

Entity A issues electronic purchase orders to its suppliers, and receives the related supplier invoices electronically. Entity A records the receipt of goods by scanning a supplier barcode on the received parcel. This initiates an automated process to match the purchase order price and quantity against the invoice price, quantity and barcode reference number.

The receipt is recorded in the inventory system, and the payable in the payables system. Both amounts are transferred to the general ledger. Given the automated nature of its process, Entity A does not retain hard copy receiving documents.

Analysis:

The process is highly automated and relies on evidence that only exists in electronic form — i.e. electronic invoices and purchase orders. Therefore, substantive procedures alone may not provide sufficient appropriate audit evidence.

As a result, the engagement team identify and test those automated process control activities and general IT controls that support the effective operation of these automated control activities. Otherwise, they may not obtain sufficient appropriate evidence in response to the identified risk.

[Example 2 | Bank](#) [ISA | 597.10977]

Fact pattern:

Bank J relies heavily on IT systems to process deposit transactions. These transactions are captured through various means, including branch tellers, automated clearing house (ACH) transactions, wire transfers, automated teller machines (ATMs), telephone, online banking and correspondent banks.

We have identified the following RMM:

Deposits are not recorded as liabilities at the time they are received by the entity.

As part of our substantive procedures to address this RMM, we plan to perform procedures over the daily deposit suspense/transit account reconciliations at period end.

Analysis:

The process is highly automated, and relies on evidence that only exists in electronic form — i.e. checks deposited in the bank, wire transfers, ACH transactions, ATMs, branch tellers. Therefore, substantive procedures alone may not provide sufficient appropriate audit evidence.

As a result, the engagement team identify and test those automated process control activities and general IT controls that support the effective operation of these automated control activities. Otherwise, they may not obtain sufficient appropriate evidence in response to the identified risk.

Evaluating the Audit Evidence Obtained from the Risk Assessment Procedures

International Standards on Auditing: ISA 315.35

Evaluating the Audit Evidence Obtained from the Risk Assessment Procedures

35. The auditor shall evaluate whether the audit evidence obtained from the risk assessment procedures provides an appropriate basis for the identification and assessment of the risks of material misstatement. If not, the auditor shall perform additional risk assessment procedures until audit evidence has been obtained to provide such a basis. In identifying and assessing the risks of material misstatement, the auditor shall take into account all audit evidence obtained from the risk assessment procedures, whether corroborative or contradictory to assertions made by management. (Ref: Para. A230-A232)

ISA Application and Other Explanatory Material: ISA 315.A230-A232

Evaluating the Audit Evidence Obtained from the Risk Assessment Procedures (Ref: Para 35)

Why the Auditor Evaluates the Audit Evidence from the Risk Assessment Procedures

A230. Audit evidence obtained from performing risk assessment procedures provides the basis for the identification and assessment of the risks of material misstatement. This provides the basis for the auditor's design of the nature, timing and extent of further audit procedures responsive to the assessed risks of material misstatement, at the assertion level, in accordance with ISA 330. Accordingly, the audit evidence obtained from the risk assessment procedures provides a basis for the identification and assessment of risks of material misstatement whether due to fraud or error, at the financial statement and assertion levels.

The Evaluation of the Audit Evidence

A231. Audit evidence from risk assessment procedures comprises both information that supports and corroborates management's assertions, and any information that contradicts such assertions.⁶²

⁶² ISA 500, paragraph A1

Professional Skepticism

A232. In evaluating the audit evidence from the risk assessment procedures, the auditor considers whether sufficient understanding about the entity and its environment, the applicable financial reporting framework and the entity's system of internal control has been obtained to be able to identify the risks of material misstatement, as well as whether there is any evidence that is contradictory that may indicate a risk of material misstatement.

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Continue to assess RMMs, and revise audit approach as necessary [ISA | 578]

What do we do?

Continue our assessment of the risks of material misstatement, including fraud risks, throughout the audit and revise the risk assessment and planned audit procedures in response to audit evidence that contradicts our original risk assessment.

Why do we do this?

If we fail to identify and properly assess a potential risk, it can negatively affect our audit. Similarly, if we ignore or fail to revise our risk assessment, our audit response may be insufficient or inappropriate. Therefore, we consider the information we learn throughout the audit process and determine whether

it affects our original risk assessment. Risk assessment drives our audit responses, so changes to our original risk assessment can affect our audit procedures.

Execute the Audit

What does it mean to continue our risk assessment throughout the audit? [ISA | 578.1300]

Risk assessment is an iterative process, rather than something we perform only at the beginning of the audit. During the course of the audit, we constantly obtain new information and evidence. This may support or contradict our original risk assessment and can affect our overall audit plan.

For example, information that supports our original risk assessment might support the fact that a specific risk exists, that we assessed it appropriately, and that we linked the risks of material misstatement (RMMs) to the appropriate assertions, accounts and disclosures.

As we obtain information or evidence throughout the audit, we consider whether it supports or contradicts our original risk assessment. 'Throughout the audit' means through performing our risk assessment, control and substantive procedures, all the way to when we form our audit opinion. This enables us to:

- identify evidence that contradicts our original risk assessment; and
- respond appropriately by revising our, or performing additional, risk assessment and planned audit procedures.

How do we identify whether information or evidence contradicts our original risk assessment? [ISA |

578.1400]

We obtain many different types of audit evidence and learn things about the entity throughout our audit. This evidence and information may or may not corroborate our original risk assessment. Asking ourselves:



Does this evidence or information tell me something new or different about the risks affecting the entity?

can help identify situations where evidence may contradict or be inconsistent with our original risk assessment.

For example, any of the following information or evidence identified when performing our procedures over cash and cash equivalents, individually or in any combination, may indicate a need to assess a heightened inherent risk or reassess our original risk assessment, including our fraud risk assessment:

Changes from prior period in account or disclosure characteristics:

- Lack of clarity regarding noticeable changes in account balance and activity compared to prior year;
- New authorized signers on a cash account without appropriate explanation;
- Change in contact address for external confirmation;

- Account balance transfers or account closures, especially those that occur at (or close to) year-end, that are unexplained or lack business purpose; or
- Newly created bank accounts, especially those that are created at (or close to) year-end, without appropriate explanation.

Susceptibility to misstatement due to error or fraud:

- Slow response time to confirmation request; or
- Unusual or unexpected responses to confirmation requests.

What types of information or evidence might contradict our original risk assessment? [ISA | 578.1500]

Evidence that contradicts our original risk assessment may come in many forms. A few common types include:

- control deficiencies;
- audit misstatements;
- overall changes in the entity's business — e.g. business combinations, dispositions;
- changes in the entity and its environment; and
- other information that appears to be inconsistent with what we obtained during our risk assessment procedures.

Will a control deficiency affect our inherent risk assessment? [ISA | 578.11494]

Our inherent risk assessment does not consider the effect of controls; however, identifying control deficiencies can provide information that contradicts our inherent risk assessment.

For example, we may identify a deficiency in controls over the measurement of the allowance for bad debts. That deficiency may highlight that the measurement is more complex and involves more judgment than we originally thought, causing us to revise our inherent risk assessment.

What if we are unsure whether information or evidence we have obtained contradicts our original risk assessment? [ISA | 578.1600]

When challenged to determine whether new information contradicts our original risk assessment, we think about the possible impacts carefully. Failing to revise our risk assessment can mean we fail to respond properly in our audit. Sometimes, it can help to think about what we might do differently as a result of the information, to better consider what risks may be affected and what we revised.

As a practical consideration, when there is uncertainty about whether information contradicts our original risk assessment, that uncertainty is a strong indicator that the information is contradictory — and we therefore revise our risk assessment and planned audit procedures.

What if we identify information that contradicts our original risk assessment? [ISA | 578.1700]

Information that contradicts our original risk assessment may suggest that:

- our inherent risk assessment for a specific risk may be incorrect — for example, evidence that a particular RMM we initially assessed at Base may actually be Elevated; and/or
- original risk assessment procedures do not provide an appropriate basis for the identification and assessment of the RMMs and we perform additional risk assessment procedures; and/or

- a potential RMM exists that we had not previously identified and assessed.

For example, during our substantive procedures over debt, we might become aware that the entity is negotiating a new financing arrangement. This new information may prompt us to identify additional RMMs related to the issuance of new debt instruments, or possibly revise our original assessment of some of the RMMs — i.e. reassess the inherent risk for some RMMs.

When we identify information that contradicts our original risk assessment, we first determine whether we have all the facts and relevant information before we can determine the effect on our risk assessment.

For example, during our substantive procedures over revenue recognition, we might identify new contracts related to a new type of service that the entity recently began offering. This may represent evidence that contradicts our original risk assessment; however, before we can determine the revisions to our risk assessment, we may perform additional procedures to understand this new revenue stream — e.g. the types of services, the materiality of the service contracts, the duration of the contracts, the locations where the service is offered and how the entity is accounting for the service revenue.

Once we have all the information, we determine the impacts on our risk assessment, we revise our risk assessment, and we determine how to modify our planned audit approach.

[How do we revise our inherent risk assessment in response to contradictory evidence?](#) [ISA | 578.1800]

The following questions can help determine whether, and how, to revise our inherent risk assessment in response to contradictory evidence.

- Does this information highlight or provide more information about a type or source of potential misstatement we had not previously considered?
- Does this information reveal a previously unidentified risk to consider and assess?
- What other accounts could be affected by this information? For example, if we find a misstatement in accounts receivable, this may lead us to revise our risk assessment for revenue.
- How does this information affect our inherent risk assessment and, as a result, our combined assessed risk (CAR) assessment?
- Does this information indicate a more widespread or pervasive issue — e.g. possible management bias, whether intentional (fraudulent) or unintentional — that may affect financial statement-level risks?
- Does this information indicate fraud risk factors or a fraud risk that we had not previously considered?

If we determine to revise our inherent risk assessment, these revisions may include one or more of the following:

- changing our assessment of inherent risk;
- identifying a new RMM that we had not previously identified; and/or
- revising an RMM that we had previously identified.

Given the complexities and potential effects on our audit, it is helpful to involve more-senior members of the engagement team when considering whether and how to revise our inherent risk assessment.

How do we modify our planned audit approach? [ISA | 578.1900]

We can modify our planned audit approach by:

- designing and performing additional procedures — e.g. performing an additional procedure that's specifically designed to address a newly identified RMM; or
- making changes to our original planned procedure(s), which may include one or a combination of the following:
 - performing additional risk assessment procedures if the original procedures do not provide an appropriate basis for the identification and assessment of the RMMs;
 - designing and implementing an overall response — especially when we are responding to a more widespread or pervasive issue;
 - changing the type of procedure we perform — e.g. we may confirm the terms and conditions of sales arrangements directly with customers rather than inspecting a signed contract, or we may determine that a test of details is more appropriate than a substantive analytical procedure — i.e. changing the nature of the procedure;
 - increasing the number of items that we choose to test — i.e. changing the extent of the procedure;
 - performing our procedures on the period-end balance, rather than at an interim date — i.e. changing the timing of the procedure;
 - testing controls to reduce control risk — e.g. identifying controls that address the risk and testing their operating effectiveness; and
 - determining whether to revise our planned employed KPMG specialist involvement — e.g. in response to a material business combination, we may amend our planned audit approach by involving an employed KPMG specialist to help audit the assumptions management used to value the acquired assets and liabilities, and evaluate the work of the management's specialist.

Do we always modify our planned audit procedures when we revise our risk assessment? [ISA | 578.2000]

If we revise our risk assessment, there is a presumption that we will modify our audit procedures in response. If we don't, we may fail to properly respond to or address an RMM in our audit.

In those situations where we revise our risk assessment and do not modify our planned audit procedures, we document the facts and circumstances that led to this conclusion to evidence our thought process and how we applied professional skepticism. This is expected to be rare.

Examples

How do we respond to evidence that contradicts the evidence on which we based our original risk assessment? [ISA | 578.2200]

Fact pattern:

The engagement team is performing audit procedures that address RMMs related to the Accuracy and Valuation of accounts receivable. In their original risk assessment, the team assessed inherent risk for the RMMs related to the Valuation assertion at Base — i.e. lower on the inherent risk continuum.

Analysis:

The following scenarios set out examples of evidence that contradicts the team's original risk assessment, and how it may affect the risk assessment and planned audit procedures.

Scenario 1 | Identifying misstatements

When the team performed substantive testing, they identified misstatements in the receivables recorded at period end, because the entity did not properly account for certain rebates offered to customers.

Revision to the original risk assessment

When investigating the nature and cause of audit misstatements, the team found that they may be the result of the entity not accounting for certain rebates offered to customers.

The team had not previously identified an RMM in connection with customer rebates. They therefore identified a new RMM because rebates were not appropriately accounted for.

Revision to planned audit procedures

In response to the newly identified RMM, the engagement team planned additional audit procedures, to confirm the terms of rebate arrangements directly with customers, as well as to recalculate the rebate due and the appropriate closing balance of accounts receivable.

Scenario 2 | Identifying misstatements

During the team's risk assessment procedures, they obtained an understanding of how management measures its allowance for bad debt. They specifically identified that the measurement uses a few simple non-judgmental based inputs — e.g. the number of days that an invoice is outstanding.

As the team performed their audit procedures over revenue, they learned that the entity changed its payment terms during the period. This resulted in a change to how it determines the amount of the allowance necessary at each period end. The entity now has specific payment terms with each customer, and evaluates the collectability of each customer balance separately, using a variety of qualitative factors to determine the appropriate allowance.

Revision to the original risk assessment

The allowance for bad debt is now measured based on more subjective, qualitative factors instead of a non-judgmental determination.

The team determined that inherent risk for the RMMs related to the Valuation assertion of accounts receivable is higher on the inherent risk continuum than they originally assessed and conclude it is Elevated or Significant.

As a result, the team revised their CAR assessment compared to their original assessment (for example EN/EC or SN/SC depending on whether the team selected the control approach and/or the result of test of controls).

Revision to planned audit procedures

As the team revised their CAR assessment, they reconsidered the specific audit procedures to address the RMMs related to the Valuation assertion of accounts receivable.

They decided to change the nature of their audit procedures to confirm the payment terms directly with the customer. Additionally, they confirmed accounts receivable balances with a larger proportion of the population — i.e. they increased the extent of their procedures.

Classes of Transactions, Account Balances and Disclosures that Are Not Significant, but Which Are Material

International Standards on Auditing: ISA 315.36

Classes of Transactions, Account Balances and Disclosures that Are Not Significant, but Which Are Material

36. For material classes of transactions, account balances or disclosures that have not been determined to be significant classes of transactions, account balances or disclosures, the auditor shall evaluate whether the auditor's determination remains appropriate. (Ref: Para. A233-A235)

ISA Application and Other Explanatory Material: ISA 315.A233-A235

Classes of Transactions, Account Balances and Disclosures that Are Not Significant, but Which Are Material (Ref: Para. 36)

A233. As explained in ISA 320,⁶³ materiality and audit risk are considered when identifying and assessing the risks of material misstatement in classes of transactions, account balances and disclosures. The auditor's determination of materiality is a matter of professional judgment, and is affected by the auditor's perception of the financial information needs of users of the financial statements.⁶⁴ For the purpose of this ISA and paragraph 18 of ISA 330, classes of transactions, account balances or disclosures are material if omitting, misstating or obscuring information about them could reasonably be expected to influence the economic decisions of users taken on the basis of the financial statements as a whole.

63 ISA 320, paragraph A1

64 ISA 320, paragraph 4

A234. There may be classes of transactions, account balances or disclosures that are material but have not been determined to be significant classes of transactions, account balances or disclosures (i.e., there are no relevant assertions identified).

Example:

The entity may have a disclosure about executive compensation for which the auditor has not identified a risk of material misstatement. However, the auditor may determine that this disclosure is material based on the considerations in paragraph A233.

A235. Audit procedures to address classes of transactions, account balances or disclosures that are material but are not determined to be significant are addressed in ISA 330.⁶⁵ When a class of

transactions, account balance or disclosure is determined to be significant as required by paragraph 29, the class of transactions, account balance or disclosure is also a material class of transactions, account balance or disclosure for the purposes of paragraph 18 of ISA 330.

65 ISA 330, paragraph 18

How do we comply with the Standards? [ISA | KAEGLDWC]

1 Identify significant accounts and disclosures and their relevant assertions [ISA | 566]

What do we do?

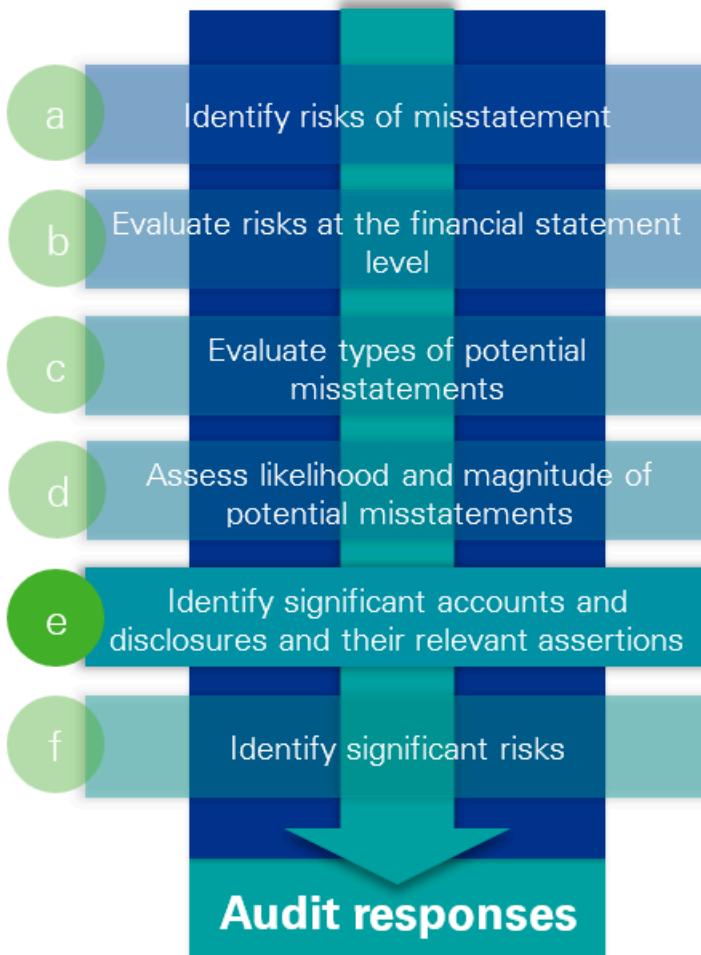
Identify significant accounts and disclosures and their relevant assertions

Why do we do this?

Determining relevant assertions and significant accounts and disclosures helps us identify the specific elements of the financial statements to focus on in our audit and design procedures in response to the identified risks of material misstatements (RMMs).

Execute the Audit

Where are we in our risk assessment? [ISA | 566.1300]



What is a significant account or disclosure, and what is a relevant assertion? [ISA | 566.1400]

Significant accounts and disclosures and their relevant assertions are those with a reasonable possibility of containing a material misstatement. In other words, they relate to an RMM.

Relevant assertion	Each assertion that has one or more RMM
Significant account or significant disclosure	Each account or disclosure that has one or more relevant assertion (and therefore one or more RMM)

Following that logic, if we *don't* identify an assertion as relevant, or an account or disclosure as significant, then we've concluded that there is a remote chance of a material misstatement arising, both individually and when aggregated with others.

In other words, it doesn't relate to an RMM — so we may perform *no* specific audit procedures over that assertion, financial statement line item or disclosure.*

- * There are certain areas within the financial reporting process where procedures are always performed even if there is no RMM (e.g. disclosures: agree/reconcile information in the disclosure to the underlying accounting records).

How do we identify significant accounts and disclosures and their relevant assertions? [ISA | 566.8693]

We have already associated each RMM with the specific accounts, disclosures and assertions it affects. This means we've essentially identified our initial population of significant accounts, disclosures and relevant assertions.

After identifying our initial population, we perform three additional activities that help validate the population of significant accounts, disclosures and relevant assertions.

1	Evaluate inherent risk factors	<p>Evaluate the inherent risk factors (see question 'What factors do we consider in assessing likelihood and magnitude and level of inherent risk?') related to each financial statement line item and disclosure and their assertions.</p> <p>This helps us consider whether we missed any significant accounts, disclosures and relevant assertions through our initial analysis.</p>
2	Step back and assess accounts and disclosures we did not identify as significant, and assertions we did not identify as relevant	<p>Consider the accounts and disclosures we did not identify as significant and the assertions we did not identify as relevant.</p> <p>Step back and assess whether those accounts, disclosures and assertions — both individually and in the aggregate — have a reasonable possibility of containing a material misstatement.</p> <p>This aggregate assessment includes considering possible similarities in the accounts and disclosures. This acts as an additional check on our population of significant accounts, disclosures and relevant assertions.</p> <p>We perform the individual assessment on an assertion-by-assertion basis for each account and disclosure. This aggregate assessment includes thinking about:</p> <ul style="list-style-type: none"> • similarities that may exist in these accounts, disclosures and assertions; and • other factors that may increase the chances of multiple misstatements aggregating to a material misstatement. <div style="background-color: #D9D9D9; padding: 10px; margin-top: 10px;"> <p>For example, we may look at the total impact these accounts have on:</p> <ul style="list-style-type: none"> • total current assets/liabilities; • total assets/liabilities; • total revenue/expenses; or </div>

		<ul style="list-style-type: none"> • net income. <p>When we evaluate these accounts, disclosures and assertions in the aggregate, we think about the same inherent risk factors we evaluated in step 1.</p>
3	Step back and evaluate whether for material classes of transactions, account balances or disclosures, that have not been determined to be significant classes of transactions, account balances or disclosures, this remains appropriate	<p>As a final step, we consider those material accounts that we did not identify as significant accounts and evaluate whether this remains appropriate.</p> <p>This helps us to challenge and properly analyse our initial conclusions before we plan and perform audit procedures.</p>

Do we perform substantive procedures for material accounts and disclosures we have not identified as significant? [ISA | 566.8879]

Yes. See activity '[Design and perform substantive procedures for accounts and disclosures with no RMMs](#)'.

What accounts are considered 'material accounts'? [ISA | 566.11297]

Material accounts are accounts that are equal to or greater than materiality.

What if we identify an RMM after our initial assessment? [ISA | 566.11216]

If we determine there is a reasonable possibility of a material misstatement arising in:

- the accounts and disclosures we did not initially identify as significant; or
- the assertions we did not initially identify as relevant,

then we revisit our risk assessment decisions and identify additional RMMs. This may indicate that we didn't obtain a sufficient understanding of the entity's processes during risk assessment and may prompts us to reassess our understanding of the entity, including the flow of information for transactions, events and conditions.

When we identify additional significant accounts and relevant assertions, we also think about why we selected those accounts as opposed to the other accounts. We then identify the RMMs that led us to this conclusion.

Group Audit | How do we identify the significant accounts and disclosures and their relevant assertions in a group audit? [ISA | 566.1510]

As the lead group auditor, we take responsibility for the identification of all significant accounts and disclosures and their relevant assertions based on the group financial statements.

It is an iterative process. Since most assertion-level RMMs of the group financial statements will arise in components, we in practice, as the lead group auditor, may perform the following:

- (1) perform initial risk assessment procedures at the group level and evaluate qualitative and quantitative risk factors to identify those accounts, disclosures and assertions that have indicators that they are likely significant accounts or disclosures and relevant assertions
- (2) identify components for which more granular risk assessment procedures will be performed based upon the likely significant accounts and disclosures and their relevant assertions
- (3) use our knowledge from the risk assessment procedures we perform at the group level or component level
- (4) communicate with component auditors (i.e. RAPD or other two way communication) regarding their knowledge from the risk assessment procedures that they perform at the component level, including their identification of significant accounts and disclosures and their relevant assertions.

[Group Audit | What does 'take responsibility for' mean?](#) [ISA | 566.160253]

'Take responsibility for' means the lead group auditor may either design and/or perform procedures, tasks, or actions themselves or are permitted to assign the design and/or performance of procedures, tasks or actions to other appropriately skilled or suitably experienced members of the engagement team, including component auditors.

Assigning the design and/or performance of procedures to another member of the engagement team, however, does not relieve the lead group auditor of their responsibility for the overall design and performance of the audit

[At what level do we identify accounts and disclosures?](#) [ISA | 566.1600]

Our goal is to find the highest level of accounts and disclosures where similar risks exist. Therefore, we may start by capturing each financial statement line item. If the financial statement line item contains general ledger accounts or groups of general ledger accounts with different inherent risks of error, inherent risk of fraud, control risks, or controls in place, we may disaggregate them further to the level of general ledger accounts or a group of such accounts.

For example, within trade receivables there may be general ledger accounts for domestic and foreign receivables with different inherent risks that warrant disaggregating into separate accounts.

We may also disaggregate a general ledger account if that is appropriate for our purposes.

For example, the audited entity records all provisions in one general ledger account but for the purpose of our audit we disaggregate this general ledger account into separate provisions because each provision is subject to sufficiently different inherent risks of error, risks of fraud, control risks, or controls in place.

Similarly, for disclosures we may start by capturing each distinct note in the financial statements. Then we may look at the underlying source of the disclosed information to determine if each disclosure is supported by general ledger accounts, subledger accounts, documents prepared by the entity, or external documents (e.g. laws and regulations, group accounting instructions) or a combination of different sources. We may consider whether these sources have different inherent risk characteristics

that warrant disaggregating a disclosure. We may consider how the accounts related to the disclosure have been disaggregated in the business process(es). Additionally, it may be helpful to associate the significant accounting policies (often from Note 1 in financial statements) with each distinct disclosure in the financial statements.

For example, the property and equipment significant accounting policies in Note 1 and the property disclosures in Note 5 have similar inherent risks and relate to the PP&E business process. We may aggregate these into a distinct disclosure in the PP&E business process.

[What if a certain financial statement line item or disclosure contains different types of transactions?](#) [ISA | 566.1700]

Some of an entity's financial statement line items or disclosures will contain several different types of transactions. This is often the case for accounts that contain several different components — e.g. miscellaneous, other and general accounts.

In order to consider all possible risks affecting the account, we understand the different types of transactions included in the accounts and the types of misstatements that could arise. This can help us disaggregate the account risks and properly identify all the RMs and RMMs related to those different types of transactions.

Our audit response addresses each RMM we identify, so we design procedures that consider these different types of potential misstatements.

[Do we perform substantive audit procedures for accounts or disclosures that don't have an RMM?](#) [ISA | 566.8695]

Yes. We perform substantive audit procedures for accounts or disclosures that don't have an RMM, but those instances are limited to:

- when we perform procedures related to material non-significant accounts (MNSAs) (see activity '[Design and perform substantive procedures for accounts and disclosures with no RMMs](#)' for additional information);
- when we perform procedures specifically to incorporate an element of unpredictability in our audits (see activity '[Incorporate elements of unpredictability](#)' for additional information);
- when we perform additional substantive procedures in response to possible undetected misstatements that could make the financial statements materially misstated (see activity '[Consider the possibility of undetected misstatements and its implications](#)' for additional information);
- certain areas within the financial reporting process where procedures are always performed even if there is no RMM (e.g. disclosures: agree/reconcile information in the disclosure to the underlying accounting records).

[What are financial statement assertions?](#) [ISA | 566.11274]

Financial statement assertions are representations by management, explicit or otherwise, that are embodied in the financial statements, as used by us to consider the different types of potential misstatements that may occur.

In representing that the financial statements are in accordance with the applicable financial reporting framework, management implicitly or explicitly makes assertions regarding recognition, measurement and presentation of classes of transactions and events, account balances and disclosures.

For example, when management provides us with a draft of the financial statements, they are implicitly asserting that accounts payable is complete. We relate these assertions associated with significant accounts to the potential types of RMs when identifying RMMs and ultimately designing our planned audit procedures to gather audit evidence that is responsive to those RMMs.

[What financial statement assertions do we use?](#) [ISA | 566.11276]

The following table describes the relevant assertions for classes of transactions, account balances and their related disclosures, which is derived from the standards:

KPMG Assertion	Income Statement Classes of Transactions	Balance Sheet Account balances
C Completeness	All transactions and events have been recorded. These transactions and events have been recorded in the correct accounting period (i.e. no understatement due to cut-off).	All assets, liabilities and equity interests have been recorded.
E Existence (account balances) and Occurrence (class of transaction)	Transactions and events that have been recorded have occurred. These transactions and events have been recorded in the correct accounting period (i.e. no overstatement due to cut-off).	Assets, liabilities and equity interests exist.
A Accuracy	Amounts and other data relating to recorded transactions and events have been recorded correctly.	Amounts and other data relating to recorded assets, liabilities and equity interests have been recorded correctly.

V Valuation	Transactions and events have been recorded at appropriate amounts (i.e. are appropriately valued).	Assets, liabilities and equity interests have been recorded at appropriate amounts and any resulting valuation or allocation adjustments are appropriately recorded
O Obligations and Rights	The entity has the rights and obligations to transactions and events that it has recorded (i.e. transactions and events pertain to the entity).	The entity holds or controls the rights to assets. Liabilities and equity interests are the obligations of the entity.
P Presentation	<p>Financial information is appropriately presented and disclosed in the financial statements.</p> <p>Classes of transactions and events or assets, liabilities and equity interests:</p> <ul style="list-style-type: none"> • have been recorded in the proper accounts and are classified to the appropriate financial statement line item; • are appropriately aggregated or disaggregated and clearly described; • have occurred and/or are relevant to the accounting period; and • pertain to the entity. <p>Disclosures related to classes of transactions and events or assets, liabilities and equity interests:</p> <ul style="list-style-type: none"> • are relevant and understandable in the context of the requirements of the applicable financial reporting framework; • are complete (i.e. all disclosures related to classes of transaction, account balances and other matters have been included in the financial statements); and • are disclosed at appropriate amounts (i.e. are appropriately measured and described). 	

Other matters disclosed in the financial statements are disclosures not directly related to recorded classes of transaction or account balances.

For example, the entity may describe its exposure to risks arising from financial instruments, including:

- how the risks arise;

- the objectives, policies and processes for managing the risks; and
- the methods used to measure the risks.

Examples

How do we consider accounts, disclosures and assertions not identified as significant in the aggregate?

[ISA | 566.11279]

Fact pattern:

Entity X records operating expenses in multiple accounts.

Account	Balance (\$)
Payroll expense	37,000
Depreciation expense	29,000
Rent expense	8,500
Advertising expense	7,600
Utilities expense	750
Amortization expense	250
Total operating expenses	\$83,100

First, the engagement team identify RMMs related to payroll expense and depreciation expense, making these significant accounts. The relevant assertions for those identified RMMs are Completeness, Existence and Accuracy.

Analysis:

Stepping back, the team analyze the remaining accounts, disclosures and assertions that they did not identify as significant or relevant.

Their initial decision to identify no RMMs over the completeness of each remaining expense account remains appropriate. But they reach a different conclusion when they step back and consider these accounts in combination — i.e. that an RMM exists in the aggregate relating to the Completeness of these expense accounts.

In this case, they identify that the performance of procedures over the Completeness assertion of the other expense accounts are necessary. They identify RMMs relating to the Completeness of rent expenses (\$8,500) and advertising expenses (\$7,600). They then step back and conclude that there is no longer a reasonable possibility of material misstatement in the remaining expense accounts.

If the team hadn't been able to identify specific accounts for which Completeness was relevant, they might instead have identified Completeness as a relevant assertion for *all* the remaining expense accounts, and included them as significant accounts.

Revision of Risk Assessment

International Standards on Auditing: ISA 315.37

Revision of Risk Assessment

37. If the auditor obtains new information which is inconsistent with the audit evidence on which the auditor originally based the identification or assessments of the risks of material misstatement, the auditor shall revise the identification or assessment. (Ref: Para. A236)

ISA Application and Other Explanatory Material: ISA 315.A236

Revision of Risk Assessment (Ref: Para. 37)

A236. During the audit, new or other information may come to the auditor's attention that differs significantly from the information on which the risk assessment was based.

Example:

The entity's risk assessment may be based on an expectation that certain controls are operating effectively. In performing tests of those controls, the auditor may obtain audit evidence that they were not operating effectively at relevant times during the audit. Similarly, in performing substantive procedures the auditor may detect misstatements in amounts or frequency greater than is consistent with the auditor's risk assessments. In such circumstances, the risk assessment may not appropriately reflect the true circumstances of the entity and the further planned audit procedures may not be effective in detecting material misstatements. Paragraphs 16 and 17 of ISA 330 provide further guidance about evaluating the operating effectiveness of controls.

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Continue to assess RMMs, and revise audit approach as necessary [ISA | 578]

What do we do?

Continue our assessment of the risks of material misstatement, including fraud risks, throughout the audit and revise the risk assessment and planned audit procedures in response to audit evidence that contradicts our original risk assessment.

Why do we do this?

If we fail to identify and properly assess a potential risk, it can negatively affect our audit. Similarly, if we ignore or fail to revise our risk assessment, our audit response may be insufficient or inappropriate. Therefore, we consider the information we learn throughout the audit process and determine whether it affects our original risk assessment. Risk assessment drives our audit responses, so changes to our original risk assessment can affect our audit procedures.

Execute the Audit

What does it mean to continue our risk assessment throughout the audit? [ISA | 578.1300]

Risk assessment is an iterative process, rather than something we perform only at the beginning of the audit. During the course of the audit, we constantly obtain new information and evidence. This may support or contradict our original risk assessment and can affect our overall audit plan.

For example, information that supports our original risk assessment might support the fact that a specific risk exists, that we assessed it appropriately, and that we linked the risks of material misstatement (RMMs) to the appropriate assertions, accounts and disclosures.

As we obtain information or evidence throughout the audit, we consider whether it supports or contradicts our original risk assessment. 'Throughout the audit' means through performing our risk assessment, control and substantive procedures, all the way to when we form our audit opinion. This enables us to:

- identify evidence that contradicts our original risk assessment; and
- respond appropriately by revising our, or performing additional, risk assessment and planned audit procedures.

How do we identify whether information or evidence contradicts our original risk assessment? [ISA | 578.1400]

We obtain many different types of audit evidence and learn things about the entity throughout our audit. This evidence and information may or may not corroborate our original risk assessment. Asking ourselves:



Does this evidence or information tell me something new or different about the risks affecting the entity?

can help identify situations where evidence may contradict or be inconsistent with our original risk assessment.

For example, any of the following information or evidence identified when performing our procedures over cash and cash equivalents, individually or in any combination, may indicate a need to assess a heightened inherent risk or reassess our original risk assessment, including our fraud risk assessment:

Changes from prior period in account or disclosure characteristics:

- Lack of clarity regarding noticeable changes in account balance and activity compared to prior year;
- New authorized signers on a cash account without appropriate explanation;
- Change in contact address for external confirmation;
- Account balance transfers or account closures, especially those that occur at (or close to) year-end, that are unexplained or lack business purpose; or
- Newly created bank accounts, especially those that are created at (or close to) year-end, without appropriate explanation.

Susceptibility to misstatement due to error or fraud:

- Slow response time to confirmation request; or
- Unusual or unexpected responses to confirmation requests.

What types of information or evidence might contradict our original risk assessment? [ISA | 578.1500]

Evidence that contradicts our original risk assessment may come in many forms. A few common types include:

- control deficiencies;
- audit misstatements;
- overall changes in the entity's business — e.g. business combinations, dispositions;
- changes in the entity and its environment; and
- other information that appears to be inconsistent with what we obtained during our risk assessment procedures.

Will a control deficiency affect our inherent risk assessment? [ISA | 578.11494]

Our inherent risk assessment does not consider the effect of controls; however, identifying control deficiencies can provide information that contradicts our inherent risk assessment.

For example, we may identify a deficiency in controls over the measurement of the allowance for bad debts. That deficiency may highlight that the measurement is more complex and involves more judgment than we originally thought, causing us to revise our inherent risk assessment.

What if we are unsure whether information or evidence we have obtained contradicts our original risk assessment? [ISA | 578.1600]

When challenged to determine whether new information contradicts our original risk assessment, we think about the possible impacts carefully. Failing to revise our risk assessment can mean we fail to respond properly in our audit. Sometimes, it can help to think about what we might do differently as a result of the information, to better consider what risks may be affected and what we revised.

As a practical consideration, when there is uncertainty about whether information contradicts our original risk assessment, that uncertainty is a strong indicator that the information is contradictory — and we therefore revise our risk assessment and planned audit procedures.

What if we identify information that contradicts our original risk assessment? [ISA | 578.1700]

Information that contradicts our original risk assessment may suggest that:

- our inherent risk assessment for a specific risk may be incorrect — for example, evidence that a particular RMM we initially assessed at Base may actually be Elevated; and/or
- original risk assessment procedures do not provide an appropriate basis for the identification and assessment of the RMMs and we perform additional risk assessment procedures; and/or
- a potential RMM exists that we had not previously identified and assessed.

For example, during our substantive procedures over debt, we might become aware that the entity is negotiating a new financing arrangement. This new information may prompt us to identify additional RMMs related to the issuance of new debt instruments, or possibly revise our original assessment of some of the RMMs — i.e. reassess the inherent risk for some RMMs.

When we identify information that contradicts our original risk assessment, we first determine whether we have all the facts and relevant information before we can determine the effect on our risk assessment.

For example, during our substantive procedures over revenue recognition, we might identify new contracts related to a new type of service that the entity recently began offering. This may represent evidence that contradicts our original risk assessment; however, before we can determine the revisions to our risk assessment, we may perform additional procedures to understand this new revenue stream — e.g. the types of services, the materiality of the service contracts, the duration of the contracts, the locations where the service is offered and how the entity is accounting for the service revenue.

Once we have all the information, we determine the impacts on our risk assessment, we revise our risk assessment, and we determine how to modify our planned audit approach.

[How do we revise our inherent risk assessment in response to contradictory evidence?](#) [ISA | 578.1800]

The following questions can help determine whether, and how, to revise our inherent risk assessment in response to contradictory evidence.

- Does this information highlight or provide more information about a type or source of potential misstatement we had not previously considered?
- Does this information reveal a previously unidentified risk to consider and assess?
- What other accounts could be affected by this information? For example, if we find a misstatement in accounts receivable, this may lead us to revise our risk assessment for revenue.
- How does this information affect our inherent risk assessment and, as a result, our combined assessed risk (CAR) assessment?
- Does this information indicate a more widespread or pervasive issue — e.g. possible management bias, whether intentional (fraudulent) or unintentional — that may affect financial statement-level risks?
- Does this information indicate fraud risk factors or a fraud risk that we had not previously considered?

If we determine to revise our inherent risk assessment, these revisions may include one or more of the following:

- changing our assessment of inherent risk;

- identifying a new RMM that we had not previously identified; and/or
- revising an RMM that we had previously identified.

Given the complexities and potential effects on our audit, it is helpful to involve more-senior members of the engagement team when considering whether and how to revise our inherent risk assessment.

How do we modify our planned audit approach? [ISA | 578.1900]

We can modify our planned audit approach by:

- designing and performing additional procedures — e.g. performing an additional procedure that's specifically designed to address a newly identified RMM; or
- making changes to our original planned procedure(s), which may include one or a combination of the following:
 - performing additional risk assessment procedures if the original procedures do not provide an appropriate basis for the identification and assessment of the RMMs;
 - designing and implementing an overall response — especially when we are responding to a more widespread or pervasive issue;
 - changing the type of procedure we perform — e.g. we may confirm the terms and conditions of sales arrangements directly with customers rather than inspecting a signed contract, or we may determine that a test of details is more appropriate than a substantive analytical procedure — i.e. changing the nature of the procedure;
 - increasing the number of items that we choose to test — i.e. changing the extent of the procedure;
 - performing our procedures on the period-end balance, rather than at an interim date — i.e. changing the timing of the procedure;
 - testing controls to reduce control risk — e.g. identifying controls that address the risk and testing their operating effectiveness; and
 - determining whether to revise our planned employed KPMG specialist involvement — e.g. in response to a material business combination, we may amend our planned audit approach by involving an employed KPMG specialist to help audit the assumptions management used to value the acquired assets and liabilities, and evaluate the work of the management's specialist.

Do we always modify our planned audit procedures when we revise our risk assessment? [ISA | 578.2000]

If we revise our risk assessment, there is a presumption that we will modify our audit procedures in response. If we don't, we may fail to properly respond to or address an RMM in our audit.

In those situations where we revise our risk assessment and do not modify our planned audit procedures, we document the facts and circumstances that led to this conclusion to evidence our thought process and how we applied professional skepticism. This is expected to be rare.

Examples

How do we respond to evidence that contradicts the evidence on which we based our original risk assessment? [ISA | 578.2200]

Fact pattern:

The engagement team is performing audit procedures that address RMMs related to the Accuracy and Valuation of accounts receivable. In their original risk assessment, the team assessed inherent risk for the RMMs related to the Valuation assertion at Base — i.e. lower on the inherent risk continuum.

Analysis:

The following scenarios set out examples of evidence that contradicts the team's original risk assessment, and how it may affect the risk assessment and planned audit procedures.

Scenario 1 | Identifying misstatements

When the team performed substantive testing, they identified misstatements in the receivables recorded at period end, because the entity did not properly account for certain rebates offered to customers.

Revision to the original risk assessment

When investigating the nature and cause of audit misstatements, the team found that they may be the result of the entity not accounting for certain rebates offered to customers.

The team had not previously identified an RMM in connection with customer rebates. They therefore identified a new RMM because rebates were not appropriately accounted for.

Revision to planned audit procedures

In response to the newly identified RMM, the engagement team planned additional audit procedures, to confirm the terms of rebate arrangements directly with customers, as well as to recalculate the rebate due and the appropriate closing balance of accounts receivable.

Scenario 2 | Identifying misstatements

During the team's risk assessment procedures, they obtained an understanding of how management measures its allowance for bad debt. They specifically identified that the measurement uses a few simple non-judgmental based inputs — e.g. the number of days that an invoice is outstanding.

As the team performed their audit procedures over revenue, they learned that the entity changed its payment terms during the period. This resulted in a change to how it determines the amount of the allowance necessary at each period end. The entity now has specific payment terms with each customer, and evaluates the collectability of each customer balance separately, using a variety of qualitative factors to determine the appropriate allowance.

Revision to the original risk assessment

The allowance for bad debt is now measured based on more subjective, qualitative factors instead of a non-judgmental determination.

The team determined that inherent risk for the RMMs related to the Valuation assertion of accounts receivable is higher on the inherent risk continuum than they originally assessed and conclude it is Elevated or Significant.

As a result, the team revised their CAR assessment compared to their original assessment (for example EN/EC or SN/SC depending on whether the team selected the control approach and/or the result of test of controls).

Revision to planned audit procedures

As the team revised their CAR assessment, they reconsidered the specific audit procedures to address the RMMs related to the Valuation assertion of accounts receivable.

They decided to change the nature of their audit procedures to confirm the payment terms directly with the customer. Additionally, they confirmed accounts receivable balances with a larger proportion of the population — i.e. they increased the extent of their procedures.

Documentation

International Standards on Auditing: ISA 315.38

Documentation

38. The auditor shall include in the audit documentation:¹³ (Ref: Para. A237-A241)

- (a) The discussion among the engagement team and the significant decisions reached;
- (b) Key elements of the auditor's understanding in accordance with paragraphs 19, 21, 22, 24 and 25; the sources of information from which the auditor's understanding was obtained; and the risk assessment procedures performed;
- (c) The evaluation of the design of identified controls, and determination whether such controls have been implemented, in accordance with the requirements in paragraph 26; and
- (d) The identified and assessed risks of material misstatement at the financial statement level and at the assertion level, including significant risks and risks for which substantive procedures alone cannot provide sufficient appropriate audit evidence, and the rationale for the significant judgments made.

¹³ ISA 230, Audit Documentation, paragraphs 8-11, and A6-A7

ISA Application and Other Explanatory Material: ISA 315.A237-A241

Documentation (Ref: Para. 38)

A237. For recurring audits, certain documentation may be carried forward, updated as necessary to reflect changes in the entity's business or processes.

A238. ISA 230 notes that, among other considerations, although there may be no single way in which the auditor's exercise of professional skepticism is documented, the audit documentation may nevertheless provide evidence of the auditor's exercise of professional skepticism.⁶⁶ For example, when the audit evidence obtained from risk assessment procedures includes evidence that both corroborates and contradicts management's assertions, the documentation may include how the auditor evaluated that evidence, including the professional judgments made in evaluating whether the audit evidence provides an appropriate basis for the auditor's identification and assessment of the risks of material misstatement. Examples of other requirements in this ISA for which documentation may provide evidence of the exercise of professional skepticism by the auditor include:

- Paragraph 13, which requires the auditor to design and perform risk assessment procedures in a manner that is not biased towards obtaining audit evidence that may corroborate the existence of risks or towards excluding audit evidence that may contradict the existence of risks;
- Paragraph 17, which requires a discussion among key engagement team members of the application of the applicable financial reporting framework and the susceptibility of the entity's financial statements to material misstatement;
- Paragraphs 19(b) and 20, which require the auditor to obtain an understanding of the reasons for any changes to the entity's accounting policies and to evaluate whether the entity's accounting policies are appropriate and consistent with the applicable financial reporting framework;
- Paragraphs 21(b), 22(b), 23(b), 24(c), 25(c), 26(d) and 27, which require the auditor to evaluate, based on the required understanding obtained, whether the components of the entity's system of internal control are appropriate to the entity's circumstances considering the nature and complexity of the entity, and to determine whether one or more control deficiencies have been identified;
- Paragraph 35, which requires the auditor to take into account all audit evidence obtained from the risk assessment procedures, whether corroborative or contradictory to assertions made by management, and to evaluate whether the audit evidence obtained from the risk assessment procedures provides an appropriate basis for the identification and assessment of the risks of material misstatement; and
- Paragraph 36, which requires the auditor to evaluate, when applicable, whether the auditor's determination that there are no risks of material misstatement for a material class of transactions, account balance or disclosure remains appropriate.

66 ISA 230, paragraph A7

Scalability

A239. The manner in which the requirements of paragraph 38 are documented is for the auditor to determine using professional judgment.

A240. More detailed documentation, that is sufficient to enable an experienced auditor, having no previous experience with the audit, to understand the nature, timing and extent of the audit procedures performed, may be required to support the rationale for difficult judgments made.

A241. For the audits of less complex entities, the form and extent of documentation may be simple and relatively brief. The form and extent of the auditor's documentation is influenced by the nature, size and complexity of the entity and its system of internal control, availability of information from the entity and the audit methodology and technology used in the course of the audit. It is not necessary to document the entirety of the auditor's understanding of the entity and matters related to it. Key elements⁶⁷ of understanding documented by the auditor may include those on which the auditor based the assessment of the risks of material misstatement. However, the auditor is not required to document every inherent risk factor that was taken into account in identifying and assessing the risks of material misstatement at the assertion level.

Example:

In audits of less complex entities audit documentation may be incorporated in the auditor's documentation of the overall strategy and audit plan.⁶⁸ Similarly, for example, the results of the risk assessment may be documented separately, or may be documented as part of the auditor's documentation of further audit procedures.⁶⁹

67 ISA 230, paragraph 8

68 ISA 300, Planning an Audit of Financial Statements, paragraphs 7, 9 and A11

69 ISA 330, paragraph 28

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Discuss accounting policies or principles and susceptibility of financial statements to material misstatement [ISA | 553]

What do we do?

Discuss (1) the entity's selection and application of accounting policies or principles, including related disclosure requirements and (2) the susceptibility of financial statements to material misstatement due to error or fraud

Why do we do this?

Engaging in a meaningful discussion about the entity's accounting policies or principles, how they've been applied, and whether they're appropriate — while considering where the entity's financial statements may be more susceptible to material misstatement — is likely to confirm, or may point us to new, risks of material misstatement (RMMs).

Execute the Audit

What do we focus on when discussing the application of the financial reporting framework including accounting policies or principles, and related disclosure requirements? [ISA | 553.1300]

The Risk Assessment and Planning Discussion (RAPD) includes a meaningful, thought-provoking analysis of:

- the financial reporting framework, including the entity's accounting policies or principles;
- how they have been applied;
- whether they are appropriate to the entity and its circumstances, and
- related disclosure requirements.

Prior-period knowledge and understanding is valuable, and we incorporate it in our discussion. However, all participants in the discussion take a fresh look at these matters.

What questions might we ask during this discussion? [ISA | 553.11518]

Throughout the discussion, we may find it helpful to ask ourselves the following questions.

- Are the accounting policies or principles appropriate for the entity?
- Are they common practice in the industry?
- How have they been implemented — especially in emerging areas, or areas in which the accounting requirements are less prescriptive?
- Will changes in financial reporting requirements result in significant new or revised disclosures?
- Will changes in the entity's environment, financial condition or activities result in significant new or revised disclosures — e.g. a significant business combination in the period under audit?
- Has it been difficult in the past to obtain sufficient appropriate audit evidence for certain disclosures?
- Are there any disclosures about complex matters, including those involving significant management judgment as to what information to disclose?

[How might we begin this discussion? \[ISA | 553.11519\]](#)

We might begin the discussion by inspecting the results of our risk assessment procedures or the entity's accounting policies note from the prior period financial statements, and by considering any changes we are aware of in the current period.

Changes can occur for many reasons, including:

- changes in the entity's business during the period - e.g. a new line of business;
- new accounting policies or principles that were adopted during the period;
- recent significant changes in the economic, regulatory, industry, or other aspects of the environment in which the entity operates; and
- changes in the way the entity applies its current accounting policies or principles.

[What do we focus on when discussing the susceptibility of the entity's financial statements to material misstatement? \[ISA | 553.1400\]](#)

In discussing the susceptibility of the entity's financial statements to material misstatement, we:

- consider all the information gathered throughout risk assessment; and
- share our thoughts about where there may be indications of RMMs, due to both error and fraud.

Our discussion also includes specific consideration of the susceptibility of the financial statements to material misstatement due to error that could result from the entity's related party relationships and transactions.

This may include the matters raised during our RAPD discussion about selecting and applying accounting policies or principles, including related disclosure requirements.

However, we are not limited to items coming from the RAPD discussion. We might also use the prior-period financial statements and related notes as a springboard for discussion, combined with the results of our current-period risk assessment procedures to date.

Our primary goal is to have a robust discussion about the areas of the entity's financial statements that may be susceptible to material misstatements, and therefore evaluate whether RMMs may exist.

Example

What matters might we discuss regarding the entity's selection and application of accounting policies or principles? [ISA | 553.1500]

The table below sets out examples of matters we might identify during risk assessment, and discuss in the RAPD, about the selection and application of accounting policies or principles, including related disclosure requirements.

As we discuss these matters, we consider their effects on risk assessment — specifically on identifying and assessing RMMs.

Matter we identify	Example discussion points	Possible effect
The entity is in the early stages of its lifecycle and has just begun to generate sales. It is now implementing revenue recognition policies.	This is the first time the entity is implementing a revenue accounting policy, so there are increased risks associated with selecting and applying the policy. These are affected by the industry and nature of the sales process.	We identify an RMM related to how the entity records and reports revenue in the financial statements and related disclosures.
The entity has completed a significant business combination and is therefore applying business combination accounting policies or principles for the first time.	This is the first time the entity is applying these accounting policies or principles, and the principles are complex. Significant judgments are involved in accounting for business combinations.	We identify an RMM related to the accounting for business combinations, including related disclosures.
The entity has changed its method for accounting for inventory (from FIFO to average cost).	We explore a series of questions, including: <ul style="list-style-type: none"> • What is the reason for change? • What is accepted within the industry? • Are the entity's systems equipped to manage the change — e.g. can its IT systems properly calculate the average cost? • Was the change adopted at the beginning of the period or mid-period? • How will this be disclosed? 	We identify an RMM related to the cost of inventory recorded and consider whether a fraud risk exists.
Due to rising interest rates, the entity	Given the economic environment, the entity needed to update significant	We identify an RMM related to the

<p>updates significant assumptions in its cash flow model for goodwill valuation.</p>	<p>assumptions in its cash flow model for goodwill to account for the current economic environment, including the discount rate, inflation, and other projected financial information such as revenue and expenses.</p>	<p>valuation of goodwill, including related disclosures.</p>
---	---	--

2 Communicate important matters to team members not involved in the RAPD [ISA | 555]

What do we do?

The lead engagement partner determines which matters are to be communicated to engagement team members not involved in the Risk Assessment and Planning Discussion. The lead engagement partner or other key engagement team members communicate those matters accordingly.

Why do we do this?

Key members of the engagement team may be unable to participate in the Risk Assessment and Planning Discussion (RAPD).

The lead engagement partner is responsible for making sure they are informed of the important matters that were discussed, as these will impact the procedures we perform in response to the risks of material misstatement (RMMs) identified.

Execute the Audit

Who attends the RAPD? [ISA | 555.1300]

Whether we hold one or multiple discussions with the key engagement team members, the lead engagement partner — or another key engagement team member, such as the lead engagement manager — participates in each discussion.

They do this to help maintain consistency, consider each of the key points raised and communicate important matters across the engagement team.

As we plan and conduct the discussion, we think about the overriding objective — to share knowledge and inform team members about important matters that can affect our audit.

Do all key team members participate in the RAPD? [ISA | 555.1400]

It's helpful to have all the key team members in the same place, so we try to find a time where everyone can gather in one place to have the discussion.

However, this may not always be practical, and we may choose to hold separate discussions with some members of the team. For example, an employed KPMG specialist may not be available at the same time as the rest of the team.

Rather than postpone the meeting and potentially delay the planning process, we may meet with those team members separately.

What if key engagement team members are unable to participate in the RAPD? [ISA | 555.1500]

When key engagement team members are unable to participate in the RAPD:

- the lead engagement partner determines which matters to discuss with them; and
- the lead engagement partner (or another key engagement team member) discusses those matters.

A communications plan, agreed by the engagement partner, may be useful.

How else might we hold the RAPD, so that all key engagement team members can be involved? [ISA | 555.1600]

When key engagement team members are unable to participate in person — e.g. if they're in multiple locations — there may be other ways to involve them in the RAPD.

For example, we may use conference calls and/or video-conferencing so that all appropriate people can participate in one discussion.

3 Understand relevant industry, regulatory and other external factors [ISA | 343]

What do we do?

Obtain an understanding of relevant industry, regulatory and other external factors.

Why do we do this?

Risks can arise from the entity's industry or regulatory environment, or from economic conditions.

For example, an oil and gas company is likely affected by risks from rising and falling commodity prices. These fluctuations can affect not only the entity's operations but also its asset values, its ability to service debt, and other areas that could lead to a risk of misstatement.

Understanding the industry, regulatory and other external factors helps us identify and assess risks of material misstatement (RMMs).

Execute the Audit

What does our understanding include? [ISA | 343.1300]

A broad range of topics may be relevant to our understanding. At a minimum, we understand:

- industry factors, including the competitive environment and technological developments;
- the regulatory environment, including the applicable financial reporting framework and the legal and political environment; and
- external factors, including general economic conditions.

See '[Understand the applicable legal and regulatory framework](#)' for additional guidance.

What sources of information can help us understand the relevant industry, regulatory and other external factors? [ISA | 343.1400]

Along with the [common sources of information](#) we use to understand the entity and its environment, we can also use the [Geographical Market Summaries](#) <https://alex.kpmg.com/AROWeb/bridge/6209/17939?d=INTL,US>. These outline potential audit considerations and risks for specific geographic markets.

When we audit entities with operations in multiple locations, these summaries can help us understand the local operating environments.

[What is a financial reporting framework?](#) [ISA | 343.7468]

All financial statements are prepared in accordance with a 'financial reporting framework' — i.e. a set of criteria used to determine how material items are measured, recognized, presented and disclosed in the financial statements. Commonly used financial reporting frameworks include US GAAP and IFRS.

[What matters might we consider when obtaining an understanding of the financial reporting framework?](#)

[ISA | 343.7469]

When obtaining an understanding of the entity's applicable financial reporting framework, and how it applies in the context of the nature and circumstances of the entity and its environment we may consider:

- The entity's financial reporting practices in terms of the applicable financial reporting framework, such as:
 - Accounting principles and industry-specific practices, including for industry-specific significant classes of transactions, account balances and related disclosures in the financial statements (for example, loans and investments for banks, or research and development for pharmaceuticals).
 - Revenue recognition.
 - Accounting for financial instruments, including related credit losses.
 - Foreign currency assets, liabilities and transactions.
 - Accounting for unusual or complex transactions including those in controversial or emerging areas (for example, accounting for cryptocurrency).
- Other accounting rules, regulations and guidance that may apply. For example:
 - Entities in the banking industry may follow other regulatory reporting requirements specific to the jurisdiction in which the entity operates.
 - Entities filing with the SEC also follow SEC rules, regulations and interpretative guidance.

[What information might help us understand the industry, regulatory and other external factors?](#) [ISA |

343.1600]

The table below sets out examples of information we may gather as we obtain our understanding of the relevant industry, regulatory and other external factors.

Type of understanding	Examples of information we may gather
Industry, including competitive environment and technological developments	<ul style="list-style-type: none"> • The entity's competitive environment, including demand, capacity and price competition. For example, the entity may operate in an industry populated with aggressively

	<p>growth-focused start-ups, putting pressure on pricing and margins.</p> <ul style="list-style-type: none"> Highly cyclical or seasonal activity in the entity's industry. For example, entities in the retail industry may see higher sales during holiday seasons. Technological developments. For example, rapid technological changes may make the entity's products obsolete. Energy supplies and costs. For example, volatile fuel prices or disruptions in fuel supplies could affect the operations and financial results of a commercial airline.
Regulatory environment, including applicable financial reporting framework and legal and political environment	<ul style="list-style-type: none"> Applicable financial reporting framework (e.g., US GAAP, IFRS), as well as specific industry practices and changes in accounting standards that are relevant to the entity. Government legislation, regulation or policies. For example, the entity may receive government aid, or be subject to foreign exchange controls, fiscal tariffs or trade restrictions. Tax and environmental laws. For example, the entity may be subject to complex tax laws in multiple tax jurisdictions.
External factors, including general economic conditions	<ul style="list-style-type: none"> Changes in general economic conditions or interest rates. For example, the entity may operate in an inflationary environment or economy in recession. Volatile commodity prices. For example, fluctuating oil prices could affect the operations and financial results of an oil and gas company. Lack of available capital in the marketplace. For example, the entity may have to refinance debt in the next 12 months in a public market with very limited liquidity.

4 Understand the nature of the entity [ISA | 344]

What do we do?

Obtain an understanding of the nature of the entity, including understanding certain specific elements.

Why do we do this?

Risks can arise not only from external factors but also from entity-specific conditions. These include:

- the entity's defining characteristics;
- how the entity conducts business, including its business model; and
- how the entity is organized.

Understanding the nature of the entity can help us identify potential risks of material misstatement (RMMs) in the financial statements.

Execute the Audit

[What do we consider when understanding the nature of the entity?](#) [ISA | 344.1300]

Obtaining an understanding of certain specific elements of the business model can help us understand the nature of the entity overall. These include the entity's:

- organizational structure and management personnel, including ownership and governance structure, including the extent to which the business model integrates the use of IT;
- sources of funding for operations and investment activities, including its capital structure, non-capital funding - e.g. subordinated debt, dependencies on supplier financing - and other debt instruments;
- significant investments, including equity method investments, joint ventures, special-purpose entities and variable-interest entities;
- operating characteristics, including its size and complexity, which might affect the risks of misstatement (RMs) and how the entity addresses those risks;
- sources of earnings, including the relative profitability of key products and services; and
- key supplier and customer relationships.

Our goal in gathering this information is to obtain information that helps us identify and assess risk. We do not gather a detailed history of the entity - e.g. the period in which it was founded - unless we expect that information could lead us to identify RMMs.

[What are examples for each of the specific elements?](#) [ISA | 344.7474]

Obtaining an understanding of certain specific elements can help us understand the nature of the entity overall.

The table below sets out examples for each of the specific elements.

Elements	Examples
Organizational structure and management personnel, including ownership and governance	<ul style="list-style-type: none"> • The scope of the entity's activities, and why it does them. • The entity's structure and scale of its operations. • Whether the entity operates in multiple locations with multiple management levels. Complex structures may give rise to RMMs. For example, there may be RMMs related to accounting for goodwill, joint ventures, investments and special-purpose entities. • Relationships between owners and other people or entities. For example, this information helps determine whether related-party transactions were appropriately identified, accounted for and disclosed in the financial statements.

	<ul style="list-style-type: none"> Few owners with significant ownership interests and seats on the board of directors. Publicly traded and thus owned by many shareholders. In some cases, some or all of those charged with governance may be involved in managing the entity. In other cases, those charged with governance and management may comprise different persons. Governance of the entity may be the collective responsibility of a governing body - e.g. board of directors, supervisory board, partners, trustees, equivalent persons. In smaller entities, one person may be charged with governance, such as an owner-manager or sole trustee.
Sources of funding for operations and investment activities, including capital structure, non-capital funding, and other debt instruments	<ul style="list-style-type: none"> Relies on debt financing involving complex debt covenants. Has significant off-balance sheet financing or leasing arrangements. The entity's capital structure - i.e. proportion of debt versus equity - may have changed from prior periods. Uses derivative financial instruments. The entity may have subsidiaries and associated entities, including consolidated and unconsolidated structures. The beneficial owners may be local or foreign, with or without appropriate business reputation and experience. Obtained financing from a related party. Using newly created digital assets to raise capital in the form of an ICO (initial coin offering).
Significant investments, including equity method investments, joint ventures special-purpose entities and variable-interest entities	<ul style="list-style-type: none"> Significant equity method investments or consolidated SPEs or VIEs, including some with a limited or specific purpose. Holds cryptocurrencies or digital assets as investments for long-term capital appreciation or as a means of exchange during normal operations. Has or plan to make non-recurring acquisitions or divestitures, which may count as significant unusual transactions. Plans to carry out substantial research and development, or make capital expenditures. Investments and dispositions of securities and loans.
Operating characteristics, including size and complexity	<ul style="list-style-type: none"> The entity may be large and complex, operating in several markets and geographic locations. Operates some business segments centrally and others de-centrally. How the entity's business model integrates the use of IT in its interactions with customers, suppliers, lenders and other stakeholders through IT interfaces and other technologies. Uses multiple, distinct IT systems in its business processes. Nature of revenue sources, products or services, and markets.

	<ul style="list-style-type: none"> • Extent of integration of electronic commerce into the entity's operations, for example, in Internet sales and marketing activities. • Conduct of operations (for example, stages and methods of production, or activities exposed to environmental risks). • Alliances, joint ventures, and outsourcing activities. • Geographic dispersion and industry segmentation. • Location of production facilities, warehouses, and offices, and location and quantities of inventories. • Key customers and important suppliers of goods and services, employment arrangements (including the existence of union contracts, pension and other post-employment benefits, stock option or incentive bonus arrangements, and government regulation related to employment matters). • Research and development activities and expenditures. • Transactions with related parties.
Sources of earnings, including relative profitability of key products and services	<ul style="list-style-type: none"> • One profitable revenue stream and others that are near break-even or making losses. • Earns a significant net income from non-operating activities.
Key supplier and customer relationships	<ul style="list-style-type: none"> • Depends on only a few suppliers for its main income-earning activities. • Sells specialized products and services to only a few key customers. • Key supplier may have recently filed for bankruptcy.

What sources of information can help us understand the nature of the entity? [ISA | 344.1400]

We can use the [common sources of information](#) related to understanding the entity and its environment.

How does the organizational structure and physical locations of the entity factor into our understanding of the nature of the entity? [ISA | 344.11456]

We understand the organizational structure of the entity in order to better understand how the entity's physical and geographic locations and presence can generate risks of material misstatement. The information also helps us determine whether the audit represents a group audit or multi-location audit, and how to best organize the audit to address the risks rising from the entity's locations and / or components.

Why does the governance of the entity factor into our understanding of the nature of the entity? [ISA | 344.7471]

We understand the governance of the entity in order to better understand the entity's ability to provide appropriate oversight of its system of internal control. However, this understanding may also provide

evidence of deficiencies, which may indicate an increase in the susceptibility of the entity's financial statements to risks of material misstatement.

[What is a business model?](#) [ISA | 344.7487]

An entity's business model describes how an entity considers, for example its organizational structure, operations or scope of activities, business lines (including competitors and customers of the business lines), processes, growth opportunities, globalization, regulatory requirements and technologies. The entity's business model describes how the entity creates, preserves and captures financial or broader value, for its stakeholders.

[Why does the entity's business model factor into our understanding of the nature of the entity?](#) [ISA | 344.7472]

Understanding the entity's objectives, strategy and business model helps us to understand the entity at a strategic level, and to understand the business risks the entity takes and faces. An understanding of the business risks that have an effect on the financial statements assists us in identifying risks of material misstatement, since most business risks will eventually have financial consequences and, therefore, an effect on the financial statements.

For example, an entity's business model may rely on the use of IT in different ways -

- the entity sells shoes from a physical store, and uses an advanced stock and point of sale system to record the selling of shoes; or
- the entity sells shoes online so that all sales transactions are processed in an IT environment, including initiation of the transactions through a website.

For both of these entities the business risks arising from a significantly different business model would be substantially different, even though both entities sell shoes.

See '[Understand the entity's objectives, strategies and related business risks](#)' for more information.

[What if the entity has invested in special purpose entities \(SPEs\) or variable-interest entities \(VIEs\)?](#) [ISA | 344.1500]

Financial reporting frameworks often set conditions that are deemed to amount to control or circumstances for consolidating an SPE or VIE. The frameworks may also set different bases for recognizing income from them. To interpret these requirements, we often obtain a detailed knowledge of the agreements involving the SPE or VIE.

[What may we understand about how the entity integrates IT into the business model?](#) [ISA | 344.8074]

Our understanding may include the extent and automation of electronic communication with third parties including customers, suppliers, and governments. Additionally, we may understand the extent of use of cryptocurrencies and digital assets including blockchain.

[What are cryptocurrencies and digital assets?](#) [ISA | 344.8080]

A digital asset, in the context of currency and finance, is characterized by its ability to be used for a variety of purposes, including as a means of exchange, as a representation to provide or access goods or services, or as a financing vehicle, such as a security, among other uses. The terms crypto asset and cryptocurrency refer to a type of digital asset that uses cryptography to secure transactions digitally recorded on a distributed ledger (such as a blockchain) and purports to be an item of inherent

value (similar, for instance, to real assets like gold or virtual assets) that are designed to enable purchases, sales, barter or other financial transactions.

Blockchain is a distributed ledger technology that records a list of records, referred to as blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp and transaction data. A block is a collection of digital asset transactions to be recorded on a blockchain.

Virtual currencies, tokens and coins may entitle the holder to other rights as well, such as rights to goods or services from the issuer of the token or a right to financial distributions from the issuing entity or the right to virtual digital assets.

Blockchains, virtual currencies, tokens, and virtual coins may be fully decentralized (i.e. they are not associated with a particular individual or organization), or they may be associated with a particular backing organization (or several organizations in a consortium). In certain cases, whether backed by a traditional organization or not, such digital assets may be considered as being securities.

[What may we understand about the extent of use of cryptocurrencies and digital assets?](#) [ISA | 344.8089]

Addressing certain considerations can be helpful when identifying and assessing risks of misstatement related to cryptocurrency and digital assets when an entity transacts or invests in cryptocurrency and digital assets. These may include:

- What is the purpose or strategy for transacting in digital assets and how do those strategies align with the nature of the entity (e.g. operating characteristics, key performance indicators, sources of earnings, etc.)? Are there associated business risks related to digital asset transactions? What is the entity's underlying business and how do the digital assets relate to the entity's business model?
- Are digital asset transactions intended to be used as a source of funding for the entity's operations (e.g. an initial coin offering or "ICO")? Does the entity keep certain digital assets off the balance sheet?
- What are the relevant legal and regulatory requirements governing the entity's use of digital assets? For example, sales of digital assets (e.g. in an ICO), may represent sales of securities subject to jurisdictional regulations and securities laws. Entities that buy and sell digital assets for others may be subject to other laws and regulations, such as money transmitter rules, 'Anti-Money Laundering' and 'Know Your Customer' considerations. Has the entity considered laws and regulations over digital assets and ICOs in other countries and jurisdictions?
- Does the entity use a third-party exchange or service provider to transact digital assets? Has the entity evaluated whether any of the digital assets it holds or transacts (directly or indirectly through a third-party exchange or servicer) are appropriately registered with securities regulators? Does the entity use exchanges that are appropriately registered based on the nature of the digital assets?
- Has the entity identified relevant regulatory frameworks and compliance requirements (i.e. Bank Secrecy Act 'BCA' or Foreign Account Tax Compliance Act 'FATCA', federal securities laws, depository and/or custodial regulations)? What policies and procedures are in place related to compliance with regulatory frameworks?
- Do the digital assets carry specific rights and obligations including rights to cash flows, ownership characteristics, or utility/discount rights?

- What are the entity's accounting policies related to digital assets, including related disclosures? Has the entity evaluated alternative accounting literature and treatments that could apply to its facts and circumstances? Do accounting and finance personnel have the appropriate knowledge and understanding of the digital asset transactions and how to apply existing accounting policies or principles?
- For subsequent measurements associated with digital assets (e.g., when measuring an impairment of a cryptocurrency investment), how does the entity determine the principal market? For example, some digital assets are listed on multiple exchanges while others are not listed on any exchange and as such an entity may have to employ different methods to subsequently measure these assets in an environment where there may be limited trading history and significant volatility for the asset.
- Are the digital assets held by the entity more common (e.g. Bitcoin, litecoin, XRP, Ether), less common, or emerging? Less common or emerging digital assets are likely to carry additional risks resulting in additional considerations.
- Does the entity offer new products or services to customers that incorporate digital assets (e.g. new investment funds)? How do these products or services differ from the entity's existing product and service lines? Is the entity holding onto the digital assets from a speculative perspective or obtaining the assets through a form of payment related to its primary business? Is the entity consistently trading the digital assets or buying and holding?
- Has the entity considered potential risks associated with the IT requirements to transact in digital assets and compatibility with existing systems? If so, has the entity identified and implemented appropriate policies and procedures to address these potential IT risks?

[What other considerations exist regarding cryptocurrencies and digital assets?](#) [ISA | 344.11457]

Blockchain, distributed ledger technologies, and associated 'digital assets' (e.g. cryptocurrencies, tokens, and coins) can raise a number of auditing, accounting, and financial reporting considerations. Where cryptocurrencies and digital assets are significant to the financial statements, we consider the consultation requirements in the [Global Quality and Risk Management Manual section 9.1.4.](#) <https://www.gqrmm-prod.kworld.kpmg.com/G/0/Content/81?jm=82-policy-23021>

5 Understand and evaluate the entity's selection and application of accounting policies or principles, including related disclosures

[ISA | 346]

What do we do?

Understand and evaluate the entity's selection and application of accounting policies or principles, including related disclosures.

Why do we do this?

An entity's accounting policies or principles can create risks of misstatement (RMs), generally at the assertion level. Our understanding and evaluation of the accounting policies or principles that the entity has selected and applied (including related disclosures) can help us identify and assess risks of material

misstatement (RMMs). Without this understanding, we may be unable to determine whether the entity's transactions are recorded in accordance with generally accepted accounting principles (GAAP), or identify relevant RMs that could stem from applying the financial reporting framework.

Execute the Audit

[What is the output of understanding the entity's selection and application of accounting policies or principles?](#) [ISA | 346.160220]

The output of this activity is generally a technical accounting analysis for each audit area. This analysis outlines our understanding of the accounting policies or principles selected and applied for each audit area. Among other things, the analysis covers the related disclosures, and considers the expertise and experience of the entity's financial reporting personnel. We generally analyze more complex accounting areas in more detail than less complex areas.

[What are accounting policies or principles?](#) [ISA | 346.1400]

Accounting policies or principles are standards and guidelines an entity selects and applies when preparing and presenting financial statements in accordance with a financial reporting framework.

For example, when US GAAP is the financial reporting framework, the FASB's Accounting Standards Codification is the authoritative source of accounting principles. US GAAP entities that are SEC registrants also follow SEC rules and interpretive releases.

Many accounting policies or principles set out in financial reporting frameworks are complex or call for considerable judgment. This is because the underlying economics of a business transaction may be complex or difficult to present without applying judgment or providing detailed disclosures.

In some cases, the financial reporting framework allows an entity to select an accounting principle from a number of alternatives. For example, the entity may have alternatives such as first-in-first-out (FIFO) or average cost for measuring its inventory costs. In other cases, the entity has no choice.

[What sources of information can help us understand the entity's selection and application of accounting policies or principles?](#) [ISA | 346.1600]

The [common sources of information](#) we use to understand the entity and its environment can help us understand the accounting policies or principles the entity has selected and how they are applied. Additional sources that can help us to obtain this understanding include:

- the accounting policies disclosed in the financial statements and, if applicable, management's description of the entity's critical accounting policies and estimates — e.g. information included in an annual report;
- the entity's formal accounting policies and procedures manual;
- authoritative literature from financial reporting standard setters - e.g. FASB Accounting Standards Codification, SEC Staff Accounting Bulletins - and firm publications and interpretations about accounting policies or principles, which can help us understand, for example:
 - whether the standards are complex;
 - whether they require judgment or estimation;
 - what the disclosure requirements are;
 - whether alternative accounting treatments exist;

- resumes and credentials of financial reporting personnel; and
- prior-period work papers, which can help us identify disclosures or accounting policies for which obtaining sufficient appropriate evidence may be difficult.

How do we use this information to understand the entity's selection and application of accounting policies or principles? [ISA | 346.1700]

The common sources of information about the entity and its environment, along with additional sources of information about its accounting framework, policies and practices, can help us understand the entity's selected accounting policies or principles and how they are applied. We begin to obtain our understanding by reading this information, making inquiries and using our knowledge of the financial reporting framework and industry.

In particular, we focus on:

- comparing the entity's accounting policies or principles to those normally used in the industry;
- areas where there is more judgment and complexity in the accounting;
- areas where there are new or revised accounting standards; and
- areas that are ambiguous or not addressed by the entity's financial reporting framework, with attention to information that could help us identify and assess risk.

We then assess those potential risk areas, including those involving complexity, judgment, significant unusual transactions, and changes from the prior period.

How do we evaluate whether the entity has selected and applied the accounting policies or principles appropriately? [ISA | 346.1800]

Once we understand the entity's selection and application of accounting policies or principles, we evaluate their appropriateness. The table below sets out the questions we consider, along with examples of the information we may gather.

Are the accounting policies or principles:	Example
Appropriate for the entity's business?	If the entity chose to depreciate a piece of equipment on a straight-line basis and that method is not a systematic and rational allocation of cost based on the asset's expected usage, we may determine that the related accounting policies or principles are not appropriate for the business.
Consistent with the applicable financial reporting framework?	If the entity uses an accelerated tax depreciation method to depreciate its property, plant and equipment for book purposes, we may determine that the accounting principle selected is not consistent with the entity's applicable financial reporting framework.
Consistent with the accounting policies or principles used	If the entity uses the retail method to account for inventory but is not a retailer, we may determine that the accounting principle selected is not consistent with the entity's business and industry.

in the entity's industry?

What other matters do we evaluate while obtaining an understanding of the entity's selection and application of accounting policies or principles? [ISA | 346.1900]

In certain areas, the likelihood of potential misstatements may be increased. Evaluating these areas may help us understand the accounting policies or principles selected and how they are applied.

These areas include:

- The entity's financial reporting practices in terms of the applicable financial reporting framework. This may include items such as:
 - Accounting principles and industry-specific practices, including for industry-specific significant classes of transactions, account balances and related disclosures in the financial statements (for example, loans and investments for banks, or research and development for pharmaceuticals).
 - Revenue recognition.
 - Accounting for financial instruments, including related credit losses.
 - Foreign currency assets, liabilities and transactions.
 - Accounting for unusual or complex transactions including those in controversial or emerging areas (for example, accounting for cryptocurrency).
- An understanding of the entity's selection and application of accounting policies, including any changes to those policies as well as the reasons for the changes, may encompass such matters as:
 - The methods the entity uses to recognize, measure, present and disclose significant and unusual transactions.
 - The effect of significant accounting policies in controversial or emerging areas for which there is a lack of authoritative guidance or consensus.
 - Changes in the environment, such as changes in the applicable financial reporting framework or tax reforms that may necessitate a change in the entity's accounting policies.
 - Financial reporting standards and laws and regulations that are new to the entity and when and how the entity will adopt, or comply with, such requirements.

When we determine that any of the above matters are present, we seek more information that may help us understand whether these matters affect the identification and assessment of RMMs. This understanding can be particularly useful when we are assessing the likelihood and potential magnitude of misstatements that could occur.

How do we identify and assess RMMs related to omitted, incomplete or inaccurate disclosures? [ISA | 346.2000]

We obtain an understanding of the entity and the environment which helps us identify and assess RMMs related to omitted, incomplete or inaccurate disclosures.

To support our understanding, we may review prior-period disclosure checklists prepared by the entity (if it exists), as well as our own disclosure checklist.

Also keep in mind that disclosure requirements may change from the prior period because of changes in the entity or the applicable financial reporting framework. Therefore, we also consider any changes in the entity and the environment and those changes necessary to comply with the applicable financial reporting framework in the current period.

Our understanding of the entity can also help us recognize areas where disclosures may be subject to factors that increases the risk of a material misstatement, such as:

- new and/or complex disclosure requirements;
- subjectivity in relation to their preparation;
- whether they may use data that comes from outside of the general ledger and subsidiary ledgers;
- omissions or errors identified in prior periods.

Examples

What information might we gather that helps us understand the selection and application of accounting policies or principles? [ISA | 346.2200]

The table below sets out examples of information we may gather as we obtain our understanding of the entity's selection and application of accounting policies or principles.

Matter	Examples of information we may gather
Significant changes in the entity's accounting policies or principles, financial reporting policies or disclosures, and the reasons for such changes	<ul style="list-style-type: none"> • The entity may have completed a significant business combination and be applying business combination accounting policies or principles for the first time.
Financial reporting competencies of personnel involved in selecting and applying significant new or complex accounting policies or principles	<ul style="list-style-type: none"> • Business combinations may be uncommon for the entity, so the entity's accounting personnel may lack experience and expertise in selecting or applying business combination accounting policies or principles and disclosures, or performing necessary internal controls.
Accounts or disclosures requiring judgment in applying significant accounting policies or principles, especially in determining management's estimates and assumptions	<ul style="list-style-type: none"> • The entity may have recognized goodwill and intangible assets, which have complex accounting policies or principles for subsequent measurement. • The entity may have revenue streams with significant variable consideration that is difficult to identify or measure.
Effect of significant accounting policies or principles in controversial or emerging areas	<ul style="list-style-type: none"> • The entity may have adopted a new accounting standard, raising questions about applying the

lacking authoritative guidance or consensus	standard for which authoritative guidance or consensus is not yet available.
Methods used to account for significant unusual transactions	<ul style="list-style-type: none"> The entity may create a joint venture with an entity controlled by its CEO to conduct business activities that seem designed to keep the entity's liabilities off its balance sheet.
Financial reporting standards and laws and regulations that are new to the entity, including when and how the entity will adopt such requirements	<ul style="list-style-type: none"> An entity may have a high number of leases, and a comprehensive new lease accounting standard may require a significant change to the entity's financial statements, processes and internal controls.

6 Understand the entity's objectives, strategies and related business risks [ISA | 347]

What do we do?

Obtain an understanding of the entity's objectives, strategies and related business risks.

Why do we do this?

Industry, regulatory and other internal and external factors set the context for the entity's business. In response to these factors, the entity's management or those charged with governance define overall plans, or 'objectives', for the entity. 'Strategies' are the approaches that management plans to take to achieve these objectives. Strategies and objectives may change over time as internal and external forces evolve.

Even with the best intentions and well-reasoned decisions, objectives and strategies may not lead to the expected outcomes, resulting in business risks with financial consequences. Understanding the business risks facing the entity can help us identify risks of material misstatement (RMMs).

Execute the Audit

[What sources of information can help us understand the entity's objectives, strategies and related business risks? \[ISA | 347.1300\]](#)

We may have already obtained information relevant to understanding the entity's objectives, strategies and business risks when we performed other procedures to understand the entity and its environment, including its internal controls.

We can also obtain information to help us understand the entity's objectives, strategies and related business risks by:

- considering the [common sources of information](#) that we use to understand the entity and its environment; and
- reviewing the entity's enterprise risk assessment — i.e. its process to assess risks and opportunities related to achieving its objectives.

The risks identified through an enterprise risk assessment and discussed with those charged with governance (often in the form of a heat map) may result in risks of misstatement (RMs).

[What are business risks?](#) [ISA | 347.1400]

Business risks are risks that threaten an entity's ability to generate profits or to meet its goals. They generally comprise any factors that may contribute towards business failure — such as loss of customers, increase in production costs, decline in product demand, increase in market competition etc.

Business risks may arise from change or complexity, or from failing to see a need for change. For example, a business risk may arise from:

- developing new products or services that may fail;
- developing a market that may be inadequate to support a product or service;
- developing a flawed product or service that may lead to liabilities and reputational risk;
- new entrant to the market increases competition and lowers margins;
- new technology causes disruption and loss of market share; or
- changes in laws and regulations increase costs of doing business, making some business lines significantly less profitable.

[What is the difference between a business risk and an RMM?](#) [ISA | 347.1500]

Business risks can give rise to RMMs — especially financial statement-level RMMs, which may have a more pervasive impact.

However, not all business risks result in RMMs. In fact, some business risks may relate purely to the operations of the business and may not result in misstatement of the financial statements.

[Do we obtain an understanding of all the business risks facing the entity?](#) [ISA | 347.1600]

No. We are not responsible for identifying and assessing all business risks because not all business risks give rise to risks of material misstatement.

When we understand the entity's objectives and strategies, we consider whether there are related business risks that may give rise to a risk of material misstatement.

[How can business risks affect the financial statements?](#) [ISA | 347.1700]

Business risks can affect financial statements in a variety of ways. Their effects may be immediate or long-term, and impacts may arise at the financial statement level or assertion level. For example:

- the business risk from a shrinking customer base in a consolidating industry may raise an RM for valuations of accounts receivable and inventory that have become obsolete (immediate assertion-level RM); or
- the business risk of a decline in the entity's industry may affect the entity's ability to continue as a going concern (long-term financial statement-level RM)

Examples

In what situations might business risks lead to RMMs? [ISA | 347.1800]

The table below sets out examples of matters we may consider when obtaining an understanding of the entity's objectives, strategies and related business risks that may result in RMMs.

Situation	Examples of related business risk
Industry developments	The entity does not have the personnel or expertise to deal with a change in the industry.
New products and services	A newly introduced product or service may expose the entity to liability, and/or the new product or service may not succeed.
Changes in supply chain	Changes in the supply chain may impact the profitability of the entity's products. Disruptions in the supply chain may impact the entity's ability to fulfill customer orders.
Use of information technology (IT)	Some of the entity's systems and processes may be incompatible. New IT systems may not be implemented properly and/or migrated data may not be complete and accurate. There may be inconsistencies between the entity's IT strategy and its business strategies.
New accounting requirements	A new accounting requirement may not be implemented properly or completely, or the requirement may increase costs.
Expansion of the business	The demand for the entity's products or services may not have been accurately estimated.
Effects of implementing a strategy, particularly effects that lead to new accounting requirements	The strategy may not be implemented properly or completely.

Current and prospective financing requirements	The entity's inability to meet financing requirements may lead to a loss of financing.
Regulatory requirements	Regulatory requirements may increase the entity's legal exposure.

7 Understand the entity's measurement and analysis of its financial performance [ISA | 348]

What do we do?

Obtain an understanding of the entity's measurement and analysis of its financial performance.

Why do we do this?

Management and external stakeholders measure and review what they consider important. Performance measures, whether external or internal, create pressures for the entity. In turn, these pressures may prompt management action to improve business performance or misstate the financial statements.

Gathering information about how the entity, analysts, investors and rating agencies measure and analyze the entity's financial performance helps us understand financial statement line items that may pose greater risk of material misstatement. This understanding may help us identify accounts that may be open to manipulation, as well as accounts that the entity uses to monitor its operations.

Execute the Audit

How do we understand how the entity measures and analyzes its financial performance? [ISA | 348.1300]

We first identify the performance measures the entity considers most relevant and the measures the entity or external parties actively track.

We may have already identified some performance measures when understanding:

- [the relevant factors and metrics used to establish materiality for the financial statements](#); and
- [the nature of the entity](#).

Considering the [common sources of information](#) that we use to understand the entity and its environment may also reveal performance measures we have not already identified, or help us better understand how using performance measures we have identified may affect the identification and assessment of risks of material misstatement (RMMs).

In essence, we are searching the information produced by the entity, analysts, investors, rating agencies and others to identify the specific financial and other metrics they focus on in their reports.

Lastly, inquiries of management may reveal that it relies on certain key indicators, whether publicly available or not, for evaluating financial performance and taking action.

How can we use our understanding to identify and assess risks? [ISA | 348.1400]

Once we've identified the relevant performance measures, we may further seek to understand the following factors for each identified relevant performance measure:

- How aggressively are targets for each performance measure set by management?
- Does the entity have a history of achieving the set targets?
- How significantly is the management compensation linked to each performance measure?
- How are the performance measures defined?

The first three factors can help us gauge the importance of each performance measure to the entity and management, which may influence our assessment of risks of material misstatement connected to these performance measures.

Performance measures may also help us identify risks of misstatement. For example, understanding certain performance measures may indicate that the entity has unusually rapid growth or profitability when compared to that of other entities in the same industry. Such information, particularly if combined with other factors such as performance-based bonus or incentive remuneration, may indicate a potential risk of management bias in the preparation of the financial statements or possible fraud risk.

The last factor on understanding how the performance measure is defined, helps us identify specific accounts or disclosures that may create a greater risk of material misstatement from error or fraud. For example, when the entity and its investors and analysts use adjusted EBITDA as a relevant performance measure, we may obtain an understanding of how adjusted EBITDA is calculated and which accounts are included in the calculation.

Inspecting information about the entity's performance measures may also help us to identify items to focus on in our analytical reviews. We may identify unexpected results or trends that could indicate greater risk of material misstatement from error or fraud. For example, revenue growth that is unusually rapid compared to other entities in the same industry may indicate a potential risk of management bias in financial statement preparation — particularly when combined with other factors, such as performance-based bonus or incentive remuneration.

[Can an entity's performance measures include non-GAAP measures? \[ISA | 348.1500\]](#)

Yes. An entity's performance measures may and often do include both GAAP and non-GAAP measures. Commonly used non-GAAP performance measures include EBITDA and adjusted EBITDA, as well as net income, cash flow from operations, and other key financial ratios.

[How may our procedures to understand the entity's performance measures differ depending on its size or complexity? \[ISA | 348.7475\]](#)

Our procedures undertaken to understand the entity's performance measures may vary depending on the size or complexity of the entity, as well as the involvement of owners or those charged with governance in the management of the entity.

For some less complex entities, it may only be the terms of the entity's bank borrowings (i.e., bank covenants) that are linked to specific performance measures related to the entity's performance or financial position (e.g., a maximum working capital amount).

Whereas, for some entities whose nature and circumstances are more complex, such as those operating in the insurance or banking industries, performance or financial position may also be measured against regulatory requirements (e.g., regulatory ratio requirements such as capital adequacy and liquidity ratios performance hurdles).

Our understanding of these performance measures may help identify areas where there is increased susceptibility to the risk of material misstatement.

Examples

[What performance measures might an entity use? \[ISA | 348.1600\]](#)

The table below sets out examples of performance measures an entity may use that may be relevant to our risk assessment.

Where and how performance measures may be used	Examples of performance measures
As the basis for contractual commitments or incentive compensation arrangements	<ul style="list-style-type: none"> • Financial measures - e.g. revenue, net income, EBITDA • Period-on-period financial performance analyses • Industry-specific financial measures - e.g. Funds from Operations for real estate investment trusts, same-store sales for retailers • Non-financial measures - e.g. number of subscribers or users • Common ratios in loan agreements - e.g. debt-to-equity, interest coverage • Growth rates in financial and non-financial measures
By external parties - e.g. analysts, rating agencies - to review the entity's performance	
By the entity, to monitor its operations that may also highlight unexpected results and trends that management investigates and corrects, including correction of misstatements	<ul style="list-style-type: none"> • Ratios — e.g. accounts receivable and inventory turnover • Specific categories of operating expenses • Comparisons to budgets or forecasts • Segment or divisional operating results • Comparisons to competitors' operating results • Employee performance measures and incentive compensation policies

8 Understand and evaluate the Control Environment component [ISA | 1310]

What do we do?

Obtain an understanding of and evaluate the entity's control environment relevant to the preparation of the financial statements, including the policies and actions of management and those charged with governance concerning the entity's control environment.

Why do we do this?

We obtain an understanding of and evaluate the entity's control environment relevant to the preparation of the financial statements to support our identification and assessment of risks of material misstatement (RMMs).

Execute the Audit

[What is the Control Environment?](#) [ISA | 1310.1300]

An entity's Control Environment is the set of controls, processes and structures that provide the basis for carrying out internal control across the entity.

The Control Environment includes:

- the governance and management functions; and
- the attitudes, awareness and actions of those charged with governance and management concerning the entity's system of internal control and its importance to the entity.

The Control Environment sets the tone of an organization, influencing the control consciousness of its people and provides the overall foundation for the operation of the other components of the entity's system of internal control

[Does the Control Environment encompass all levels of an entity?](#) [ISA | 1310.11898]

Yes. The Control Environment underpins how ICFR is carried out across the organization and at all levels. So we may assess the Control Environment at levels below the parent or corporate level - e.g. regions, divisions, operating units and functional areas.

[Does the Control Environment encompass third-party service providers and business partners?](#) [ISA | 1310.11899]

Yes. The Control Environment also includes third-party service providers and business partners. Although the organization may rely on an outsourced service provider to conduct business processes, policies, and procedures on behalf of the entity, management retains ultimate responsibility for meeting the requirements for an effective system of internal control.

[Why is the Control Environment an important component of ICFR?](#) [ISA | 1310.1400]

If we consider the entity's internal control structure as like the structure of a house, the Control Environment is the foundation; thus it is the foundation for ICFR.



Process-level control activities directly affect financial reporting, but often affect only just one particular stream of transactions. In contrast, the Control Environment's effect on ICFR is indirect, yet it may have a pervasive effect on multiple business processes throughout the organization.

Not Integrated Audit | How do we obtain an understanding of the entity's Control Environment? [ISA | 1310.1800]

We obtain an understanding of the entity's Control Environment by:

- understanding, through inquiry, the set of controls, processes and structures that address the following elements/principles:
 - [how the entity demonstrates a commitment to integrity and ethical values](#)
 - [how the board of directors/those charged with governance demonstrates independence and oversight of internal control](#)
 - [structures, reporting lines, and authorities and responsibilities](#)
 - [how the entity demonstrates a commitment to attract, develop, and retain competent individuals](#)
 - [how the entity holds individuals accountable for their internal control responsibilities](#)
- [performing procedures to obtain an understanding of the CERAMIC components:](#)
 - begin by performing inquiries to obtain an understanding of each element/principle within the component.
 - consider whether certain factors apply to determine whether to perform more than inquiry
 - If at least one of the factors apply, design additional procedures to obtain an understanding (i.e. observation and/or inspection)
- Based on our understanding obtained, [evaluating the control environment component](#).

We also [consider how information is being used](#) in our procedures and [determine the appropriate audit procedures to evaluate the reliability of the information](#) used to obtain an understanding.

If we identify a control deficiency, we perform the following:

- evaluate the severity of the control deficiency and assess the impact on our audit; and
- evaluate whether the control deficiency is indicative of a fraud risk factor.
- evaluate whether control deficiencies undermine the other components of the entity's system of internal control.

What do we do if there are unaddressed elements after we obtain an understanding of CERAMIC? [ISA | 1310.8653]

When those charged with governance are not separate from management, it is appropriate for the following elements to be unaddressed:

- Element 2 - Those charged with governance demonstrates independence from management and exercises oversight of the development and performance of internal control.
- Element 11 - The entity communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control between management and those charged with governance.

In all other circumstances, if there are unaddressed elements after we have obtained an understanding of the CERAMIC component, we identify a control deficiency in the related CERAMIC component.

What are the five elements of the Control Environment component? [ISA | 1310.11926]

We obtain an understanding over the following five elements in order to evaluate the Control Environment component of ICFR.

Elements of the Control Environment component	<u>Element 1:</u> The organization demonstrates a commitment to integrity and ethical values. <u>Element 2:</u> When those charged with governance are separate from management, those charged with governance demonstrates independence from management and exercises oversight of the development and performance of internal control. <u>Element 3:</u> Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. <u>Element 4:</u> The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. <u>Element 5:</u>
---	---

The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

How may the Control Environment component for less complex entities be different? [ISA | 1310.2000]

Although the same principles / elements underlying the Control Environment component apply for both simpler and complex organizations; the entity's approach to address the CERAMIC component is likely to differ.

For example, a less complex entity may not have a written code of conduct, but instead, develops a culture that emphasizes the importance of integrity and ethical behavior through oral communication and by management example. Further, compared to a more complex entity, communication may be less structured and easier to achieve in a less complex entity since there may be fewer levels of responsibility and management may be more available and have greater visibility. As such, there is often more direct interaction between management and employees such that the organizational structure, reporting lines, and responsibilities are clear and evident.

A less complex entity's commitment to integrity and ethical values may appear in the variety of policies and procedures it employs or the attitudes, awareness and actions of those charged with governance and management.

Examples

9 Understand and evaluate the risk assessment process

What do we do?

Obtain an understanding of management's risk assessment process and evaluate whether the entity's risk assessment process is appropriate to the entity's circumstances considering the nature and complexity of the entity.

Why do we do this?

Our evaluation of the entity's risk assessment process may assist us in understanding where the entity has identified risks that may occur, and how the entity has responded to those risks. Our evaluation of how the entity identifies its business risks, and how it assesses and addresses those risks assists us in understanding whether the risks faced by the entity have been identified, assessed and addressed as appropriate for the nature and complexity of the entity.

If an entity does not have a risk assessment process that is appropriate for its nature and complexity, it may lead to unidentified / unaddressed risks relevant to its financial reporting objectives, ineffectively designed control activities and an increase in the possibility of a material misstatement in the financial statements.

Our understanding and evaluation of the entity's risk assessment process assists us with identifying and assessing financial statement level and assertion level risks of material misstatement.

Execute the Audit

Why is risk assessment an important component of ICFR? [ISA | 1317.1400]

Risk assessment is an essential component of ICFR because it forms the basis for how management identifies and analyzes risks relevant to its financial reporting objectives and how they determine the risks to be managed. If an entity does not have a risk assessment process that is appropriate for its nature and complexity, it may lead to unidentified / unaddressed risks relevant to its financial reporting objectives, ineffectively designed control activities and an increase in the possibility of a misstatement in the financial statements.

Using our house example, the risk assessment process is the blueprint or map of the house, and is needed to appropriately design the house.



Understanding the entity's risk assessment process, relevant to the preparation of the financial statements, gives us insight into whether the entity is appropriately identifying risks (and have a sound ICFR), which may affect our risk assessments. In addition, it also helps us plan and execute our audit and gives us insight into potential RMMs that we may not have considered.

When does an entity perform its risk assessment process? [ISA | 1317.1600]

An effective risk assessment process is iterative in nature. The four principles / elements within the Risk Assessment component are not always considered sequentially because there is considerable overlap among the principles / elements. Further, as an entity performs and monitors controls, management may identify items that require earlier risk determinations to be reassessed.

How do we obtain an understanding of the entity's risk assessment process? [ISA | 1317.1900]

We obtain an understanding of the entity's risk assessment process by:

- understanding, through inquiry, the processes that address the following elements/principles:
 - how the entity specifies objectives to identify and assess risks

- [how the entity identifies and analyses risks](#)
- [how the entity considers fraud when assessing risks](#)
- [how the entity identifies and assesses changes that impact internal control](#)
- [performing procedures to obtain an understanding of the CERAMIC components:](#)
 - begin by performing inquiries
 - consider whether certain factors apply to determine whether to perform more than inquiry
 - If at least one of the factors apply, design additional procedures to obtain an understanding (i.e. observation and/or inspection)
- based on the above, [evaluating the entity's risk assessment process](#).

We also [consider how information is being used](#) in our procedures and [determine the appropriate audit procedures to evaluate the reliability of the information](#) used to obtain an understanding.

If we identify a control deficiency in a CERAMIC component(s), [we evaluate the severity of the control deficiency and assess the impact on our evaluation](#).

What do we do if there are unaddressed elements after we obtain an understanding of CERAMIC? [ISA | 1317.8653]

When those charged with governance are not separate from management, it is appropriate for the following elements to be unaddressed:

- Element 2 - Those charged with governance demonstrates independence from management and exercises oversight of the development and performance of internal control.
- Element 11 - The entity communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control between management and those charged with governance.

In all other circumstances, if there are unaddressed elements after we have obtained an understanding of the CERAMIC component, we identify a control deficiency in the related CERAMIC component.

What are the four elements of the Risk Assessment component? [ISA | 1317.1800]

When management has an established risk assessment process, we consider the four elements outlined in the table below when obtaining an understanding of the Risk Assessment component of ICFR.

Elements of the Risk Assessment component	<p>Element 6: The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.</p> <p>Element 7: The organization identifies risks to the achievement of its objectives and analyzes risks as a basis for determining how the risks should be managed.</p> <p>Element 8:</p>
---	--

	<p>The organization considers the potential for fraud in assessing risks to the achievement of objectives.</p> <p><u>Element 9:</u></p> <p>The organization identifies and assesses changes that could significantly affect the system of internal control.</p>
--	---

Our understanding includes how the entity's risk assessment process identifies and addresses risks related to [accounting estimates](#).

[Why is it important for an entity to consider the potential for fraud?](#) [ISA | 1317.11847]

Every entity faces some risk of fraud from within, but the very nature of fraud makes it difficult to detect. It can also evolve and change over time, which makes fraud prevention or detection even more difficult.

At the same time, as shown by major corporate fraud scandals in nearly every decade of the past century, fraud can have a significant negative effect on an entity's financial reporting process, the reliability of its financial statements, and investor confidence.

[Principle / Element 8](#) highlights the importance of fraud risks to make it clear that an appropriate risk assessment process should specifically consider the vulnerability of the entity to fraudulent activity.

[Why is it important for an entity to monitor changes?](#) [ISA | 1317.11848]

Experience suggests that entities control routine business processes well. However, when something new or unusual happens, the system of ICFR is unable to process the new events or transactions in a controlled manner. This, in turn, may lead to material errors in the financial statements and deficiencies in internal control.

Identifying new transactions and events ahead of time through an entity's 'early warning systems' allows the entity time to make the necessary adjustments to the existing system of ICFR.

[Principle / Element 9](#) highlights the importance of considering whether changes result in additional risks, and whether the entity has designed and implemented control activities that appropriately mitigate those additional risks.

[How do the auditing standards map to the four elements of the Risk Assessment Process component?](#)

[ISA | 1317.11849]

The following table maps each of the processes that comprise the risk assessment process in the auditing standards to the related elements of the Risk Assessment Process component.

Process	Related Elements
Identifying business risks relevant to financial reporting objectives	<p><u>Element 6:</u></p> <p>The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.</p> <p><u>Element 7:</u></p>

	<p>The organization identifies risks to the achievement of its objectives and analyzes risks as a basis for determining how the risks should be managed.</p> <p><u>Element 8:</u></p> <p>The organization considers the potential for fraud in assessing risks to the achievement of objectives.</p> <p><u>Element 9:</u></p> <p>The organization identifies and assesses changes that could significantly impact the system of internal control.</p>
Estimating the significance of the risks and assessing the likelihood of their occurrence	<p><u>Element 7:</u></p> <p>The organization identifies risks to the achievement of its objectives and analyzes risks as a basis for determining how the risks should be managed.</p> <p><u>Element 8:</u></p> <p>The organization considers the potential for fraud in assessing risks to the achievement of objectives.</p> <p><u>Element 9:</u></p> <p>The organization identifies and assesses changes that could significantly impact the system of internal control.</p>
Deciding about actions to address those risks	<p><u>Element 7:</u></p> <p>The organization identifies risks to the achievement of its objectives and analyzes risks as a basis for determining how the risks should be managed.</p> <p><u>Element 8:</u></p> <p>The organization considers the potential for fraud in assessing risks to the achievement of objectives.</p> <p><u>Element 9:</u></p>

	The organization identifies and assesses changes that could significantly impact the system of internal control.
--	--

How may the Risk Assessment Process component for smaller, less complex entities be different? [ISA | 1317.2200]

In some less complex, smaller entities, and particularly owner-managed entities, an appropriate risk assessment may be performed through the direct involvement of management or the owner-manager (for example, the manager or owner-manager may routinely devote time to monitoring the activities of competitors and other developments in the market place to identify emerging business risks). The evidence of this risk assessment occurring in these types of entities is often not formally documented. However, discussions we have with management, corroborated by e-mails or other correspondence between management and other personnel, may provide evidence that management is, in fact, performing risk assessment procedures appropriate to the nature and complexity of the entity.

Examples

10 Understand and evaluate monitoring activities

| 1336]

What do we do?

Obtain an understanding of and evaluate the entity's monitoring activities.

Why do we do this?

Our understanding and evaluation of how the entity monitors the system of internal control relevant to the preparation of the financial statements assists us in understanding whether the other components of the entity's system of internal control are present and functioning, and therefore assists with understanding the other components of the entity's system of internal control. Our understanding and evaluation may also assist us with identifying and assessing financial statement level and assertion level risks of material misstatement.

Execute the Audit

What is a monitoring activity? [ISA | 1336.1300]

Monitoring activities help ascertain whether each of the components of internal control, including controls within each component, is present and functioning as intended.

Management's monitoring activities over internal controls involves assessing the effectiveness of internal control performance over time through ongoing activities, separate evaluations, or a combination of the two and taking necessary remedial actions.

Why are monitoring activities an important component of ICFR? [ISA | 1336.1400]

Using our house example, monitoring activities are similar to the roof of the house. They oversee and protect the other components.



Management's monitoring processes and controls continually check the other ICFR components to identify issues and determine what needs attention. Effective monitoring helps management identify necessary changes to the ICFR system to prevent or detect, on a timely basis, future errors in the financial statements.

The goal of monitoring is to determine both that the system of internal control operated and that it operated effectively.

Monitoring also includes evaluating the severity of identified deficiencies and communicating deficiencies to the appropriate parties.

Without effective monitoring, management do not have a basis to rely on their own ICFR.

[Not Integrated Audit | How do we obtain an understanding of the entity's monitoring activities?](#) [ISA |

1336.1700]

We obtain an understanding of the entity's process to monitor internal controls relevant to financial reporting by:

- understanding, through inquiry, the processes that address the following elements/principles:
 - [how the entity selects, develops, and performs monitoring activities](#)
 - [how the entity addresses internal control deficiencies](#)
- [performing procedures to obtain an understanding of the CERAMIC components:](#)
 - begin by performing inquiries
 - consider whether certain factors apply to determine whether to perform more than inquiry

- If at least one of the factors apply, design additional procedures to obtain an understanding (i.e. observation and/or inspection)
- based on our understanding obtained, evaluating whether the entity's process for monitoring the system of internal control is appropriate to the entity's circumstances, considering the nature and complexity of the entity.

We also consider how information is being used in our procedures and determine the appropriate audit procedures to evaluate the reliability of the information used to obtain an understanding.

In addition, if the entity has an internal audit function, we obtain an understanding of the internal audit function as part of understanding the entity's monitoring activities (refer to the activity '[Obtain an understanding of the IA function](#)').

If we identify a control deficiency in a CERAMIC component(s), we evaluate the severity of the control deficiency and assess the impact on our evaluation.

What do we do if there are unaddressed elements after we obtain an understanding of CERAMIC? [ISA | 1336.8653]

When those charged with governance are not separate from management, it is appropriate for the following elements to be unaddressed:

- Element 2 - Those charged with governance demonstrates independence from management and exercises oversight of the development and performance of internal control.
- Element 11 - The entity communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control between management and those charged with governance.

In all other circumstances, if there are unaddressed elements after we have obtained an understanding of the CERAMIC component, we identify a control deficiency in the related CERAMIC component.

What are the two elements of the Monitoring component? [ISA | 1336.1800]

We consider the two elements outlined in the table below when obtaining an understanding of the Monitoring component of ICFR.

Elements of the Monitoring Component	<u>Element 13:</u> The organization selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
	<u>Element 14:</u> The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action.

How may the Monitoring component for less complex entities be different? [ISA | 1336.1900]

Although the same principles / elements underlying the Monitoring component apply for both small and large organizations; the entity's process to address the CERAMIC component is likely to differ.

In less complex entities, the entity's process to monitor the system of internal control may be accomplished by management's close involvement in the entity's operations and accounting / financial reporting. In these circumstances, monitoring activities are likely to include more ongoing activities that are built into the normal recurring activities of an entity, as opposed to separate evaluations or formal testing of controls by Internal Audit or a similar function.

For example, management's close involvement in the entity's operations may involve regular and supervisory activities such as periodic reviews of the financial statement and related accounting information and/or a review of bank reconciliations, exception reports, or other information which has a role in monitoring the effectiveness of the underlying controls.

Through this close involvement, management may identify variances from expectations or inaccuracies in financial data, leading to the control being corrected. Further, management's actions and follow-up may also evidence how remedial actions are implemented.

Examples

11 Understand and evaluate information and communication [ISA | 1323]

What do we do?

Obtain an understanding of the information system relevant to financial reporting and how the entity communicates roles and responsibilities and significant matters relating to financial reporting and evaluate whether the entity's information system and communication appropriately support the preparation of the entity's financial statements in accordance with the applicable financial reporting framework.

Why do we do this?

We understand the entity's information system and communication because understanding the entity's policies that define the flows of transactions and other aspects of the entity's information processing activities relevant to the preparation of the financial statements, and evaluating whether the component appropriately supports the preparation of the entity's financial statements, supports our identification and assessment of risks of material misstatement at the assertion level.

This understanding and evaluation may also result in the identification of risks of material misstatement at the financial statement level when the results of our procedures are inconsistent with expectations about the entity's system of internal control that may have been set based on information obtained during the engagement acceptance or continuance process.

Execute the Audit

What is information and communication? [ISA | 1323.1300]

The scope of the Information and Communication component of ICFR is broad. It generally comprises people, business processes, activities, transactions, information/data elements and IT.

The information system may be located at the entity, its service organizations or both. It is used to generate relevant, quality information to execute the entity's business objectives - e.g. to produce and sell its products and services and measure its performance - and financial reporting objectives.

Communication, both internal and external, delivers the information the entity needs to carry out day-to-day controls. Communication also helps staff understand their internal control responsibilities and how they help achieve the entity's objectives.

Our understanding of information focuses on the aspects of an entity's information system relevant to financial reporting and ICFR. Even with that narrow focus, this often includes obtaining an understanding of how information flows from:

- the initiation and authorization of individual transactions;
- the occurrence of other events and conditions relevant to financial reporting; and
- how those transactions and other events and conditions are reported in the financial statements and related disclosures within the financial statements.

[How do we obtain an understanding of the Information and Communication component?](#) [ISA | 1323.1500]

We obtain an understanding of the information and communication component by:

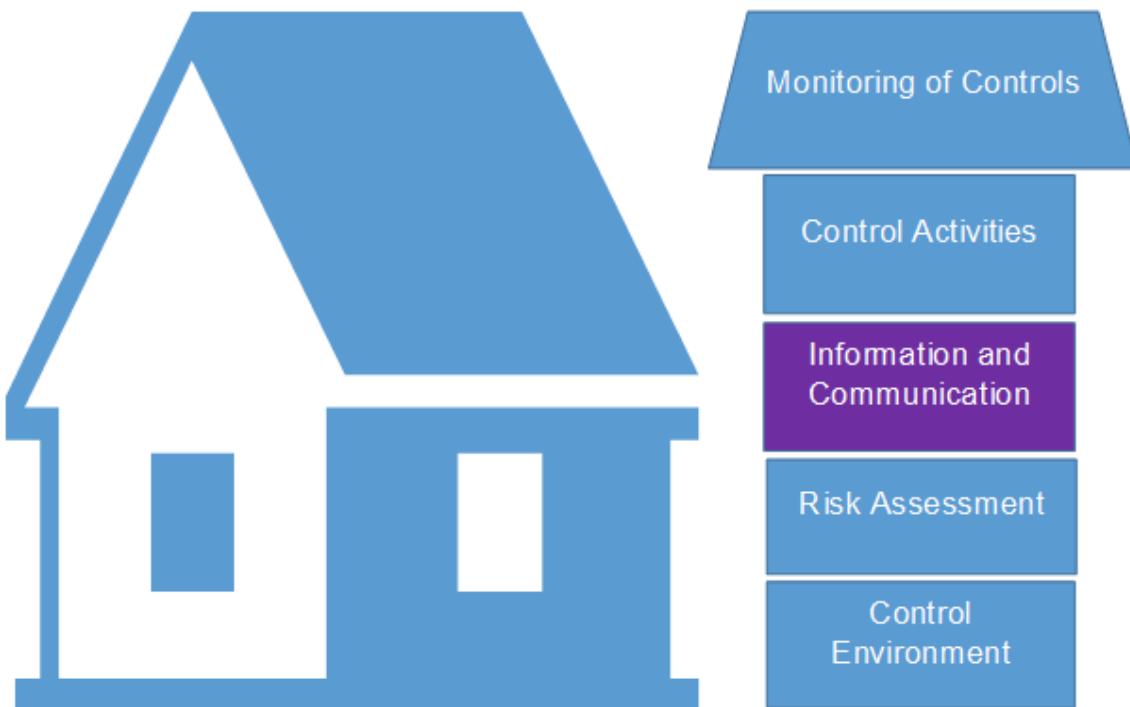
- [understanding and evaluating information](#); and
- [understanding and evaluating communication](#)

We also [consider how information is being used](#) in our procedures and [determine the appropriate audit procedures to evaluate the reliability of the information](#) used to obtain an understanding.

[Why is the Information and Communication component important to ICFR?](#) [ISA | 1323.1400]

An entity's ICFR uses information and communication to achieve its ICFR objectives across all of the ICFR components. If we recall our house example, information and communication are the walls and pipes of the house. Information and communication touch all of the components and act as a conduit for interaction between the components and throughout the entity.

The entity's ICFR could be ineffective if control operators don't receive complete, accurate, appropriate and timely information from both external and internal sources.



Because communication is so pervasive to the entity's overall ICFR, deficiencies can also have implications for our audit approach. For example, if an entity has written accounting policies but does not communicate them consistently across employees, individuals responsible for financial reporting may not appropriately account for transactions in accordance with the applicable financial reporting framework.

As auditors, if we are aware of this deficiency, it is likely to affect our risk assessment - especially as it relates to our identification of RMMs.

Similarly, if the entity does not have processes and controls in place to facilitate communication between its legal and accounting departments about a legal contingency, a higher risk of material misstatement might exist in this area. So, we may plan to respond to it.

Without obtaining an understanding of the entity's communication processes and controls, we may not have all the information we need to appropriately plan and execute our audit.

What are the three elements for the communications portion of the Information and Communications component? [ISA | 1323.1600]

We consider the three elements outlined in the table below when obtaining an understanding and evaluating the communications portion of the Information and Communication component of ICFR.

Elements for communication	<u>Element 10:</u> The organization communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control between people within the entity, including how financial reporting roles and responsibilities are communicated.
----------------------------	---

Element 11:

The organization communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control between management and those charged with governance.

Element 12:

The organization communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control to external parties, such as regulatory bodies.

Examples

12 Understand how the entity uses IT as part of financial reporting [ISA | 1325]

What do we do?

Obtain an understanding of how the entity uses IT and how IT affects the entity's flow of transactions and the financial statements by understanding the IT environment.

Why do we do this?

Understanding how the entity uses IT as part of financial reporting provides information that's useful when:

- determining whether the entity highly depends on IT processing,
- identifying and assessing risks of material misstatement (RMMs),
- obtaining an understanding of business processes, including process risk points (PRPs) and relevant automated process control activities,
- identifying the relevant IT layers, risks arising from IT (RAFITS) and relevant general IT controls (GITCs),
- identifying information we plan to use in the audit, and
- designing substantive audit procedures.

Execute the Audit

How do entities use IT systems? [ISA | 1325.1400]

Entities often use IT systems extensively within their information systems and in business processes to help them:

- manage and operate their business;
- maintain their financial records;
- and report financial results both internally and externally.

Entities may choose to automate certain processes using IT systems - including control activities to mitigate risks - to enhance efficiency and effectiveness. Automation may be particularly common when processing and reporting larger volumes of transactions, or when processing and aggregating information or data elements is not feasible without using IT systems.

A wide range of software may be part of an entity's financial reporting IT systems, including ERP systems that integrate multiple layers of technology. Common ERP software vendors include Microsoft, Oracle and SAP. In addition, many entities develop custom software to meet their specific needs or outsource IT services to service organizations, such as cloud computing (see question "[What additional considerations are there if the entity outsources cloud computing?](#)" and sub-questions for more information).

[How might service-organization-managed services affect business processes?](#) [ISA | 1325.10452]

Using service-organization-managed services may have a pervasive effect on the flow of an entity's transactions in one or many business processes. Some of these service organizations may not produce service auditor reports, which can make obtaining an understanding of the entity's information system challenging.

Using service organizations may also result in unique risks because the entity has given up control of some or all of its IT systems, while retaining responsibility for its information systems and ICFR.

In view of the wide variety of outsourced services offered and potential structures, understanding how the entity uses IT and its effect on the financial statements, and identifying and testing general IT controls, can be difficult. Using specific team members (STMs) with expertise in IT (IT Audit STMs) to help us obtain an understanding can be beneficial.

[Who do we involve in obtaining an understanding of an entity's use of IT?](#) [ISA | 1325.2100]

When obtaining an understanding of the entity's use of IT, we determine whether to involve specific team members (STMs) with expertise in IT (IT Audit STMs). See activity '[Involve specific team members with expertise in Tax and IT as appropriate](#)' for information on:

- when we involve IT Audit depending on the type of entity we are auditing,
- when we may involve IT Audit, and
- how we involve IT Audit in our audit, including what are some common areas where IT Audit is involved.

Even if we involve IT Audit, we remain responsible for obtaining an understanding of the entity's use of IT as part of financial reporting.

[How do we obtain an understanding of how the entity uses IT as part of financial reporting?](#) [ISA | 1325.2200]

Obtaining an understanding of how the entity uses IT as part of financial reporting involves obtaining an understanding of an entity's overall IT environment, which includes:

- [understanding the IT systems the entity uses as part of its financial reporting and business processes relevant to the preparation of the financial statements](#), including the various layers of technology that make up the IT system (applications, databases, operating systems and networks);
- [understanding the entity's IT processes to manage the IT environment](#);
- [understanding the entity's IT organization](#); and

- [understanding cybersecurity risks and incidents.](#)

Additionally, as part of obtaining an understanding of the entity's business processes and financial reporting process relevant to the preparation of the financial statements, we also obtain and/or confirm our understanding of how IT affects the entity's flow of transactions, accounting records and disclosures related to each process (see activity "[Understand business processes](#)" and sub-activities for further information).

[**How may the complexity of the entity's IT environment impact our understanding of the entity's use of IT?**](#)

[ISA | 1325.8676]

While the use of IT may be significant in entities with less complex IT environments, extensive descriptions of accounting and IT procedures, sophisticated accounting records, or written policies may not be available. Understanding the entity's IT environment may be easier and it may be more dependent on inquiry than on review of documentation.

When an entity has greater complexity in its IT environment, it is likely that we involve specific team members with expertise in IT in identifying the IT systems and other aspects of the IT environment, determining the related risks arising from IT, and identifying general IT controls. Such involvement is likely to be essential and may be more extensive for complex IT environments. Refer to the activity "[Involve specific team members with expertise in Tax and IT as appropriate](#)" for further information on when to involve IT Audit.

The extent of our understanding of the IT processes varies with the nature and the circumstances of the entity and its IT environment. The complexity of the IT environment may also impact the extent to which the entity has general IT controls in place, as well as the number of IT system layers that are subject to risks arising from IT.

[**What do we document when we obtain an understanding of how the entity uses IT as part of financial reporting?**](#) [ISA | 1325.10455]

We document:

- the key elements of our understanding,
- the risk assessment procedures performed, and
- the sources of information from which our understanding was obtained.

Examples

[**What procedures might we perform to obtain an understanding of how the entity uses IT as part of financial reporting?**](#) [ISA | 1325.3000]

Fact pattern:

When obtaining an understanding of how the entity uses IT as part of financial reporting, the engagement team decides to perform a combination of inquiry and inspection procedures.

Analysis

Example procedures that the engagement team may perform to obtain an understanding of the entity's IT systems IT processes and IT organization include:

- Inquiry of management (CIO/ IT director/ Head of IT/ IT manager) to obtain an understanding of matters such as:
 - the structure of IT governance;
 - an overview of the entity's IT infrastructure;
 - how IT is used to support financial reporting/ business processes that impact financial reporting;
 - relevant IT systems used for financial and business operations, including the various layers of technology that make up the IT system (applications, databases, operating systems and networks);
 - how systems interface/transfer data;
 - the extent of end-user computing in financial reporting;
 - recently implemented and new or upcoming IT projects;
 - significant upgrades or changes to relevant layers of technology;
 - management's assessment of significant IT risks;
 - the extent of reliance on centralized services, including shared service centers, and/or third-party service providers;
 - the use of any report writers, data warehouses, utility tools or ticketing tools in the processing of financial data or implementation/operation of automated controls;
 - the use of any Robotic Process Automation (RPA) and if used, its level of sophistication; and
 - the entity's IT processes to manage:
 - access to programs and data
 - program changes
 - program acquisition and development (e.g. Agile development or a more traditional approach)
 - computer operations.
- Inspection of documentation, when available, such as:
 - IT organization chart;
 - Description of IT processes to manage:
 - access to programs and data
 - program changes
 - program acquisition & development
 - computer operations;
 - Cybersecurity risk assessment;
 - IT governance / steering group meeting minutes;
 - service organization contract(s) relating to IT;
 - recent internal audit report(s) relating to IT ; and
 - evaluation report(s) (or other relevant documentation) describing the outcome of IT system(s) implemented or upgraded/ changed in the period.
- Inquiry of management (CEO/ COO/ CFO/ Head of Accounting) to obtain an understanding of matters such as:
 - the dependency of financial reporting/ business processes that impact financial reporting on the use of IT;

- the extent of end-user computing in financial reporting;
- recently completed and currently ongoing IT projects and known/ expected impact on the financial reporting process/ business operations;
- any recent or ongoing IT issues that impact the financial reporting process/ business operations; and
- any envisioned changes to IT that impact business processes and financial reporting.

What matters might we consider when obtaining an understanding of a less complex IT environment? [ISA | 1325.8677]

Fact pattern:

An entity's use of IT as part of financial reporting consists of a single commercial accounting software.

Analysis

Obtaining an understanding of an entity's use of IT may be more easily accomplished in a less complex IT environment that uses an "off-the-shelf" single commercial accounting software (e.g. QuickBooks). Matters that the engagement team may consider in understanding the nature of a single commercial accounting software may include:

- The nature and extent of modifications that have been made to the software (e.g., setting or amending reporting parameters);
- The extent to which it is possible for the entity to modify the source code of the software to include additional modules (i.e., add-ons) to the base software, or to make direct changes to data;
- The extent to which data related to the preparation of the financial statements can be directly accessed (i.e., direct access to the database without using the IT application) and the volume of data that is processed; and
- The extent to which the software is well established and has a reputation for reliability.

13 Evaluate the design and implementation of relevant process control activities

[ISA | 1343]

What do we do?

Evaluate the design and implementation of relevant process control activities

Why do we do this?

As part of obtaining an understanding of internal control over financial reporting (ICFR), we:

- evaluate the design of process control activities that are relevant to the audit; and
- determine whether they have been implemented.

We use the understanding obtained to identify and assess RMMs and consider our planned response to identified risks.

Execute the Audit

Where are we in identifying and understanding relevant process control activities? [ISA | 1343.1300]

We are in step 4 of identifying and obtaining an understanding of relevant process control activities.

- (1) Obtain an understanding of the process that is sufficient to assess the factors that affect the risks of material misstatement and to design further audit procedures.
- (2) Identify process risk points
- (3) Determine which controls are relevant to the audit.
- (4) **Evaluate the design and implementation of relevant process control activities.**

Which control activities do we understand and are relevant to the audit? [ISA | 1343.1600]

We obtain an understanding of control activities that are 'relevant to the audit'. 'Control activities relevant to the audit' or 'relevant control activities' have a specific meaning in our methodology. This terminology identifies control activities that we understand and, thus, perform procedures to evaluate their design and implementation. The following are control activities relevant to the audit:

- process control activities that address RMMs:
 - where we plan to take a controls reliance approach;
 - that are significant risks;
 - that are associated with SUTs (refer to activity '[Identify SUTs](#)') or related parties (refer to activity '[Obtain an understanding of related party processes and controls](#)'); or
 - that are associated with journal entries and other adjustments (refer to activity '[Evaluate the design and implementation of control activities over journal entries and other adjustments](#)'); or
 - where we cannot obtain sufficient evidence through substantive testing alone; or
- process control activities:
 - that we are testing over the accuracy and completeness of internal information and the RDE(s) to evaluate the reliability of such information (see activity '[Test management's controls over the accuracy and completeness of internal information](#)'); or
 - that, in our professional judgment, we consider it appropriate to understand in order to enable us to effectively identify and assess the risk of material misstatement and design further audit procedures; and
- general IT controls that address 'relevant RAFITs' associated with 'relevant automated controls' or data integrity risks (refer to question '[Under what circumstances do we obtain an understanding of general IT controls](#)').

What is an example of the differences and relationship between process activities and control activities?

[ISA | 1343.11410]

Consider the following example — the credit limit illustrates the differences and relationship between process activities and control activities.

Process activities	Customers place their purchase orders electronically. These orders are captured in the entity's enterprise resource planning (ERP) system and processed for fulfilment.
--------------------	---

Identified risk	Customers could exceed their established credit limit.
Control activities to address the identified risk	<p>The entity's ERP system compares the open receivables from the customer plus the submitted purchase order amount to the established customer credit limit.</p> <p>If the total amount of open receivables and purchase orders exceeds the credit limit, the purchase order is not processed further. Each purchase order not processed is followed-up manually.</p>

Why do we evaluate the design and implementation of process control activities? [ISA | 1343.1800]

We evaluate the design and implementation of process control activities as a part of our risk assessment activities to provide an appropriate basis for the identification, assessment of and response to risks of material misstatement.

Even though our identification and assessment of RMMs is based on inherent risk, evaluating the design and implementation of process control activities provides a contextual understanding that may be helpful when we identify and assess risks, including:

- the PRPs (the 'where' and the 'how' a misstatement could occur); and
- the control activities management have designed and implemented to mitigate them.

How do we evaluate the design of a process control activity? [ISA | 1343.12135]

Evaluating the *design* of a process control activity involves considering whether the control is capable of effectively preventing, or detecting and correcting material misstatements, either individually or in combination with other controls.

Determining whether a control has been designed effectively means determining if the control activity:

- satisfies the company's control objectives by addressing the PRPs it is intended to address, and
- operates at a level of precision that 'would' prevent or detect and correct a material misstatement.

We evaluate design through inquiry, *in combination with* observation and/or inspection.

How do we evaluate the implementation of a process control activity? [ISA | 1343.12136]

The *implementation* of a process control activity means that the control exists and that the entity is using it.

We evaluate implementation through inquiry, *in combination with* observation and/or inspection.

Determining whether a control has been implemented means determining whether the control exists and whether the entity is using it.

What do we consider when we evaluate the design and implementation of a process control activity? [ISA | 1343.12138]

The table below sets out the items we consider when we evaluate the design and implementation of a process control activity.

We specifically understand the criteria / threshold for investigation used to identify outliers and for each attribute, whether the control operator uses judgment.

What do we understand about a control?	Description
<u>Control objective</u>	The risk the control is intended to mitigate - i.e., the relevant PRPs the control addresses.
<u>Anti-fraud control</u>	Controls designed to detect, prevent or deter fraud.
<u>Nature and type of control</u>	'Nature' refers to whether the control is manual or automated. 'Type' refers to whether the control is preventive or detective.
<u>Frequency</u>	Frequency with which the manual control activity is performed: <ul style="list-style-type: none"> • annually • quarterly • monthly • weekly • daily • recurring • ad hoc
<u>Authority and competence of the control operator</u>	The level of competence and authority necessary to operate a manual control. Understanding who typically operates the control and why they do so may be useful, so that we can define what level of competence and authority is necessary.
<u>Judgment involved</u>	Subjectivity in determining whether something is an outlier and/or whether an outlier is correct/ reasonable.
<u>Level of precision</u>	The level of precision, including the criteria/threshold for investigation used to identify outliers.
<u>Investigation and resolution process</u>	If the control activity involves judgment, evaluating the steps performed by the control operator to investigate and resolve outliers.

<u>Information relied on in the performance of the control activity</u>	Information used when performing the control (e.g., system reports, manually prepared spreadsheets, data), including the relevant data elements.
Documentation maintained	A description of the documentation maintained to evidence the performance of the control activity

[What is a control operator?](#) [ISA | 1343.8445]

The control operator is a term used to describe who or what performs the control. In a manual control, the control operator is the individual who performs the control. In an automated control, the control operator is the IT system.

[What if a control activity is ineffective in its design and/or implementation?](#) [ISA | 1343.2200]

If we determine that a control activity is ineffective in its design and/or implementation (refer to activity '[Determine whether a deficiency in ICFR exists and describe it](#)'), we:

- conclude that there is a deficiency;
- do not plan to rely on or test the operating effectiveness; and
- consider the effect of that deficiency on the procedures we plan to perform as part of our response to an RMM and modify them accordingly.

[What are example process control activities related to cash and cash equivalents?](#) [ISA | 1343.8446]

Process control activities related to cash and cash equivalents may include process control activities over the segregation of duties required, such as for:

- Opening and closing bank accounts; and
- Ability to access cash (authorized signers).

Additional relevant business process control activities related to cash and cash equivalents may include process control activities over accurate classification of cash and cash equivalents.

14 Evaluate the design and implementation of process control activities over journal entries and other adjustments [ISA | 798]

What do we do?

Evaluate the design and implementation of the entity's process control activities over journal entries and other adjustments.

Why do we do this?

We identify and evaluate the design and implementation of process control activities over journal entries with a double objective:

- as part of our procedures to address the risk of management override of controls through the recording of journal entries, and
- as part of our risk assessment procedures, to address any risk identified that journal entries are susceptible of unauthorized or inappropriate intervention or manipulation due to error.

Execute the Audit

What are journal entries? [ISA | 798.1300]

Journal entries are any entries made directly within the general ledger system that are used to record transactions, allocations, adjustments and corrections. They include:

- standard journal entries used to record recurring transactions and adjustments; and
- non-standard journal entries used to record non-recurring, unusual transactions, or adjustments.

What are standard journal entries? [ISA | 798.13373]

Standard journal entries are journal entries used to record:

- recurring transactions - e.g., the day to day activities of the entity such as recurring sales, purchases, and cash disbursements; and
- recurring adjustments - e.g., adjustments related to accounting estimates that are made at each period-end such as changes in the estimate of uncollectible accounts receivable.

What are automated journal entries? [ISA | 798.13374]

Automated journal entries are standard journal entries that are automatically initiated, authorized, recorded and processed in the general ledger. The use of automated journal entries can reduce the risk of management override of controls because automated journal entries are less likely to be susceptible to unauthorized or inappropriate intervention or manipulation.

What are non-standard journal entries? [ISA | 798.13375]

Non-standard journal entries are journal entries used to record:

- non-recurring or unusual transactions - e.g., business combinations or disposals; and
- non-recurring adjustments - e.g., adjustments related to accounting estimates that are typically not made at each period-end such as the impairment of an asset.

The process and procedures used to record non-standard journal entries are typically manual journal entries.

What are manual journal entries? [ISA | 798.13376]

Manual journal entries are journal entries that are initiated by an individual and manually entered into the general ledger system. The use of manual journal entries can increase the risk of management override of controls because manual journal entries are more likely to be susceptible to unauthorized or inappropriate intervention or manipulation.

What are other adjustments? [ISA | 798.13378]

Other adjustments are adjustments made to the general ledger accounts outside of the general ledger system to determine the amounts presented on the face of the financial statements. Entities often use a spreadsheet to support other adjustments. Other times, entities may make other adjustments

directly in the financial statements or disclosures themselves. Other adjustments are most often seen in period-end financial reporting through post-closing adjustments.

Similar to manual journal entries, the use of other adjustments can increase the risk of management override of controls because there is more opportunity for manual intervention in the process and procedures.

How do we evaluate the design and implementation of process control activities over journal entries and other adjustments? [\[ISA | 798.1301\]](#)

We evaluate the design and implementation of process control activities over journal entries and other adjustments through inquiry in combination with observation and/or inspection, in the same way we evaluate the design and implementation of other relevant process control activities (refer to activity '[Evaluate the design and implementation of relevant process control activities](#)' for more information).

In what circumstances do we evaluate the design and implementation of process control activities over journal entries and other adjustments? [\[ISA | 798.157909\]](#)

We identify and evaluate the design and implementation of process control activities over journal entries and other adjustments that are relied on by management that sufficiently address:

- the risk of management override of controls; and, if identified,
- the risk that journal entries are susceptible to unauthorized or inappropriate intervention or manipulation due to error.

How do we address the risk that journal entries are susceptible to unauthorized or inappropriate intervention or manipulation due to fraud? [\[ISA | 798.157910\]](#)

The risk that journal entries are susceptible to unauthorized or inappropriate intervention or manipulation due to fraud is addressed as part of our response to the risk of management override of controls.

What is the difference between the risk of management override of controls through journal entries and the risk of unauthorized or inappropriate intervention or manipulation of journal entries and how we address these risks? [\[ISA | 798.157911\]](#)

The difference between the risk of management override of controls through journal entries and the risk of unauthorized or inappropriate intervention or manipulation of journal entries and how we address these risks is shown in the table below:

Risk	Characteristics	Risk addressed by
Management override of controls through journal entries	Fraud risk (i.e., significant risk) present in all entities, although the level of risk may vary from entity to entity	Testing the appropriateness of journal entries and other adjustments, which includes evaluating the design and implementation of process control activities over journal entries and other adjustments

Unauthorized or inappropriate intervention or manipulation of journal entries	<p>Presumed to be a fraud risk since the unauthorized or inappropriate intervention or manipulation of journal entries will derive from an intentional act in most cases.</p> <p>However, in certain cases, we may determine that the risk also derives from an unintentional act and therefore be considered a risk due to error.</p>	<p>Addressing the fraud risk as part of our response to the risk of management override of controls.</p> <p>If we determine there is also a risk due to error, we:</p> <ul style="list-style-type: none"> • determine whether there is a risk of material misstatement at the assertion level and, if there is, we • identify and evaluate the design and implementation of process control activities over journal entries that address the risk due to error. <p>We also take this into account in our substantive procedures to select and test high-risk journal entries that address both the risk of management override of controls and the risk that journal entries are susceptible to unauthorized or inappropriate intervention or manipulation due to error, for example, we may consider unusual account combinations when determining the high-risk criteria.</p>
---	--	---

What journal entries may be susceptible to unauthorized or inappropriate intervention or manipulation?

[ISA | 798.157922]

These journal entries include:

- non-standard journal entries, where the journal entries are automated or manual and are used to record non-recurring, unusual transactions or adjustments;
- standard journal entries, where the journal entries are automated or manual and are susceptible to unauthorized or inappropriate intervention or manipulation.

Due to their nature, non-standard journal entries are typically manual journal entries and, therefore, more likely to be susceptible to unauthorized or inappropriate intervention or manipulation.

Standard journal entries can be used to record:

- recurring transactions (e.g., daily routine sales)

In this case, in today's environment where there are significant automated processes, these standard journal entries are typically automated journal entries and therefore less likely to be susceptible to unauthorized or inappropriate intervention or manipulation.

In particular, for system-generated journal entries that are directly and routinely processed to the general ledger, we may judgmentally determine that there is little or no susceptibility to unauthorized or inappropriate intervention or manipulation and therefore would not give rise to a risk of material misstatement and we would not identify controls over those journal entries to evaluate their D&I.

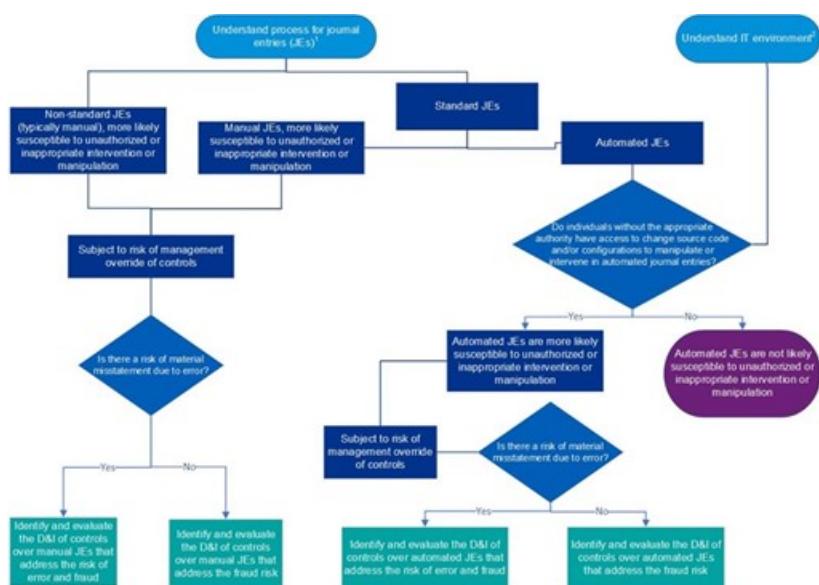
However, there could be other scenarios where a journal entry, although automated, could be manipulated. For example, if individuals without the appropriate authority have access to the source code or are able to make inappropriate changes to configurations.

See questions "[What is an example scenario that indicates likely susceptibility versus little to no susceptibility to unauthorized or inappropriate intervention or manipulation of automated journal entries?](#)" and "[What do we do when it is not clear whether automated journal entries are susceptible to unauthorized or inappropriate intervention or manipulation?](#)" for more information on automated journal entries that could be susceptible to unauthorized or inappropriate intervention or manipulation.

- recurring adjustments (e.g., adjustments related to accounting estimates that are made at each period-end such as changes in the estimate of uncollectible accounts receivable).

In this case, these standard journal entries are more likely to be manual journal entries and therefore more likely to be susceptible to unauthorized or inappropriate intervention or manipulation

The following diagram depicts the process we follow to determine the journal entries that could be susceptible to unauthorized or inappropriate intervention or manipulation and how we address any related risk of material misstatement identified:



¹ This includes understanding the types of journal entries, i.e. standard and non-standard, manual and automated. See activity "Understand processes and procedures for journal entries and other adjustments" [797] for further guidance.

² This includes understanding the IT process to manage changes. See activity "Understand IT processes" [7842] for further guidance.

For guidance on the decisions to be made regarding what controls over journal entries to identify when we do not plan to test their operating effectiveness, refer to the decision tree in the question "[How do we identify process control activities over journal entries and other adjustments over which to evaluate their design and implementation?](#)".

[What is an example scenario that indicates likely susceptibility versus little to no susceptibility to unauthorized or inappropriate intervention or manipulation of automated journal entries?](#) [ISA | 798.157942]

The table below shows an example scenario that indicates likely susceptibility versus little to no susceptibility to unauthorized or inappropriate intervention or manipulation of automated journal entries:

Factor	Likely susceptibility	Little to no susceptibility
Type of general ledger IT system	Entity uses a custom in-house built system or a highly customized ERP system.	Entity uses a standard off the shelf general ledger IT system.
Access to source code/system configuration	Individuals within the entity without the appropriate authority have access to the general ledger IT system's source code.	Individuals within the entity do not have access to the general ledger IT system source code and the entity does not have the ability to change system configurations related to how journal entries are posted to general ledger IT system (i.e., access to configurations or source code to change how journal entry general ledger accounts, dates, amounts, journal entry type are recorded in the general ledger).

When there is likely susceptibility to unauthorized or inappropriate intervention or manipulation of automated journal entries, we identify and evaluate the design and implementation of process control activities over those automated journal entries. If the process control activities are automated, we also identify the relevant layers of technology, RAFITs and GITCs, and evaluate the D&I of GITCs that support the continued effective operation of those automated process control activities.

What do we do when it is not clear whether automated journal entries are susceptible to unauthorized or inappropriate intervention or manipulation? [ISA | 798.157943]

When it's not clear whether automated journal entries are susceptible to unauthorized or inappropriate intervention or manipulation, we take into account our understanding of the IT environment and business processes. We also think about the following questions to help us determine if automated journal entries are susceptible to unauthorized or inappropriate intervention or manipulation and therefore whether to identify and evaluate the design and implementation of process control activities over automated journal entries as well as relevant GITCs, if the process control activities identified are automated.

1. Does management have access to the general ledger IT system's source code? If yes:

- Who has access?

- Is access restricted to authorized personnel (e.g., only IT personnel have access and there is segregation of duties between IT and accounting)?
- Can the entity provide evidence of who has access to the source code?
- If those in the accounting department have access to the general ledger IT system source code, what are the controls in place to detect unauthorized changes to source code impacting journal entries?

2. Are there any system configurations that impact how journal entries are posted (i.e., how journal entry general ledger accounts, dates, amounts, journal entry type are recorded in the general ledger)? If yes:

- What are the configurations related to journal entries?
- Who has access to change the system configurations?
- Is access restricted to authorized personnel (e.g., only IT personnel have access and there is segregation of duties between IT and accounting)?
- Can the entity provide evidence of who has access to the system configurations?
- What controls over system configurations related to journal entries are in place?

For examples as to how these questions we think about would impact our audit approach, refer to the question "[How might an entity's responses to the questions we think about to identify when automated journal entries may be susceptible to unauthorized or inappropriate intervention or manipulation, impact our audit approach?](#)".

[How do we identify process control activities over journal entries and other adjustments over which to evaluate their design and implementation? \[ISA | 798.9409\]](#)

When understanding the entity's financial reporting process, we use the knowledge obtained to identify, at a minimum, process risk points (PRPs) where management override of controls could occur through the recording of journal entries and other adjustments. Additionally, we consider whether there are any additional PRPs related to the risk associated with journal entries that could be susceptible to unauthorized or inappropriate intervention or manipulation.

When understanding the entity's business processes, we specifically understand how the transactions are initiated, and how information about them is recorded, processed, corrected as necessary, incorporated in the general ledger and reported in the financial statements. In obtaining this understanding, we obtain knowledge about how transactions and events are processed, and therefore we may identify journal entries that could be susceptible to unauthorized or inappropriate intervention or manipulation and PRPs related to those journal entries. Additionally, when we take a controls-based approach to respond to RMMs related to the recording of transactions and events in the business process, we may identify PRPs related to the recording of those transactions in the general ledger through journal entries.

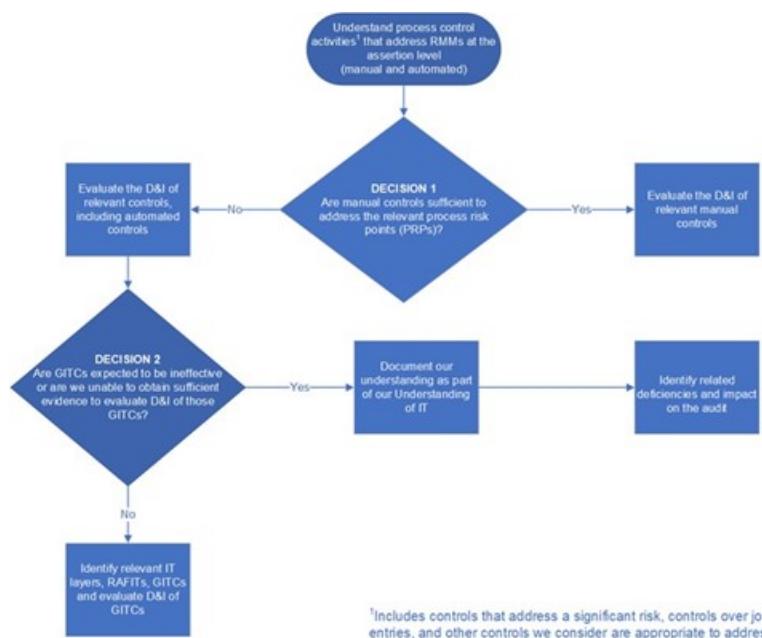
For each PRP identified, we obtain an understanding of the process control activities that are relied on by management to address the PRP.

Most entities maintain their general ledger in an application and posting of journal entries is at least in part performed automatically, so it is likely that control activities over journal entries will include automated controls over the posting of journal entries to the general ledger. However, that does not mean we identify those automated controls as process control activities over journal entries that we will evaluate design and implementation of to address the risk of management override of controls

and/or to address the risk associated with journal entries that could be susceptible to unauthorized or inappropriate intervention or manipulation. For example, entity management may implement manual controls over the automated posting of journal entries or a review process over manual journal entries such that they do not rely on the automated processing of journal entries to address the risk of management override of controls and/or to address the risk associated with journal entries that could be susceptible to unauthorized or inappropriate intervention or manipulation due to error.

In cases where management relies on automated controls to address the risk of management override of controls through journal entries or the risk associated with journal entries that could be susceptible to unauthorized or inappropriate intervention or manipulation, we evaluate the design and implementation of those automated controls, we also identify relevant IT layers, RAFITs and evaluate the design and implementation of general IT controls that support the continued effective operation of those automated controls.

The following decision tree provides an illustration of the decisions to be made and the implications when we evaluate the design and implementation of process control activities but we do not plan to test their operating effectiveness, including controls over journal entries and other adjustments (see question "[Under what circumstances do we evaluate the design and implementation of GITCs](#)" for more information on decision 2 of the decision tree below):



[What are some examples of process control activities over journal entries and other adjustments?](#) [ISA | 798.13524]

Examples of process control activities that may reduce the risk of management override of controls or the risk that journal entries are susceptible to unauthorized or inappropriate intervention or manipulation are:

- the CFO or CEO are prevented from initiating, processing or authorizing journal entries within the IT system;
- objective oversight by personnel independent from the journal entry process reviewing journal entries and supporting documentation;

- all journal entries and supporting documentation are reviewed and approved by an individual separate from the individual posting the journal entry;
- a control exists that prevents the reviewer of a journal entry from posting it.
- accounting manager that neither prepares, reviews nor posts journal entries reviews all manual journal entries posted during the period to the general ledger. If a threshold is applied to this review, the magnitude of those entries not subject to review does not have a risk of material misstatement.
- reconciliation of balance sheet and income statement accounts by an accounting manager that neither prepares, reviews nor posts journal entries by comparing two or more data elements and investigates reconciling items at an appropriate level of precision;
- automated process control activities over journal entries that limit privileged user access to the system to one or two senior IT staff. Only staff with privileged access have the ability to change automated journal entries based on the design of the IT systems or no staff have the ability to change automated journal entries;
- automated control activities that prevent changes in relevant information after a journal entry has been posted, such as preventing management from changing the identity of the person posting a journal entry.

The last two bullets are examples of effective control activities that could suggest that automated journal entries are not a characteristic of high risk journal entries.

[Core and Less Complex | What is an additional example of process control activities over journal entries and other adjustments in a less-complex entity? \[ISA | 798.8909\]](#)

An additional example of process control activities that may reduce the risk of management override of controls or the risk that journal entries are susceptible to unauthorized or inappropriate intervention or manipulation in a less-complex entity is:

- Where senior management are closely involved in the day to day operations, senior management review of financial information on a periodic basis to assess if it is in line with expectations, may be relied on and precise enough to identify material misstatements caused by incorrect journal entries.

[Do we evaluate the design and implementation of controls over journal entries and other adjustments for all audit engagements? \[ISA | 798.13525\]](#)

Yes, for all audit engagements we evaluate the design and implementation of process control activities over journal entries and other adjustments that sufficiently address the risk of management override of controls through the recording of journal entries and other adjustments, which is a fraud risk and thus, a significant risk. Therefore, we evaluate the design and implementation of an entity's process control activities over journal entries and other adjustments as part of our audit that respond to that risk even when we have not identified other controls relevant to our audit.

Additionally, we may identify process control activities that address the risk associated with journal entries that are susceptible to unauthorized or inappropriate intervention or manipulation.

For example, in an audit of a less complex entity, the entity's information system may not be complex and we may not plan to rely on the operating effectiveness of controls. Further, we may not have identified any significant risks or any other risks of material misstatement for which it is necessary for us to evaluate the design and implementation of controls. In such an audit, we may only evaluate the

design and implementation of control activities over journal entries and other adjustments that address the risk of management override of controls and, when relevant, the risk that journal entries could be susceptible to unauthorized or inappropriate intervention or manipulation due to error.

At what point in the audit do we evaluate the design and implementation of process control activities over journal entries and other adjustments? [ISA | 798.1700]

We evaluate the design and implementation of the entity's process control activities over journal entries and other adjustments as part of our risk assessment procedures - i.e., as part of the planning phase of the audit.

Do we test the operating effectiveness of process control activities over journal entries and other adjustments when we perform a financial statement audit? [ISA | 798.1800]

Not necessarily. We test the operating effectiveness of process control activities over journal entries and other adjustments when we plan to rely on the operating effectiveness of those controls as part of our response to a particular risk of material misstatement, including our approach to identifying and testing high risk journal entries

We may plan to rely on the operating effectiveness of process control activities over journal entries and other adjustments in order to reduce the extent of our testing of journal entries and other adjustments (e.g., when excluding automated journal entries from the population of journal entries that we apply high risk criteria to).

Examples

How might an entity's responses to the questions we think about to identify when automated journal entries may be susceptible to unauthorized or inappropriate intervention or manipulation, impact our audit approach? [ISA | 798.157925]

Fact pattern 1

Consider an entity that responds as follows:

Question	Example response
Is the general ledger IT system a custom in-house built system or a highly customized purchased general ledger IT system?	No. The general ledger IT system is a standard off the shelf system
Does management have access to the general ledger IT system's source code?	No. The entity uses an off-the-shelf accounting software. Source code is compiled, and management does not have access to it.
Are there any system configurations (i.e., access to configurations or source code to change how journal entry general ledger	No.

accounts, dates, amounts, journal entry type are recorded in the general ledger) that impact how journal entries are posted?

Analysis

Given:

- The entity uses a standard off the shelf general ledger IT system;
- Management does not have access to the source code, and
- There are no system configurations (i.e., access to configurations or source code to change how journal entry general ledger accounts, dates, amounts, journal entry type are recorded in the general ledger) that impact how the journal entries are posted,

the engagement team determines that automated journal entries are not likely susceptible to unauthorized or inappropriate intervention or manipulation and therefore the engagement team does not identify or evaluate the design and implementation of process control activities over automated journal entries.

Fact pattern 2

Consider an entity that responds as follows:

Question	Example response
Is the general ledger IT system a custom in-house built system or a highly customized purchased general ledger IT system?	Yes. The general ledger IT system is a custom in-house built system.
Does management have access to the general ledger IT system's source code?	Yes. IT management has access to the source code.
Is access restricted to authorized personnel (e.g., only IT personnel have access and there is segregation of duties between IT and accounting)?	Yes. Only personnel in the IT department with the appropriate authority in accordance with the entity's policies has access to the source code.
If those in the accounting department have access to the general ledger IT system, are there controls in place to detect unauthorized changes to source code impacting journal entries? If yes, describe the controls	N/A. The accounting department does not have access to the source code
Are there any system configurations (i.e., access to configurations or source code to change how journal entry general ledger	Yes. The system allows the ability to override how journal entry general ledger accounts and

accounts, dates, amounts, journal entry type are recorded in the general ledger) that impact how journal entries are posted?	journal entry type are recorded in the general ledger.
Who has access to change the system configurations?	Only personnel in the IT department with the appropriate authority in accordance with the entity's policies has access to change the system configurations.
Can the entity provide evidence of who has access to source code and system configurations?	Yes. Management provided a system generated report of users that have access to update source code and system configurations of the general ledger IT system. The engagement team confirmed the controller does not have access to modify source code or system configurations of the general ledger IT system.

Analysis

Given:

- The entity uses a custom in-house built general ledger IT system,
- Only personnel in the IT department with the appropriate authority in accordance with the entity's policies has access to the source code,
- Although the system allows the ability to override how journal entry general ledger accounts and journal entry type are recorded in the general ledger, only personnel in the IT department with the appropriate authority in accordance with the entity's policies has access to change the system configurations, and
- The engagement team obtained and inspected a system-generated report confirming that the controller did not have access to modify source code, system configurations, or journal entries,

the engagement team determines that automated journal entries are not likely susceptible to unauthorized or inappropriate intervention or manipulation and therefore the engagement team does not identify or evaluate the design and implementation of process control activities over automated journal entries.

Fact pattern 3

Consider an entity that responds as follows:

Question	Example response
Is the general ledger IT system a custom in-house built system or a highly customized purchased general ledger IT system?	Yes. The general ledger IT system is a custom in-house built system.

Does management have access to the general ledger IT system's source code?	Yes. IT management has access to the source code.
Is access restricted to authorized personnel (e.g., only IT personnel have access and there is segregation of duties between IT and accounting)?	Yes. Only personnel in the IT department with the appropriate authority in accordance with the entity's policies has access to the source code
If those in the accounting department have access to the general ledger IT system, are there controls in place to detect unauthorized changes to source code impacting journal entries? If yes, describe the controls	N/A. The accounting department does not have access to the source code
Are there any system configurations (i.e., access to configurations or source code to change how journal entry general ledger accounts, dates, amounts, journal entry type are recorded in the general ledger) that impact how journal entries are posted?	Yes. The system allows the ability to override how journal entry general ledger accounts and journal entry type are recorded in the general ledger
Who has access to change the system configurations?	An Accounting Analyst.
Is access restricted to authorized personnel (e.g., only IT personnel have access and there is segregation of duties between IT and accounting)?	No, since an Accounting Analyst has access.
Can the entity provide evidence of who has access to source code and system configurations?	Yes. Management provided a system generated report of users that have access to update source code and system configurations of the general ledger IT system. The engagement team confirmed the controller does not have access to modify source code or system configurations of the general ledger IT system
Are there manual controls in place over journal entries?	Yes. On a monthly basis, the controller reviews a report of journal entries.

<p>What automated process control activities does the entity have in place over journal entries?</p>	<p>The following automated process control activities are in place over the general ledger IT system:</p> <ul style="list-style-type: none"> - AC-1: The system is configured to appropriately post journal entries
--	--

Analysis

Given:

- The entity uses a custom in-house built general ledger IT system,
- Entity Management has access to the source code,
- The general ledger IT system has a system configuration that impacts how journal entries are posted (i.e., access to configurations or source code to change how journal entry general ledger accounts, dates, amounts, journal entry type are recorded in the general ledger) and the Accounting Analyst has access to change the configuration, and
- The engagement team obtained and inspected a system-generated report confirming that the controller did not have access to modify source code, system configurations, or journal entries,

the engagement team determines that journal entries are likely susceptible to unauthorized or inappropriate intervention or manipulation. Additionally, the engagement team determines that the manual process control activity of the controller reviewing a report of journal entries monthly relied on by management is performed at a sufficient level of precision to address the risk of journal entries being subject to unauthorized or inappropriate intervention or manipulation, even though there are also automated process control activities addressing such risk. Therefore, the engagement team evaluates the design and implementation of the manual process control activity only.

Fact pattern 4

Consider an entity that responds in the same way to the questions in Fact pattern 3 above, except that the response to the question "Are there manual controls in place over journal entries?" is that there are no manual controls.

Analysis

Given:

- The entity uses a custom in-house built general ledger IT system,
- The general ledger IT system has a system configuration (i.e., access to configurations or source code to change how journal entry general ledger accounts, dates, amounts, journal entry type are recorded in the general ledger) that impacts how journal entries are posted and the Accounting Analyst has access to change the configuration,
- There are no manual controls in place over journal entries, and
- The engagement team identified automated process control activities over journal entries,

the engagement team determines that journal entries are likely susceptible to unauthorized or inappropriate intervention or manipulation and there is no manual control in place over journal entries. Therefore, the engagement team identifies and evaluates the design and implementation of automated process control activities over journal entries and the relevant GITCs.

The engagement team identifies the following RAFITs relevant to the above automated process control activities and evaluates the design and implementation of the GITCs listed below.

RAFIT	GITC
1.4 APD - Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	Privileged-level access (e.g., configuration, data and security administrators) in the IT system is authorized and appropriately restricted.
2.1 PC - Changes to IT programs were inappropriate (i.e., unapproved or do not function as intended).	Changes to IT system programs are approved prior to implementation into the production environment.
2.2 PC - Changes to IT configurations were inappropriate (i.e., unapproved or do not function as intended).	Changes to IT system configurations are approved prior to implementation into the production environment.
2.3 PC - Logical access to implement changes to IT system program or configurations into the production environment is inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	Changes into the production environment, including configuration changes, are reviewed by IT management personnel to determine if they are appropriately authorized, restricted and segregated from the development environment.

15 Identify and evaluate the design and implementation of relevant GITCs [ISA | 1353]

What do we do?

Identify and evaluate the design and implementation of relevant general IT controls.

Why do we do this?

Identifying and evaluating the design and implementation of GITCs that address relevant RAFITs gives us evidence to support the:

- continued effective operation of automated controls; and/or
- integrity of data and information within the IT systems that we plan to rely on as part of our audit.

Execute the Audit

What are general IT controls? [ISA | 1353.1300]

General IT controls (GITCs) are control activities over the entity's IT processes that support the continued effective operation of the IT environment, including:

- the continued effective operation of automated controls, and
- the integrity of data and information within the entity's IT system.

The IT processes are the entity's processes to manage access to programs and data, manage program changes, manage program acquisition and development, and manage computer operations (see activity '[Understand the entity's IT processes](#)' for more information).

The IT environment encompasses the IT systems the entity uses as part of its financial reporting and business processes, including its layers of technology (application, database, operating system and network), the IT processes and the IT organization (see activity '[Understand how the entity uses IT as part of financial reporting](#)' for more information).

GITCs are not expected to directly prevent, or detect and correct, material misstatements on a timely basis, but ineffective GITCs may lead to automated controls that don't operate consistently and effectively, and therefore might not prevent, or detect and correct, a material misstatement on a timely basis.

How are GITCs different from automated process control activities? [ISA | 1353.10549]

	Automated process control activities	GITCs
Purpose	Address process risk points (PRPs).	<p>Address risks arising from IT (RAFITs).</p> <p>Support the continued effective operation of the IT environment, including:</p> <ul style="list-style-type: none"> • the continued effective operation of automated controls, and the integrity of data and information within the entity's IT system.
Identified	When obtaining an understanding of the business processes and we intend to evaluate the design and implementation.	<p>After identifying automated controls and relevant layers of technology and RAFITs.</p> <p>When, as part of testing management's controls over the completeness and accuracy of internal information data integrity risks are addressed by GITCs.</p>

When we determine whether a control activity is an automated process control activity or a GITC, it is helpful to think about whether the control activity directly mitigates a PRP and an identified risk of material misstatement (RMM).

For example, consider a process control activity related to the individuals who have access to create journal entries in an entity's IT system. This directly addresses a PRP related to the creation of fraudulent journal entries.

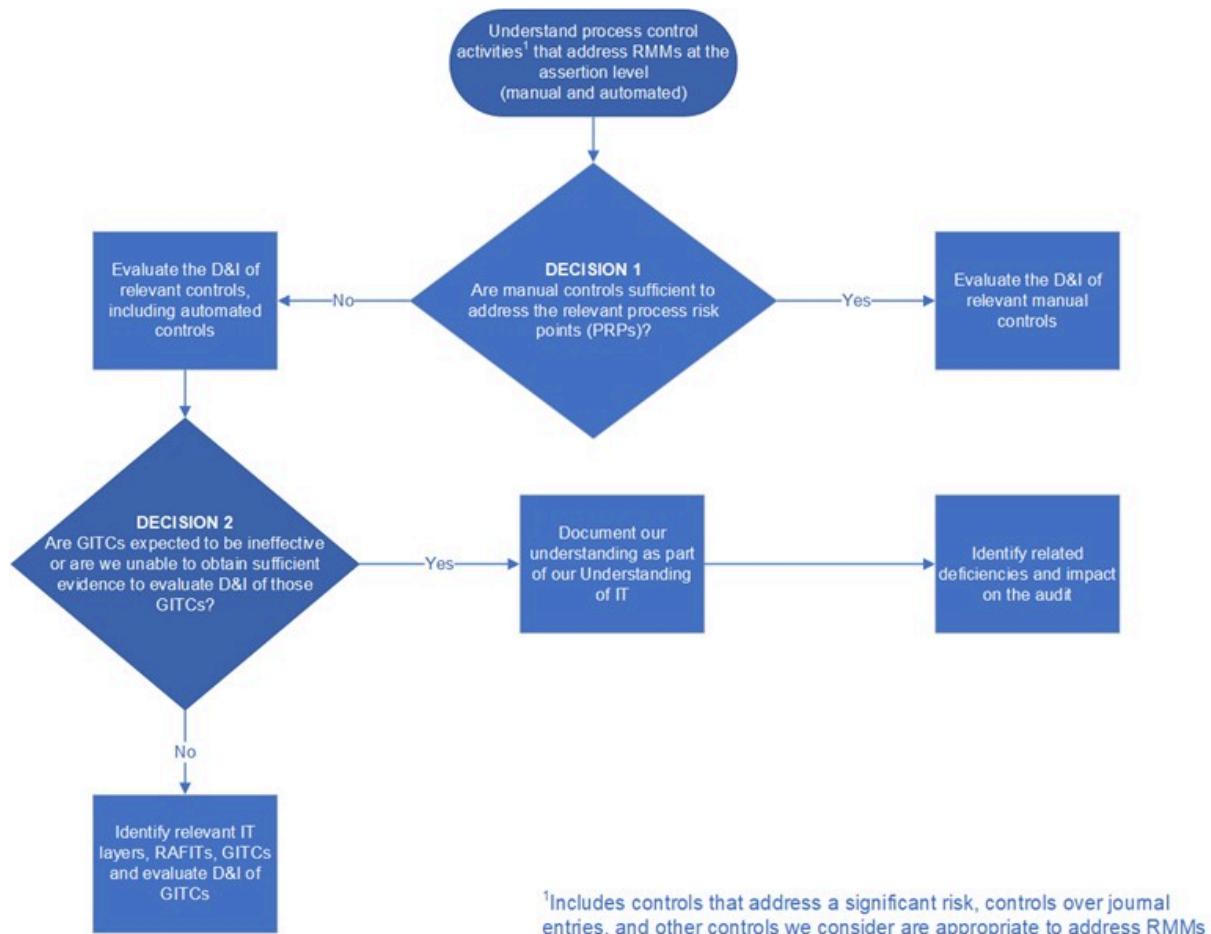
Alternatively, consider a GITC related to the creation of new users and modifications to user permissions within the IT application layer. This supports the effective operation of an automated process control activity that addresses a PRP related to the creation of fraudulent journal entries.

[Under what circumstances do we evaluate the design and implementation of GITCs?](#) [ISA | 1353.1500]

We identify and evaluate the design and implementation of GITCs where we have identified relevant layers of technology and RAFITs (see question '[Under what circumstances do we identify relevant layers of technology and RAFITs?](#)'). In our methodology we name these GITCs as 'relevant GITCs'. In practice, this means that we identify and evaluate the design and implementation of GITCs that:

- support the effective operation of automated control activities, when we:
 - plan to rely on and test the operating effectiveness of those automated control activities, or
 - evaluate the design and implementation of automated control activities, even though we do not plan to test their operating effectiveness (e.g., when we evaluate the design and implementation of an automated process control activity that addresses a significant risk or over journal entries). However, when GITCs are a) informal and, therefore, unable to be evaluated for design and implementation or b) expected to be ineffective (i.e. resulting in a control deficiency), we may document our understanding of relevant layers of technology, RAFITs and GITCs in summary as part of our understanding of the IT environment rather than identifying the individual layers of technology, RAFITS and GITCs for each automated control activity; or
- address the RAFIT(s) identified for the applicable IT system layer (e.g., database) related to data integrity risk, when we are testing management's controls over the accuracy and completeness of internal information to evaluate the reliability of such information (see question '[Are there specific risks that we consider when testing management's controls over internal information?](#)' for more information on audit considerations regarding data integrity risks).

The following decision tree provides an illustration of the decisions to be made and the implications with regards to evaluating the design and implementation of GITCs in the scenario where we evaluate the design and implementation of control activities but we do not plan to test their operating effectiveness:



How may we document our understanding of relevant layers of technology, RAFITs and GITCs in summary as part of our understanding of the IT environment? [ISA | 1353.8899]

When we evaluate the design and implementation of automated control activities but we do not plan to test their operating effectiveness, and GITCs are a) informal and, therefore, unable to be evaluated for design and implementation or b) expected to be ineffective (i.e. resulting in a control deficiency), we may document our understanding of relevant layers of technology, RAFITs and GITCs in summary as part of our understanding of the entity's IT processes within our understanding of the IT environment.

For example, consider an entity with the following circumstances:

- Has a less complex IT environment
- Uses System A, a single commercial accounting software application
- GITCs are not always formalized and documented
- We identified GITC deficiencies in the previous audit
- We have evaluated the design and implementation of an automated control that addresses a significant risk, but we do not plan to rely on the operating effectiveness of that control

Our understanding of the entity's IT processes may include the following:

IT process	Description

Access to programs and data	<p>The IT Manager and the Accounting Manager (as a backup) have security administrative responsibility to administer access to the system. The prior year deficiency related to the privileged access GITC was not remediated in the current year¹. RAFITs related to access to programs and data in system A are considered relevant to automated controls and they are addressed by the following steps in the process.</p> <p>The process to provision access is initiated when the Accounting department identifies a new user that needs access. Generally, the Accounting Manager sends a request either verbally or via email to the IT Manager requesting a new user account. The emails are not always retained².</p> <p>The user is required to change the password upon initial logon. The entity has password rules in place for minimum password length, password expiration, and complexity requirements.</p> <p>The process to de-provision access occurs when the IT Manager is notified of an employee resignation or termination. Upon notification of termination, the IT Manager will revoke the terminated employees' access. The IT Manager indicated that he does not always retain documentation to evidence the timely removal of access².</p> <p>There is no data processing center, as the system is maintained on the cloud.</p>
<p>Footnotes</p> <p>¹ KPMG identifies this as a deficiency</p> <p>² Since the entity has a less complex IT environment and uses a single commercial accounting software application, GITCs may not always be formalized and documented, which in this case is considered appropriate for the size and complexity of the entity and its IT environment.</p>	

Remember: When documenting our understanding of IT processes, we obtain an understanding for all four IT processes even if we identify a deficiency in one process. In this example, only one row was completed to illustrate example documentation when a deficiency is identified.

How do we evaluate the design and implementation of GITCs? [ISA | 1353.1505]

We evaluate the design and implementation of GITCs through inquiry in combination with observation and/or inspection.

Determining whether a GITC has been designed effectively means determining if the GITC satisfies the company's control objectives by addressing the RAFIT(s) it is intended to address.

Determining whether a GITC has been implemented means determining whether the GITC exists and whether the entity is using it.

What do we consider when we evaluate the design and implementation of a GITC? [ISA | 1353.8662]

We evaluate the design and implementation of a GITC considering the same items as when we evaluate the design and implementation of a process control activity, except for:

- anti-fraud control, and
- level of precision.

Given the different characteristics of GITCs and how they function, those characteristics aren't relevant to our evaluation. Remember that a GITC's objective is different from a process control activity's objective, specifically:

- The objective of GITCs is to address RAFITs, whereas
- The objective of process control activities is to mitigate PRPs to prevent, or detect and correct, material misstatements in the entity's financial statements.

[How do we determine whether the design of a GITC achieves its objectives?](#) [ISA | 1353.1600]

A GITC achieves its control objective when it adequately addresses each RAFIT it is designed to address.

To evaluate whether a GITC addresses each RAFIT it is intended to address, we understand how the GITC is performed, which means identifying control attributes. Control attributes are the specific procedures performed by the control operator (an individual or person for manual controls or IT systems for automated controls) that make-up the GITC and that are relevant to the design of the control.

Another way of thinking about control attributes is that they are the specific elements that are necessary for the GITC to be designed, implemented, and operating effectively. For example, if determining whether access to IT systems has been approved by an appropriate individual based on a pre-determined list is a necessary part of how a RAFIT is addressed, then that's a control attribute. If providing access within a certain number of days has no bearing on whether a RAFIT is addressed, then that is not a control attribute. The table below shows example control attributes for an example GITC.

RAFIT	GITC Description	Example Control Attributes - How the GITC is performed
1.2 APD - Logical access permissions (new or modified) are granted to users and accounts (including shared or generic accounts) that are inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	Management approves the nature and extent of user access permissions for new and modified user access in ABC system.	Control operator determines requests for new ABC system access or modification to existing ABC system access, are approved by an authorized user commensurate with the entity's IT delegation of authority.
		Control operator compares the permissions requested in the form/ticket to the entity's approved security profiles or roles by job function.
		Control operator determines that the access provisioned is consistent with access requested and approved.

[Can there be common GITCs across multiple layers of technology? \[ISA | 1353.8663\]](#)

Yes, an entity may use common IT processes across its IT environment or across certain layers of technology, in which case common RAFITs and common GITCs may be identified.

[Are there additional considerations when GITCs exist across multiple layers of technology? \[ISA | 1353.8664\]](#)

Yes, when manual GITCs exist across multiple layers of technology, we consider the shared characteristics to determine whether the GITCs are designed and implemented to operate consistently.

When manual GITCs are designed and implemented to operate consistently across multiple layers of technology, we may test the operating effectiveness of those GITCs to address the relevant RAFITs by using the common approach.

[What shared characteristics indicate a GITC operates consistently across multiple layers of technology? \[ISA | 1353.8665\]](#)

When manual GITCs exist across multiple IT systems and/or layers of technology, we consider the following characteristics to determine that the GITCs are designed and implemented to operate consistently:

Characteristics	Description
Same policies, practices, and procedures	Standard policies, practices, and procedures are followed by the control operators when performing the GITCs and any tools used in the performance of the control are the same
Same type of information used in the performance of the control	Information used by the control operators in the performance of the control is same type of information (e.g., the relevant data elements are the same and the information is generated in the same manner).
Subject to same monitoring activities	Monitoring activities are performed consistently across to monitor internal controls. Refer to activity ' Understand and evaluate monitoring activities ' for guidance.

[What is the common approach to testing the operating effectiveness of manual GITCs? \[ISA | 1353.8666\]](#)

The common approach is summarized below.

Guidance	Common approach
Applicability	Applies to manual GITCs that are designed to operate consistently across multiple layers of technology. Refer to the question 'What shared characteristics indicate a GITC operates consistently across multiple layers of technology?' for guidance.

Population	Single population across all relevant layers of technology. The completeness of the population is important in supporting GITC conclusions; therefore we do not exclude relevant IT systems and/or layers of technology nor do we include non-relevant layers of technology.
Sample size	Follow the guidance in activity ' Determine the control sample size ' .
Deficiencies	Any deviations in GITCs are considered control deficiencies. The deficiencies apply to all layers of technology in the population. It is not appropriate to isolate deficiencies to a single layer of technology when reaching a conclusion.
Conclusions	GITC conclusions apply to all relevant layers of technology included in the population.

Automated GITCs may also be designed to operate consistently across multiple layers of technology; however the testing approach is the same for all automated GITCs whether they operate over one or more layers.

How does an ineffective GITC affect our audit? [ISA | 1353.1700]

If we determine that a GITC is ineffective in its design and/or implementation (see activity '[Determine whether a deficiency in ICFR exists and describe it](#)' for more information), we:

- conclude that there is a deficiency;
- do not plan to rely on or test the operating effectiveness of that GITC.; and
- consider the effect of that deficiency on the automated controls it supports or the integrity of data used in the audit (for example, if the deficient GITC supports a process control activity, it may affect our planned audit response to an identified RMM and our assessment of CAR related to an identified RMM).

See activity '[In response to GITC deficiencies, test other GITCs, perform procedures or conclude on related automated control\(s\) and/or reliability of data within the IT system](#)' for more information on how to respond to GITC deficiencies.

Although GITC deficiencies, on their own, do not directly cause financial statement misstatements, deficient GITCs may render an automated control ineffective or the data within an IT system not reliable, and this may lead to financial statement misstatements that could be material. The significance of a GITC deficiency relates to its impact on the effectiveness of automated controls and/or integrity of data within an IT system.

Examples

How do we support our conclusion that a GITC operates consistently across multiple layers of technology? [ISA | 1353.8674]

Fact pattern

The entity has 3 relevant IT systems. Based on the engagement team's understanding of the relevant business processes, automated process control activities were identified as relevant in each of the three relevant IT systems. The following GITC was identified to address relevant RAFTs in each of the IT systems:

PC2-1: Changes to IT system programs are tested and approved prior to implementation into the production environment.

Additional information:

- The layers of technology relevant to the automated process control activities include the application and database layers.
- Following are the relevant IT systems:
 - System 1: SAP application; SQL server database
 - System 2: Oracle application; Oracle database
 - System 3: Hyperion Financial Management (HFM); SQL server database
- Based on the engagement team's understanding of IT:
 - The IT department is comprised of application development groups that support each of the IT systems - one group supports SAP; one group supports Oracle and one group supports HFM. There is one group that supports all databases.
 - The IT department follows the same program change policies, practices and procedures for all applications
 - The IT department uses the same change management ticketing tool, ServiceNow, to initiate change requests, evidence testing, track changes, and obtain approvals.
 - The control owners indicate the GITC is designed and implemented to operate consistently across all three IT systems and layers of technology.

Analysis

To evaluate the design of the GITC, the engagement team:

- Inquired of the control owners for SAP, Oracle, HFM, and databases to confirm they all follow the same change management process.
- Inspected the change management policies and procedures to determine the requirements for testing system program changes and the required approvals to indicate that testing was successful and applies to ALL relevant layers of technology
- Inspected the change management ticketing tool, ServiceNow configuration (e.g., drop-down list) that shows that all relevant layers of technology are listed.

[How do we determine the population using the common approach?](#) [ISA | 1353.8675]

Fact pattern

An entity has 10 IT systems but only 3 IT systems (systems A, B, and C) are relevant to the audit. Based on the engagement team's understanding of the relevant business processes, 3 automated process control activities were identified as relevant:

- One implemented in system A with the following RAFT: PC1 in SAP and PC 1 in SQL (SAP)
- One implemented in system B with the following RAFT: PC1 in Oracle financials and PC1 in Oracle DB

- One implemented in system C with the following RAFIT: PC1 in Hyperion and PC1 in SQL(Hyperion)

These six layers are therefore all relevant.

The engagement team identifies one GITC to address all six relevant program changes RAFITs.

Based on inquiry and inspection, it was noted that the GITC is designed and implemented to operate consistently across all the entity's relevant layers.

Management provides a listing of 3,750 changes; however, 750 changes are for layers that do not relate to any of the six layers.

The RAWTC for all three automated process control activities was assessed as base and the RAWTC for the GITC was assessed as base.

Analysis

The relevant population of program changes is 3,000. The 750 changes for systems that are not relevant to the audit are excluded from the population from which samples are selected to test the program change control.

The engagement team selects a sample of 25 operations from the population haphazardly. Provided the selection is random or haphazard, the selection does not have to include controls operations for each of the six layers although in this example it is likely to.

16 Document planning and risk assessment activities [ISA | 1645]

What do we do?

Prepare audit documentation to clearly evidence planning and risk assessment activities

Why do we do this?

In preparing the audit documentation, we document a summary of the identified RMMs and our assessment of the CAR, and our assessment of financial statement level risks, in order to properly evidence how the procedures performed, including control testing, and conclusions reached appropriately respond to the RMMs identified.

Execute the Audit

What information relative to the risks identified and responses to those risks do we include in our audit documentation? [ISA | 1645.1400]

Our audit documentation specifically includes:

- A summary of the identified and assessed risks of material misstatement at both the assertion level and financial statement level including significant risks and risks for which substantive procedures alone cannot provide sufficient appropriate audit evidence, and the rationale for the significant judgments made;

- Our audit responses with a linkage back to the risks of material misstatement. This includes tests of controls, overall responses and substantive procedures; and
- Conclusions reached related to those audit procedures (e.g. effective/ineffective controls, misstatements identified, if substantive test was achieved).

How do we document the information about the risks identified and our response as part of our audit? [ISA | 1645.1500]

KPMG Clara workflow facilitates the documentation of risks as part of our risk assessment process and audit planning (to identify and assess risks and connect RMMs to our planned responses) and as our procedures are performed (we document the conclusions reached in relation to the procedures performed).

17 Identify and assess RMMs [ISA | 561]

What do we do?

Identify and assess the risks of material misstatement at the financial statement level and the assertion level

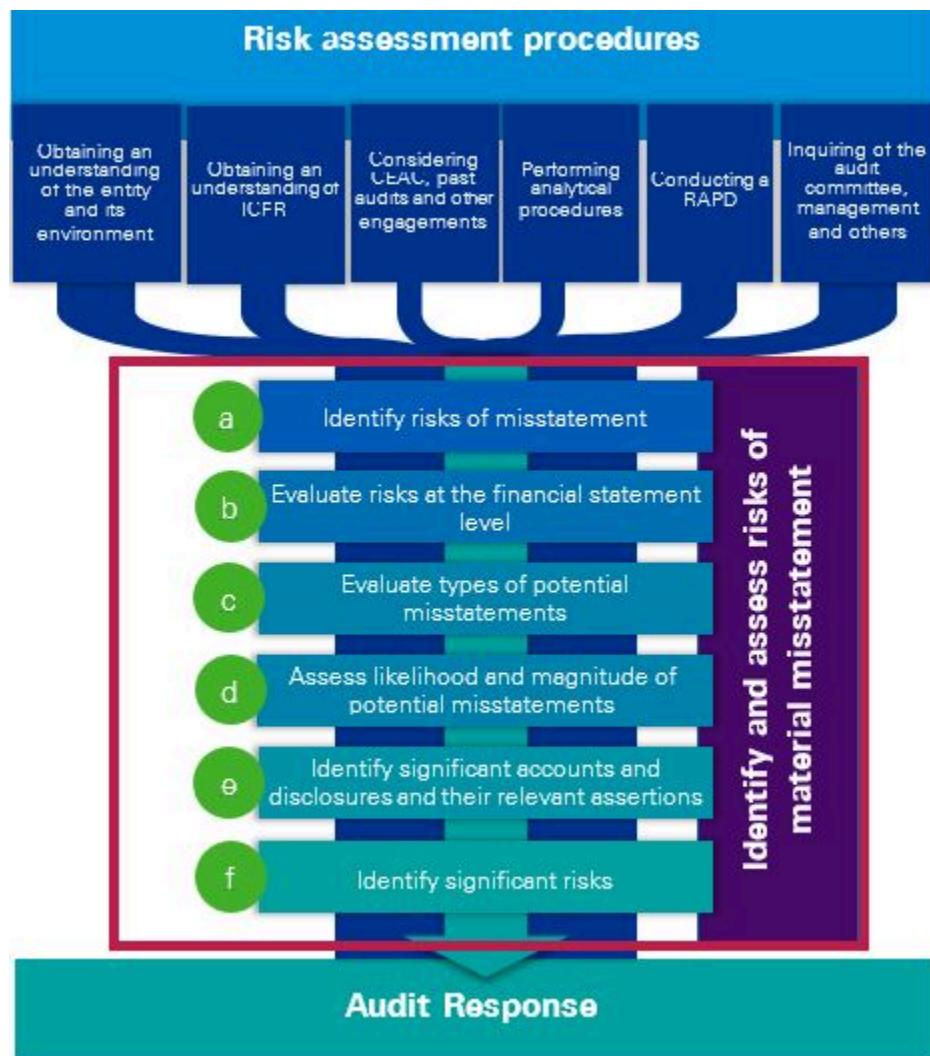
Why do we do this?

Identifying and assessing the risks of material misstatement (RMMs) provides the basis for the determination of relevant assertions, significant accounts and disclosures and to provide a basis for designing and performing further audit procedures.

Execute the Audit

Where does this activity fit into our risk assessment? [ISA | 561.1300]

We perform our risk assessment procedures with a specific purpose in mind: to collect information to identify and assess RMMs. These RMMs will then drive our audit responses. Visually, we may think of the process as follows.



What are the different types of risks, and how are they interrelated? [ISA | 561.1400]

There are three types of risk.

Risks of misstatement (RMs)	Risks that could result in a misstatement to the financial statements. These can be either assertion-level RMs or financial statement-level RMs . This is the population of risks we assess further.
Risks of material misstatement (RMMs)	Risks that could result in a <i>material</i> misstatement to the financial statements. These can be either assertion-level RMMs or financial statement-level RMMs .
<u>Significant risks</u>	Risks that are closer to the upper end of the spectrum of inherent risk.

	Special audit consideration is given for these RMMs because of the nature of the risk or the potential likelihood and magnitude of misstatement related to the risk. These include fraud risks and significant unusual transactions with related parties.
--	---

These are subsets of one another, representing an increasingly narrow focus. As such, we identify the different types of risk in this order.

The graphic below shows one way to visualize the relationship between these different types of risks.



What are assertion level and financial-statement level RMMs? [ISA | 561.8552]

The following table explains the differences between assertion-level and financial statement level risks:

Type of risks	What are they?
Assertion-level RMMs	Risks of material misstatement that: <ul style="list-style-type: none"> relate to specific assertions for classes of transactions, account balances, or disclosures; and relate to misstatements that can arise when the financial reporting framework (e.g. IFRS, US GAAP), is not applied appropriately.
Financial statement-level RMMs	Risks of material misstatement that: <ul style="list-style-type: none"> relate pervasively to the financial statements as a whole may affect many accounts and/or assertions don't necessarily relate to applying particular accounting policies or principles

- may arise from the entity and its environment, including business risks and broad internal control issues

How do we identify and assess RMMs? [ISA | 561.1500]

We follow a six-step process to identify and assess RMMs. This process uses the information we have obtained during our risk assessment procedures, as well as any other relevant knowledge we may have.



Step a	Identify RMs using information from risk assessment procedures and considering the characteristics of the accounts and disclosures
Step b	Evaluate whether the identified RMs relate pervasively to the financial statements as a whole and potentially affect many assertions
Step c	Evaluate the types of potential misstatements that could result from the identified risks and the accounts, disclosures and assertions that could be affected
Step d	Assess the likelihood and magnitude of potential misstatements, including the possibility of multiple misstatements to determine RMMs and assess inherent risk

Step e	Identify significant accounts and disclosures and their relevant assertions
Step f	Determine whether any of the identified and assessed RMMs are significant risks

As part of this six-step process we also document our rationale for significant judgements made regarding the identification and assessment of RMMs.

18 Determine significant risks [ISA | 573]

What do we do?

Determine whether any of the identified and assessed risks of material misstatement are significant risks

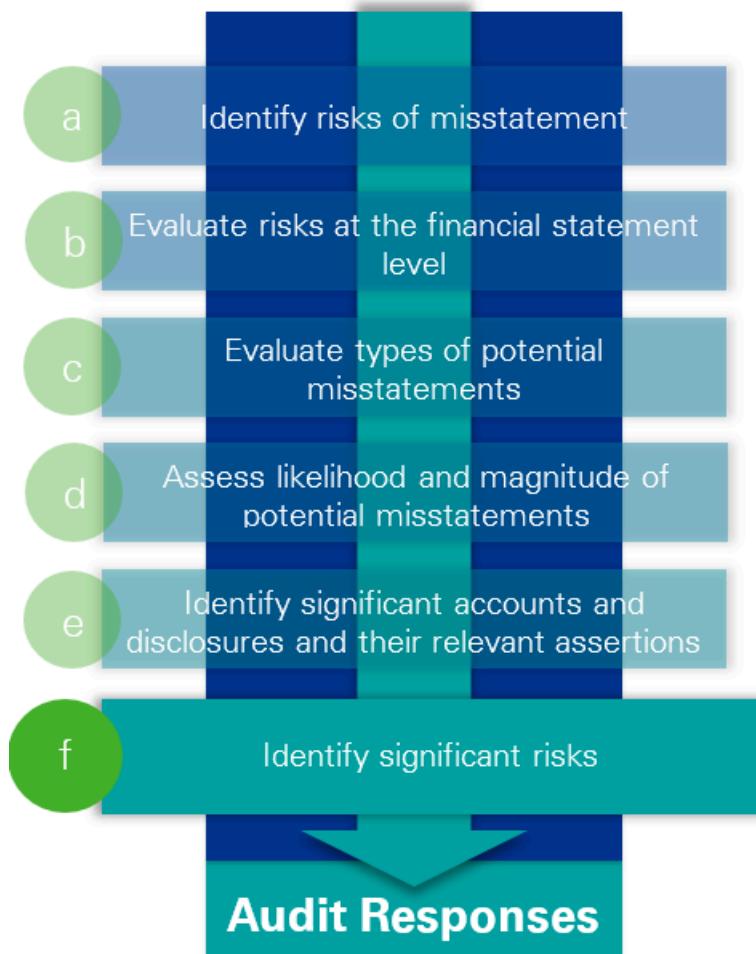
Why do we do this?

The determination of significant risks allows for the auditor to focus more attention on those risks that are on the upper end of the continuum of inherent risk. If we fail to assess the inherent risk as Significant, we could perform the wrong audit procedures to address the risk.



Execute the Audit

Where are we in our risk assessment? [ISA | 573.1300]



What is a significant risk? [ISA | 573.1400]

A significant risk is a risk of material misstatement (RMM) which is:

- close to the upper end of the continuum of inherent risk due to the degree to which inherent risk factors affect the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement should that misstatement occur; or
- fraud risks; or
- significant unusual transactions with related parties.

We document special audit considerations in response to significant risks.

What does 'special audit consideration' mean? [ISA | 573.8652]

'Special audit consideration' means focusing more attention on those risks that are on the upper end of the continuum of inherent risk, through the performance of certain procedures including:

- Evaluating design and implementation of control activities that address the RMM (see '[Evaluate the design and implementation of relevant control activities](#)');
- Designing and performing substantive procedures that specifically respond to the significant risk (see '[Perform substantive procedures that respond to significant risks](#)');
- Obtaining more persuasive audit evidence as our assessment of inherent risk increases (see '[Design and perform substantive procedures whose nature is responsive to CAR](#)');

- Communicating with those charged with governance about the significant risks we identified (see '[Communicate planned scope and timing of the audit](#)')
- Taking into account significant risks when determining those matters that required significant auditor attention, which are matters that may be key audit matters (see '[Determine if there are any KAMs in the current audit period](#)')
- Required review of audit documentation related to significant risks and our audit response thereto by the engagement partner (see '[Perform minimum required review](#)')
- For group audits, increased involvement by the group engagement partner if the significant risk relates to a component in a group audit and for the group engagement team to direct the necessary work at the component by the component auditor (see '[Group Audit | Be involved in the component auditor's risk assessment when they perform an audit of a significant component](#)' and '[Group Audit | Evaluate the appropriateness of, and determine whether to be involved in, the component auditor's planned audit procedures over group significant risks](#)').
- In addition, where we plan to rely on the operating effectiveness of control activities that address significant risks, we cannot rely on prior period testing of such controls.

We think carefully about how we identify and describe significant risks and include the 'what, where, why and how' associated with each significant risk.

Being specific helps us to better tailor our responses to these risks and apply 'special audit consideration'. With this in mind, it may be useful to take a second look at the population of significant risks, and carefully think about whether we've identified them with enough specificity.

[How do we determine whether any of the identified and assessed RMMs are significant risks?](#) [ISA |

573.11802]

In addition to considering those risks that are closer to the upper end of the continuum of inherent risk noted in question '[What are the inherent risk factors?](#)' the following table shows the factors we consider to determine whether any identified and assessed RMMs are significant risks:

Factors	Example of being lower on the inherent risk continuum	Example of being higher on the inherent risk continuum
Whether the risk is a fraud risk	A risk that is not a fraud risk.	An identified fraud risk. Remember: a fraud risk is a significant risk.
Whether the risk relates to recent significant economic, accounting or other developments	Risks related to the valuation of certain assets, when: <ul style="list-style-type: none"> • a commodity price is a primary input in the valuation model; and • the commodity's prices have been relatively 	Risks related to the valuation of certain assets, when: <ul style="list-style-type: none"> • a commodity price is a primary input in the valuation model; and • there has been significant volatility in

	<p>stable in the current period.</p>	<p>the commodity's prices in the current period.</p> <p>Changes in the entity's business that involve changes in accounting, for example, mergers and acquisitions.</p>
The complexity of transactions	<p>Risks associated with the issuance of new debt when the debt instrument is simple and does not have unique or complex features.</p>	<p>Risks associated with the issuance of new debt when the debt instrument has multiple conversion features and embedded derivatives.</p> <p>Complexity in data collection and processing to support account balances.</p> <p>Accounting policies or principles that may be subject to differing interpretation.</p> <p>Accounting for unusual or complex transactions, including those in controversial or emerging areas (for example, accounting for revenue with multiple performance obligations that are difficult to value).</p>
Whether the risk involves significant transactions with related parties	<p>Risks associated with accounting for and disclosing a transaction between an entity and an unrelated third party for the purchase of land to be used to build a new corporate headquarters.</p>	<p>Risks associated with accounting for and disclosing a transaction between an entity and a board member, to buy land to build a new corporate headquarters.</p> <p>Remember: significant unusual transactions with related parties are assessed as a significant risk. (see activity 'Identify and assess RMMs, including significant risks, associated with</p>

		related parties' for additional considerations)
The degree of complexity or judgment in recognizing or measuring financial information related to the risk	Risks related to the valuation of investment securities that are exchange-traded, and for which published prices are available in active markets — i.e. Level 1.	Risks related to the valuation of investment securities that are valued using multiple unobservable inputs — i.e. Level 3. Accounting policies or principles that may be subject to differing interpretation. Transactions for which there are multiple acceptable accounting treatments such that subjectivity is involved.
Whether the risk involves significant unusual transactions	Risks related to a transaction that is routine and in the normal course of business — e.g. processing monthly payroll transactions.	Risks related to a transaction that is (or could be) many times greater than materiality and outside of the normal course of business — e.g. a large, speculative investment in a business unrelated to the entity's core operations. Not <i>all</i> risks related to significant unusual transactions will be significant risks, however, these risks may be higher on the inherent risk continuum because they may involve one or more of the following: <ul style="list-style-type: none"> • greater management intervention to specify the accounting treatment • greater manual intervention for data collection and processing • more complex calculations or

		<ul style="list-style-type: none"> accounting policies or principles • non-routine transactions, whose nature may make it difficult for the entity to implement effective processes to account for the transactions <p>Remember: significant unusual transactions with related parties are assessed as a significant risk. (see activity 'Identify and assess RMMs, including significant risks, associated with related parties' for additional considerations)</p>
--	--	--

We consider these factors as a whole, which means that no individual factor determines where a risk falls on the inherent risk continuum. We identify significant risks based on inherent risk, without regard to control activities.

19 Understand relevant control activities that address significant risks [ISA | 576]

What do we do?

IF we determine that a significant risk, including a fraud risk, exists, THEN obtain an understanding of the relevant control activities that are intended to address the risks, by evaluating the design and implementation of those controls

Why do we do this?

As part of our risk assessment procedures, we obtain an understanding of a process to help us identify risks of material misstatement (RMMs). When we have a significant risk, including a fraud risk, we go even further, and evaluate the design and implementation of relevant control activities. This helps us better understand the risk, and informs our overall assessment of significant risks and how best to respond to them.

Execute the Audit

How do we identify relevant control activities that address a significant risk? [ISA | 576.1400]

We identify relevant control activities that address a significant risk by:

- understanding ICFR, including the entity's processes and CERAMIC;
- identifying all the process risk points related to the significant risk;
- identifying and obtaining an understanding of the control activities that address the relevant process risk points and risks arising from IT.

Not all control activities related to a significant risk may be relevant. Relevant control activities are those that address the PRP/RAFITs related to an RMM.

[How do we identify controls that address fraud risks?](#) [ISA | 576.1500]

All fraud risks are significant risks, so we identify relevant control activities that address fraud risks in the same manner as all other significant risks.

We describe process control activities that address process risk points related to a fraud risk as anti-fraud controls. There are specific considerations about the nature, timing and extent of audit procedures we design and perform to test anti-fraud controls.

A process control activity is an anti-fraud control when:

- we have identified a fraud risk at the assertion level or financial statement level; and
- that process control activity directly mitigates the identified fraud risk, either individually or when combined with other controls.

[Can anti-fraud controls also address a risk of error?](#) [ISA | 576.11815]

Yes. Some process control activities are designed to address the risk of fraud (anti-fraud controls) and the risk of error simultaneously.

An example of this might relate to an estimate that:

- has a high degree of judgment (risk of error); and
- creates an opportunity for management to intentionally manipulate assumptions to achieve a desired result (risk of fraud).

Management may implement process control activities that address risks related to determining the key assumptions, and evaluating the potential for management bias in selecting those assumptions. If so, the identified control may respond to the fraud risk and the risk of error for the estimate.

[What if control activities are not designed and implemented for significant risks?](#) [ISA | 576.2000]

Failure of the design or implementation of control activities addressing a significant risk is a deficiency in internal control and may indicate a significant deficiency. We evaluate deficiencies like this, and communicate them, as appropriate — even if we're performing a financial statement audit in which we do not intend to test the operating effectiveness of such control activities.

Examples

[How may anti-fraud controls be designed to address the risk of management override for an accounting estimate?](#) [ISA | 576.11816]

Fact pattern:

An entity prepares a cash flow forecast to support its going concern assessment. The Financial Controller prepares the forecast and the CFO reviews it.

During the engagement team's fraud planning meeting — i.e. the RAPD — they identified incentives, opportunities and rationalizations that caused them to identify a fraud risk associated with the going concern disclosures. The team determined it may be easy for the CFO to tweak the revenue or expenses in the forecast, so that the entity's cash appeared sufficient for the relevant assessment period required by the financial reporting framework.

The entity has introduced a process control activity that is an anti-fraud control to address the risk of management override, whereby the board — i.e. those charged with governance — review the components of the going concern assessment. The board receive an analysis of each estimate used in the forecast, including:

- the range of reasonableness of each estimate;
- how that range was determined;
- how the range compares to prior periods; and
- where within the range management's estimate fell in this period compared to prior periods.

The board also receive an analysis of how the estimates as a whole affected earnings.

Analysis:

In this case, the review of each estimate by those charged with governance is an anti-fraud control designed to mitigate the risk of management bias in the estimates.

Bias may be evident in management's changes to:

- how the range of reasonable results is determined;
- where within that range their estimate falls (at the lower end, in the middle, or at the higher end); and
- how the relative placement of the point estimate changed period over period.

As this example illustrates, process control activities that are anti-fraud controls addressing the risk of management override in estimates can involve the board or audit committee. In many cases, estimates are reviewed by senior management — but that's where the risk of fraud due to management override lies. Involving the board in the review of certain assumptions can be an effective way for an entity to introduce anti-fraud controls.

20 Test control activities when substantive procedures alone cannot provide sufficient audit evidence [ISA | 597]

What do we do?

IF substantive procedures alone cannot provide sufficient appropriate audit evidence, THEN test the operating effectiveness of control activities over those assessed risks of material misstatement

Why do we do this?

We test the operating effectiveness of controls over a risk of material misstatement (RMM) when we can't design substantive procedures capable of obtaining sufficient appropriate audit evidence on their own.

Execute the Audit

When may we be unable to obtain sufficient appropriate audit evidence from substantive procedures alone? [ISA | 597.1300]

We may not be able to obtain sufficient appropriate audit evidence from substantive procedures alone when a significant amount of information or data elements are electronically initiated, recorded, processed or reported. In this case, our ability to obtain sufficient appropriate audit evidence may depend on the entity's controls.

However, it is not necessary to test controls for every process with automated control activities or evidence in electronic form, except when the sufficiency and appropriateness of the substantive audit evidence depends on the entity's controls.

What are examples of when substantive procedures alone may not provide sufficient appropriate audit evidence? [ISA | 597.1400]

The following table sets out examples of situations in which performing substantive procedures alone may not provide sufficient appropriate audit evidence.

Scenario	Examples
The entity's financial reporting and accounting information systems rely heavily on IT, with little or no manual intervention. The entity also relies on embedded, automated process control activities to prevent or detect and correct misstatements that may occur during the activities to initiate, process and record financial transactions, and to create its financial statements.	<ul style="list-style-type: none"> Customer orders are placed directly on the entity's system via the web, without a customer purchase order, contract or data file. Customer agreements are signed online and maintained electronically in the entity's systems. Approvals or document matching are performed online by the IT system with little or no manual intervention. The entity runs an internet-based consumer marketplace that aggregates data about consumers and bills suppliers on a per click basis. It relies heavily on IT to deliver products and bill customers. We have identified financial statement-level RMMs or significant risks arising from the use of IT.
Important information may exist solely in electronic form. The entity uses an IT system to provide summarized information from many different IT systems to business process owners or management, and management	<ul style="list-style-type: none"> Each day, a retail entity's IT systems gather store sales data from multiple IT systems. Only automated process control activities exist to ensure management receives complete store sales data and aggregated sales data by region. There is no manual intervention, and there are no manual controls. Data transferred between IT systems

rely on database information and/or system-generated reports to generate the financial statements.	<p>does not include individual transactions to allow management (or us) to trace back to the source transactions.</p> <ul style="list-style-type: none"> We seek to use the history of price markdowns to audit a retail entity's markdowns reserve. We can only get this information at a sufficiently granular level through reports from the entity's enterprise resource planning or point-of-sale system. Therefore, we test controls to obtain evidence over the accuracy of markdown information and the completeness and accuracy of the entity's report for use in our substantive procedures.
The entity transacts electronically with third parties. Sales and purchases are automatically recorded between the entity and third parties, with little or no manual intervention.	<ul style="list-style-type: none"> An entity's customers buy software services direct from its website, with little or no manual intervention. The entity's recorded revenues are generated directly through these website sales. It receives daily sales summary reports but cannot trace individual transactions to their source. An entity conducts much of its business with vendors or customers over the web — e.g. when the entity places an order, its IT system automatically sends the order information to the vendor. The IT system then automatically matches the receipt and makes payment without manual intervention.
The entity uses a model to develop complex accounting estimates using data comprised of many small balances resulting from a high volume of transactions.	<ul style="list-style-type: none"> Data used in developing a complex expected credit loss provision for a financial institution or a utility entity.

What do we do if substantive procedures alone cannot provide sufficient appropriate audit evidence and the control activities related to the RMM are ineffective? [ISA | 597.8596]

If we assess control risk as no controls reliance for an RMM where we are unable to obtain sufficient appropriate audit evidence from substantive procedures alone, then we have a scope limitation for that RMM. We perform procedures in accordance with '[Modify the audit opinion for specific circumstances](#)'.

Example

When might substantive procedures alone not provide sufficient appropriate audit evidence? [ISA | 597.1500]

[Example 1 | Manufacturing entity](#) [ISA | 597.10976]

Fact pattern:

Entity A issues electronic purchase orders to its suppliers, and receives the related supplier invoices electronically. Entity A records the receipt of goods by scanning a supplier barcode on the received parcel. This initiates an automated process to match the purchase order price and quantity against the invoice price, quantity and barcode reference number.

The receipt is recorded in the inventory system, and the payable in the payables system. Both amounts are transferred to the general ledger. Given the automated nature of its process, Entity A does not retain hard copy receiving documents.

Analysis:

The process is highly automated and relies on evidence that only exists in electronic form — i.e. electronic invoices and purchase orders. Therefore, substantive procedures alone may not provide sufficient appropriate audit evidence.

As a result, the engagement team identify and test those automated process control activities and general IT controls that support the effective operation of these automated control activities. Otherwise, they may not obtain sufficient appropriate evidence in response to the identified risk.

Example 2 | Bank [ISA | 597.10977]**Fact pattern:**

Bank J relies heavily on IT systems to process deposit transactions. These transactions are captured through various means, including branch tellers, automated clearing house (ACH) transactions, wire transfers, automated teller machines (ATMs), telephone, online banking and correspondent banks.

We have identified the following RMM:

Deposits are not recorded as liabilities at the time they are received by the entity.

As part of our substantive procedures to address this RMM, we plan to perform procedures over the daily deposit suspense/transit account reconciliations at period end.

Analysis:

The process is highly automated, and relies on evidence that only exists in electronic form — i.e. checks deposited in the bank, wire transfers, ACH transactions, ATMs, branch tellers. Therefore, substantive procedures alone may not provide sufficient appropriate audit evidence.

As a result, the engagement team identify and test those automated process control activities and general IT controls that support the effective operation of these automated control activities. Otherwise, they may not obtain sufficient appropriate evidence in response to the identified risk.

Considerations for Understanding the Entity and its Business Model

International Standards on Auditing: ISA 315.Appendix 1

Appendix 1 Considerations for Understanding the Entity and its Business Model

(Ref: Para. A61.A67)

This appendix explains the objectives and scope of the entity's business model and provides examples of matters that the auditor may consider in understanding the activities of the entity that may be included in the business model. The auditor's understanding of the entity's business model, and how it is affected by its business strategy and business objectives, may assist the auditor in identifying business risks that may have an effect on the financial statements. In addition, this may assist the auditor in identifying risks of material misstatement.

Objectives and Scope of an Entity's Business Model

1. An entity's business model describes how an entity considers, for example its organizational structure, operations or scope of activities, business lines (including competitors and customers thereof), processes, growth opportunities, globalization, regulatory requirements and technologies. The entity's business model describes how the entity creates, preserves and captures financial or broader value, for its stakeholders.
2. Strategies are the approaches by which management plans to achieve the entity's objectives, including how the entity plans to address the risks and opportunities that it faces. An entity's strategies are changed over time by management, to respond to changes in its objectives and in the internal and external circumstances in which it operates.
3. A description of a business model typically includes:
 - The scope of the entity's activities, and why it does them.
 - The entity's structure and scale of its operations.
 - The markets or geographical or demographic spheres, and parts of the value chain, in which it operates, how it engages with those markets or spheres (main products, customer segments and distribution methods), and the basis on which it competes.
 - The entity's business or operating processes (e.g., investment, financing and operating processes) employed in performing its activities, focusing on those parts of the business processes that are important in creating, preserving or capturing value.
 - The resources (e.g., financial, human, intellectual, environmental and technological) and other inputs and relationships (e.g., customers, competitors, suppliers and employees) that are necessary or important to its success.
 - How the entity's business model integrates the use of IT in its interactions with customers, suppliers, lenders and other stakeholders through IT interfaces and other technologies.
4. A business risk may have an immediate consequence for the risk of material misstatement for classes of transactions, account balances, and disclosures at the assertion level or the financial statement level. For example, the business risk arising from a significant fall in real estate market values may increase the risk of material misstatement associated with the valuation assertion for a lender of medium-term real estate backed loans. However, the same risk, particularly in combination with a severe economic downturn that concurrently increases the underlying risk of lifetime credit losses on its loans, may also have a longer-term consequence. The resulting net exposure to credit losses may cast significant doubt on the entity's ability to continue as a going concern. If so, this could have implications for management's,

and the auditor's conclusion as to the appropriateness of the entity's use of the going concern basis of accounting, and determination as to whether a material uncertainty exists. Whether a business risk may result in a risk of material misstatement is, therefore, considered in light of the entity's circumstances. Examples of events and conditions that may give rise to the existence of risks of material misstatement are indicated in **Appendix 2**.

Activities of the Entity

5. Examples of matters that the auditor may consider when obtaining an understanding of the activities of the entity (included in the entity's business model) include:

(a) Business operations such as:

- Nature of revenue sources, products or services, and markets, including involvement in electronic commerce such as Internet sales and marketing activities.
- Conduct of operations (for example, stages and methods of production, or activities exposed to environmental risks).
- Alliances, joint ventures, and outsourcing activities.
- Geographic dispersion and industry segmentation.
- Location of production facilities, warehouses, and offices, and location and quantities of inventories.
- Key customers and important suppliers of goods and services, employment arrangements (including the existence of union contracts, pension and other post-employment benefits, stock option or incentive bonus arrangements, and government regulation related to employment matters).
- Research and development activities and expenditures.
- Transactions with related parties.

(b) Investments and investment activities such as:

- Planned or recently executed acquisitions or divestitures.
- Investments and dispositions of securities and loans.
- Capital investment activities.
- Investments in non-consolidated entities, including non-controlled partnerships, joint ventures and non-controlled special-purpose entities.

(c) Financing and financing activities such as:

- Ownership structure of major subsidiaries and associated entities, including consolidated and non-consolidated structures.
- Debt structure and related terms, including off-balance-sheet financing arrangements and leasing arrangements.
- Beneficial owners (for example, local, foreign, business reputation and experience) and related parties.
- Use of derivative financial instruments.

Nature of Special-Purpose Entities

6. A special-purpose entity (sometimes referred to as a special-purpose vehicle) is an entity that is generally established for a narrow and well-defined purpose, such as to effect a lease or a securitization of financial assets, or to carry out research and development activities. It may take the form of a

corporation, trust, partnership or unincorporated entity. The entity on behalf of which the special-purpose entity has been created may often transfer assets to the latter (for example, as part of a derecognition transaction involving financial assets), obtain the right to use the latter's assets, or perform services for the latter, while other parties may provide the funding to the latter. As ISA 550 indicates, in some circumstances, a special-purpose entity may be a related party of the entity.⁷⁰

⁷⁰ ISA 550, paragraph A7

7. Financial reporting frameworks often specify detailed conditions that are deemed to amount to control, or circumstances under which the special-purpose entity should be considered for consolidation. The interpretation of the requirements of such frameworks often demands a detailed knowledge of the relevant agreements involving the special-purpose entity.

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Understand relevant industry, regulatory and other external factors [ISA | 343]

What do we do?

Obtain an understanding of relevant industry, regulatory and other external factors.

Why do we do this?

Risks can arise from the entity's industry or regulatory environment, or from economic conditions.

For example, an oil and gas company is likely affected by risks from rising and falling commodity prices. These fluctuations can affect not only the entity's operations but also its asset values, its ability to service debt, and other areas that could lead to a risk of misstatement.

Understanding the industry, regulatory and other external factors helps us identify and assess risks of material misstatement (RMMs).

Execute the Audit

What does our understanding include? [ISA | 343.1300]

A broad range of topics may be relevant to our understanding. At a minimum, we understand:

- industry factors, including the competitive environment and technological developments;
- the regulatory environment, including the applicable financial reporting framework and the legal and political environment; and
- external factors, including general economic conditions.

See '[Understand the applicable legal and regulatory framework](#)' for additional guidance.

What sources of information can help us understand the relevant industry, regulatory and other external factors? [ISA | 343.1400]

Along with the [common sources of information](#) we use to understand the entity and its environment, we can also use the [Geographical Market Summaries](#) <https://alex.kpmg.com/AROWeb/bridge/6209/17939?d=INTL,US>. These outline potential audit considerations and risks for specific geographic markets.

When we audit entities with operations in multiple locations, these summaries can help us understand the local operating environments.

[What is a financial reporting framework?](#) [ISA | 343.7468]

All financial statements are prepared in accordance with a 'financial reporting framework' — i.e. a set of criteria used to determine how material items are measured, recognized, presented and disclosed in the financial statements. Commonly used financial reporting frameworks include US GAAP and IFRS.

[What matters might we consider when obtaining an understanding of the financial reporting framework?](#)

[ISA | 343.7469]

When obtaining an understanding of the entity's applicable financial reporting framework, and how it applies in the context of the nature and circumstances of the entity and its environment we may consider:

- The entity's financial reporting practices in terms of the applicable financial reporting framework, such as:
 - Accounting principles and industry-specific practices, including for industry-specific significant classes of transactions, account balances and related disclosures in the financial statements (for example, loans and investments for banks, or research and development for pharmaceuticals).
 - Revenue recognition.
 - Accounting for financial instruments, including related credit losses.
 - Foreign currency assets, liabilities and transactions.
 - Accounting for unusual or complex transactions including those in controversial or emerging areas (for example, accounting for cryptocurrency).
- Other accounting rules, regulations and guidance that may apply. For example:
 - Entities in the banking industry may follow other regulatory reporting requirements specific to the jurisdiction in which the entity operates.
 - Entities filing with the SEC also follow SEC rules, regulations and interpretative guidance.

[What information might help us understand the industry, regulatory and other external factors?](#) [ISA |

343.1600]

The table below sets out examples of information we may gather as we obtain our understanding of the relevant industry, regulatory and other external factors.

Type of understanding	Examples of information we may gather
Industry, including competitive environment and technological developments	<ul style="list-style-type: none"> • The entity's competitive environment, including demand, capacity and price competition. For example, the entity may operate in an industry populated with aggressively

	<p>growth-focused start-ups, putting pressure on pricing and margins.</p> <ul style="list-style-type: none"> Highly cyclical or seasonal activity in the entity's industry. For example, entities in the retail industry may see higher sales during holiday seasons. Technological developments. For example, rapid technological changes may make the entity's products obsolete. Energy supplies and costs. For example, volatile fuel prices or disruptions in fuel supplies could affect the operations and financial results of a commercial airline.
Regulatory environment, including applicable financial reporting framework and legal and political environment	<ul style="list-style-type: none"> Applicable financial reporting framework (e.g., US GAAP, IFRS), as well as specific industry practices and changes in accounting standards that are relevant to the entity. Government legislation, regulation or policies. For example, the entity may receive government aid, or be subject to foreign exchange controls, fiscal tariffs or trade restrictions. Tax and environmental laws. For example, the entity may be subject to complex tax laws in multiple tax jurisdictions.
External factors, including general economic conditions	<ul style="list-style-type: none"> Changes in general economic conditions or interest rates. For example, the entity may operate in an inflationary environment or economy in recession. Volatile commodity prices. For example, fluctuating oil prices could affect the operations and financial results of an oil and gas company. Lack of available capital in the marketplace. For example, the entity may have to refinance debt in the next 12 months in a public market with very limited liquidity.

2 Understand the nature of the entity [ISA | 344]

What do we do?

Obtain an understanding of the nature of the entity, including understanding certain specific elements.

Why do we do this?

Risks can arise not only from external factors but also from entity-specific conditions. These include:

- the entity's defining characteristics;
- how the entity conducts business, including its business model; and
- how the entity is organized.

Understanding the nature of the entity can help us identify potential risks of material misstatement (RMMs) in the financial statements.

Execute the Audit

[What do we consider when understanding the nature of the entity?](#) [ISA | 344.1300]

Obtaining an understanding of certain specific elements of the business model can help us understand the nature of the entity overall. These include the entity's:

- organizational structure and management personnel, including ownership and governance structure, including the extent to which the business model integrates the use of IT;
- sources of funding for operations and investment activities, including its capital structure, non-capital funding - e.g. subordinated debt, dependencies on supplier financing - and other debt instruments;
- significant investments, including equity method investments, joint ventures, special-purpose entities and variable-interest entities;
- operating characteristics, including its size and complexity, which might affect the risks of misstatement (RMs) and how the entity addresses those risks;
- sources of earnings, including the relative profitability of key products and services; and
- key supplier and customer relationships.

Our goal in gathering this information is to obtain information that helps us identify and assess risk. We do not gather a detailed history of the entity - e.g. the period in which it was founded - unless we expect that information could lead us to identify RMMs.

[What are examples for each of the specific elements?](#) [ISA | 344.7474]

Obtaining an understanding of certain specific elements can help us understand the nature of the entity overall.

The table below sets out examples for each of the specific elements.

Elements	Examples
Organizational structure and management personnel, including ownership and governance	<ul style="list-style-type: none"> • The scope of the entity's activities, and why it does them. • The entity's structure and scale of its operations. • Whether the entity operates in multiple locations with multiple management levels. Complex structures may give rise to RMMs. For example, there may be RMMs related to accounting for goodwill, joint ventures, investments and special-purpose entities. • Relationships between owners and other people or entities. For example, this information helps determine whether related-party transactions were appropriately identified, accounted for and disclosed in the financial statements.

	<ul style="list-style-type: none"> Few owners with significant ownership interests and seats on the board of directors. Publicly traded and thus owned by many shareholders. In some cases, some or all of those charged with governance may be involved in managing the entity. In other cases, those charged with governance and management may comprise different persons. Governance of the entity may be the collective responsibility of a governing body - e.g. board of directors, supervisory board, partners, trustees, equivalent persons. In smaller entities, one person may be charged with governance, such as an owner-manager or sole trustee.
Sources of funding for operations and investment activities, including capital structure, non-capital funding, and other debt instruments	<ul style="list-style-type: none"> Relies on debt financing involving complex debt covenants. Has significant off-balance sheet financing or leasing arrangements. The entity's capital structure - i.e. proportion of debt versus equity - may have changed from prior periods. Uses derivative financial instruments. The entity may have subsidiaries and associated entities, including consolidated and unconsolidated structures. The beneficial owners may be local or foreign, with or without appropriate business reputation and experience. Obtained financing from a related party. Using newly created digital assets to raise capital in the form of an ICO (initial coin offering).
Significant investments, including equity method investments, joint ventures special-purpose entities and variable-interest entities	<ul style="list-style-type: none"> Significant equity method investments or consolidated SPEs or VIEs, including some with a limited or specific purpose. Holds cryptocurrencies or digital assets as investments for long-term capital appreciation or as a means of exchange during normal operations. Has or plan to make non-recurring acquisitions or divestitures, which may count as significant unusual transactions. Plans to carry out substantial research and development, or make capital expenditures. Investments and dispositions of securities and loans.
Operating characteristics, including size and complexity	<ul style="list-style-type: none"> The entity may be large and complex, operating in several markets and geographic locations. Operates some business segments centrally and others de-centrally. How the entity's business model integrates the use of IT in its interactions with customers, suppliers, lenders and other stakeholders through IT interfaces and other technologies. Uses multiple, distinct IT systems in its business processes. Nature of revenue sources, products or services, and markets.

	<ul style="list-style-type: none"> • Extent of integration of electronic commerce into the entity's operations, for example, in Internet sales and marketing activities. • Conduct of operations (for example, stages and methods of production, or activities exposed to environmental risks). • Alliances, joint ventures, and outsourcing activities. • Geographic dispersion and industry segmentation. • Location of production facilities, warehouses, and offices, and location and quantities of inventories. • Key customers and important suppliers of goods and services, employment arrangements (including the existence of union contracts, pension and other post-employment benefits, stock option or incentive bonus arrangements, and government regulation related to employment matters). • Research and development activities and expenditures. • Transactions with related parties.
Sources of earnings, including relative profitability of key products and services	<ul style="list-style-type: none"> • One profitable revenue stream and others that are near break-even or making losses. • Earns a significant net income from non-operating activities.
Key supplier and customer relationships	<ul style="list-style-type: none"> • Depends on only a few suppliers for its main income-earning activities. • Sells specialized products and services to only a few key customers. • Key supplier may have recently filed for bankruptcy.

What sources of information can help us understand the nature of the entity? [ISA | 344.1400]

We can use the [common sources of information](#) related to understanding the entity and its environment.

How does the organizational structure and physical locations of the entity factor into our understanding of the nature of the entity? [ISA | 344.11456]

We understand the organizational structure of the entity in order to better understand how the entity's physical and geographic locations and presence can generate risks of material misstatement. The information also helps us determine whether the audit represents a group audit or multi-location audit, and how to best organize the audit to address the risks rising from the entity's locations and / or components.

Why does the governance of the entity factor into our understanding of the nature of the entity? [ISA | 344.7471]

We understand the governance of the entity in order to better understand the entity's ability to provide appropriate oversight of its system of internal control. However, this understanding may also provide

evidence of deficiencies, which may indicate an increase in the susceptibility of the entity's financial statements to risks of material misstatement.

[What is a business model?](#) [ISA | 344.7487]

An entity's business model describes how an entity considers, for example its organizational structure, operations or scope of activities, business lines (including competitors and customers of the business lines), processes, growth opportunities, globalization, regulatory requirements and technologies. The entity's business model describes how the entity creates, preserves and captures financial or broader value, for its stakeholders.

[Why does the entity's business model factor into our understanding of the nature of the entity?](#) [ISA | 344.7472]

Understanding the entity's objectives, strategy and business model helps us to understand the entity at a strategic level, and to understand the business risks the entity takes and faces. An understanding of the business risks that have an effect on the financial statements assists us in identifying risks of material misstatement, since most business risks will eventually have financial consequences and, therefore, an effect on the financial statements.

For example, an entity's business model may rely on the use of IT in different ways -

- the entity sells shoes from a physical store, and uses an advanced stock and point of sale system to record the selling of shoes; or
- the entity sells shoes online so that all sales transactions are processed in an IT environment, including initiation of the transactions through a website.

For both of these entities the business risks arising from a significantly different business model would be substantially different, even though both entities sell shoes.

See '[Understand the entity's objectives, strategies and related business risks](#)' for more information.

[What if the entity has invested in special purpose entities \(SPEs\) or variable-interest entities \(VIEs\)?](#) [ISA | 344.1500]

Financial reporting frameworks often set conditions that are deemed to amount to control or circumstances for consolidating an SPE or VIE. The frameworks may also set different bases for recognizing income from them. To interpret these requirements, we often obtain a detailed knowledge of the agreements involving the SPE or VIE.

[What may we understand about how the entity integrates IT into the business model?](#) [ISA | 344.8074]

Our understanding may include the extent and automation of electronic communication with third parties including customers, suppliers, and governments. Additionally, we may understand the extent of use of cryptocurrencies and digital assets including blockchain.

[What are cryptocurrencies and digital assets?](#) [ISA | 344.8080]

A digital asset, in the context of currency and finance, is characterized by its ability to be used for a variety of purposes, including as a means of exchange, as a representation to provide or access goods or services, or as a financing vehicle, such as a security, among other uses. The terms crypto asset and cryptocurrency refer to a type of digital asset that uses cryptography to secure transactions digitally recorded on a distributed ledger (such as a blockchain) and purports to be an item of inherent

value (similar, for instance, to real assets like gold or virtual assets) that are designed to enable purchases, sales, barter or other financial transactions.

Blockchain is a distributed ledger technology that records a list of records, referred to as blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp and transaction data. A block is a collection of digital asset transactions to be recorded on a blockchain.

Virtual currencies, tokens and coins may entitle the holder to other rights as well, such as rights to goods or services from the issuer of the token or a right to financial distributions from the issuing entity or the right to virtual digital assets.

Blockchains, virtual currencies, tokens, and virtual coins may be fully decentralized (i.e. they are not associated with a particular individual or organization), or they may be associated with a particular backing organization (or several organizations in a consortium). In certain cases, whether backed by a traditional organization or not, such digital assets may be considered as being securities.

[What may we understand about the extent of use of cryptocurrencies and digital assets?](#) [ISA | 344.8089]

Addressing certain considerations can be helpful when identifying and assessing risks of misstatement related to cryptocurrency and digital assets when an entity transacts or invests in cryptocurrency and digital assets. These may include:

- What is the purpose or strategy for transacting in digital assets and how do those strategies align with the nature of the entity (e.g. operating characteristics, key performance indicators, sources of earnings, etc.)? Are there associated business risks related to digital asset transactions? What is the entity's underlying business and how do the digital assets relate to the entity's business model?
- Are digital asset transactions intended to be used as a source of funding for the entity's operations (e.g. an initial coin offering or "ICO")? Does the entity keep certain digital assets off the balance sheet?
- What are the relevant legal and regulatory requirements governing the entity's use of digital assets? For example, sales of digital assets (e.g. in an ICO), may represent sales of securities subject to jurisdictional regulations and securities laws. Entities that buy and sell digital assets for others may be subject to other laws and regulations, such as money transmitter rules, 'Anti-Money Laundering' and 'Know Your Customer' considerations. Has the entity considered laws and regulations over digital assets and ICOs in other countries and jurisdictions?
- Does the entity use a third-party exchange or service provider to transact digital assets? Has the entity evaluated whether any of the digital assets it holds or transacts (directly or indirectly through a third-party exchange or servicer) are appropriately registered with securities regulators? Does the entity use exchanges that are appropriately registered based on the nature of the digital assets?
- Has the entity identified relevant regulatory frameworks and compliance requirements (i.e. Bank Secrecy Act 'BCA' or Foreign Account Tax Compliance Act 'FATCA', federal securities laws, depository and/or custodial regulations)? What policies and procedures are in place related to compliance with regulatory frameworks?
- Do the digital assets carry specific rights and obligations including rights to cash flows, ownership characteristics, or utility/discount rights?

- What are the entity's accounting policies related to digital assets, including related disclosures? Has the entity evaluated alternative accounting literature and treatments that could apply to its facts and circumstances? Do accounting and finance personnel have the appropriate knowledge and understanding of the digital asset transactions and how to apply existing accounting policies or principles?
- For subsequent measurements associated with digital assets (e.g., when measuring an impairment of a cryptocurrency investment), how does the entity determine the principal market? For example, some digital assets are listed on multiple exchanges while others are not listed on any exchange and as such an entity may have to employ different methods to subsequently measure these assets in an environment where there may be limited trading history and significant volatility for the asset.
- Are the digital assets held by the entity more common (e.g. Bitcoin, litecoin, XRP, Ether), less common, or emerging? Less common or emerging digital assets are likely to carry additional risks resulting in additional considerations.
- Does the entity offer new products or services to customers that incorporate digital assets (e.g. new investment funds)? How do these products or services differ from the entity's existing product and service lines? Is the entity holding onto the digital assets from a speculative perspective or obtaining the assets through a form of payment related to its primary business? Is the entity consistently trading the digital assets or buying and holding?
- Has the entity considered potential risks associated with the IT requirements to transact in digital assets and compatibility with existing systems? If so, has the entity identified and implemented appropriate policies and procedures to address these potential IT risks?

[What other considerations exist regarding cryptocurrencies and digital assets?](#) [ISA | 344.11457]

Blockchain, distributed ledger technologies, and associated 'digital assets' (e.g. cryptocurrencies, tokens, and coins) can raise a number of auditing, accounting, and financial reporting considerations. Where cryptocurrencies and digital assets are significant to the financial statements, we consider the consultation requirements in the [Global Quality and Risk Management Manual section 9.1.4.](#) <https://www.gqrmm-prod.kworld.kpmg.com/G/0/Content/81?jm=82-policy-23021>

3 Understand the entity's objectives, strategies and related business risks

[ISA | 347]

What do we do?

Obtain an understanding of the entity's objectives, strategies and related business risks.

Why do we do this?

Industry, regulatory and other internal and external factors set the context for the entity's business. In response to these factors, the entity's management or those charged with governance define overall plans, or 'objectives', for the entity. 'Strategies' are the approaches that management plans to take to achieve these objectives. Strategies and objectives may change over time as internal and external forces evolve.

Even with the best intentions and well-reasoned decisions, objectives and strategies may not lead to the expected outcomes, resulting in business risks with financial consequences. Understanding the business risks facing the entity can help us identify risks of material misstatement (RMMs).

Execute the Audit

What sources of information can help us understand the entity's objectives, strategies and related business risks? [ISA | 347.1300]

We may have already obtained information relevant to understanding the entity's objectives, strategies and business risks when we performed other procedures to understand the entity and its environment, including its internal controls.

We can also obtain information to help us understand the entity's objectives, strategies and related business risks by:

- considering the [common sources of information](#) that we use to understand the entity and its environment; and
- reviewing the entity's enterprise risk assessment — i.e. its process to assess risks and opportunities related to achieving its objectives.

The risks identified through an enterprise risk assessment and discussed with those charged with governance (often in the form of a heat map) may result in risks of misstatement (RMs).

What are business risks? [ISA | 347.1400]

Business risks are risks that threaten an entity's ability to generate profits or to meet its goals. They generally comprise any factors that may contribute towards business failure — such as loss of customers, increase in production costs, decline in product demand, increase in market competition etc.

Business risks may arise from change or complexity, or from failing to see a need for change. For example, a business risk may arise from:

- developing new products or services that may fail;
- developing a market that may be inadequate to support a product or service;
- developing a flawed product or service that may lead to liabilities and reputational risk;
- new entrant to the market increases competition and lowers margins;
- new technology causes disruption and loss of market share; or
- changes in laws and regulations increase costs of doing business, making some business lines significantly less profitable.

What is the difference between a business risk and an RMM? [ISA | 347.1500]

Business risks can give rise to RMMs — especially financial statement-level RMMs, which may have a more pervasive impact.

However, not all business risks result in RMMs. In fact, some business risks may relate purely to the operations of the business and may not result in misstatement of the financial statements.

Do we obtain an understanding of all the business risks facing the entity? [ISA | 347.1600]

No. We are not responsible for identifying and assessing all business risks because not all business risks give rise to risks of material misstatement.

When we understand the entity's objectives and strategies, we consider whether there are related business risks that may give rise to a risk of material misstatement.

[How can business risks affect the financial statements?](#) [ISA | 347.1700]

Business risks can affect financial statements in a variety of ways. Their effects may be immediate or long-term, and impacts may arise at the financial statement level or assertion level. For example:

- the business risk from a shrinking customer base in a consolidating industry may raise an RM for valuations of accounts receivable and inventory that have become obsolete (immediate assertion-level RM); or
- the business risk of a decline in the entity's industry may affect the entity's ability to continue as a going concern (long-term financial statement-level RM)

Examples

[In what situations might business risks lead to RMMs?](#) [ISA | 347.1800]

The table below sets out examples of matters we may consider when obtaining an understanding of the entity's objectives, strategies and related business risks that may result in RMMs.

Situation	Examples of related business risk
Industry developments	The entity does not have the personnel or expertise to deal with a change in the industry.
New products and services	A newly introduced product or service may expose the entity to liability, and/or the new product or service may not succeed.
Changes in supply chain	Changes in the supply chain may impact the profitability of the entity's products. Disruptions in the supply chain may impact the entity's ability to fulfill customer orders.
Use of information technology (IT)	Some of the entity's systems and processes may be incompatible. New IT systems may not be implemented properly and/or migrated data may not be complete and accurate. There may be inconsistencies between the entity's IT strategy and its business strategies.

New accounting requirements	A new accounting requirement may not be implemented properly or completely, or the requirement may increase costs.
Expansion of the business	The demand for the entity's products or services may not have been accurately estimated.
Effects of implementing a strategy, particularly effects that lead to new accounting requirements	The strategy may not be implemented properly or completely.
Current and prospective financing requirements	The entity's inability to meet financing requirements may lead to a loss of financing.
Regulatory requirements	Regulatory requirements may increase the entity's legal exposure.

4 Understand the entity's measurement and analysis of its financial performance [ISA | 348]

What do we do?

Obtain an understanding of the entity's measurement and analysis of its financial performance.

Why do we do this?

Management and external stakeholders measure and review what they consider important. Performance measures, whether external or internal, create pressures for the entity. In turn, these pressures may prompt management action to improve business performance or misstate the financial statements.

Gathering information about how the entity, analysts, investors and rating agencies measure and analyze the entity's financial performance helps us understand financial statement line items that may pose greater risk of material misstatement. This understanding may help us identify accounts that may be open to manipulation, as well as accounts that the entity uses to monitor its operations.

Execute the Audit

How do we understand how the entity measures and analyzes its financial performance? [ISA | 348.1300]

We first identify the performance measures the entity considers most relevant and the measures the entity or external parties actively track.

We may have already identified some performance measures when understanding:

- [the relevant factors and metrics used to establish materiality for the financial statements](#); and
- [the nature of the entity](#).

Considering the [common sources of information](#) that we use to understand the entity and its environment may also reveal performance measures we have not already identified, or help us better understand how using performance measures we have identified may affect the identification and assessment of risks of material misstatement (RMMs).

In essence, we are searching the information produced by the entity, analysts, investors, rating agencies and others to identify the specific financial and other metrics they focus on in their reports.

Lastly, inquiries of management may reveal that it relies on certain key indicators, whether publicly available or not, for evaluating financial performance and taking action.

[How can we use our understanding to identify and assess risks?](#) [ISA | 348.1400]

Once we've identified the relevant performance measures, we may further seek to understand the following factors for each identified relevant performance measure:

- How aggressively are targets for each performance measure set by management?
- Does the entity have a history of achieving the set targets?
- How significantly is the management compensation linked to each performance measure?
- How are the performance measures defined?

The first three factors can help us gauge the importance of each performance measure to the entity and management, which may influence our assessment of risks of material misstatement connected to these performance measures.

Performance measures may also help us identify risks of misstatement. For example, understanding certain performance measures may indicate that the entity has unusually rapid growth or profitability when compared to that of other entities in the same industry. Such information, particularly if combined with other factors such as performance-based bonus or incentive remuneration, may indicate a potential risk of management bias in the preparation of the financial statements or possible fraud risk.

The last factor on understanding how the performance measure is defined, helps us identify specific accounts or disclosures that may create a greater risk of material misstatement from error or fraud.

For example, when the entity and its investors and analysts use adjusted EBITDA as a relevant performance measure, we may obtain an understanding of how adjusted EBITDA is calculated and which accounts are included in the calculation.

Inspecting information about the entity's performance measures may also help us to identify items to focus on in our analytical reviews. We may identify unexpected results or trends that could indicate greater risk of material misstatement from error or fraud. For example, revenue growth that is unusually rapid compared to other entities in the same industry may indicate a potential risk of management bias in financial statement preparation — particularly when combined with other factors, such as performance-based bonus or incentive remuneration.

[Can an entity's performance measures include non-GAAP measures?](#) [ISA | 348.1500]

Yes. An entity's performance measures may and often do include both GAAP and non-GAAP measures. Commonly used non-GAAP performance measures include EBITDA and adjusted EBITDA, as well as net income, cash flow from operations, and other key financial ratios.

How may our procedures to understand the entity's performance measures differ depending on its size or complexity? [ISA | 348.7475]

Our procedures undertaken to understand the entity's performance measures may vary depending on the size or complexity of the entity, as well as the involvement of owners or those charged with governance in the management of the entity.

For some less complex entities, it may only be the terms of the entity's bank borrowings (i.e., bank covenants) that are linked to specific performance measures related to the entity's performance or financial position (e.g., a maximum working capital amount).

Whereas, for some entities whose nature and circumstances are more complex, such as those operating in the insurance or banking industries, performance or financial position may also be measured against regulatory requirements (e.g., regulatory ratio requirements such as capital adequacy and liquidity ratios performance hurdles).

Our understanding of these performance measures may help identify areas where there is increased susceptibility to the risk of material misstatement.

Examples

What performance measures might an entity use? [ISA | 348.1600]

The table below sets out examples of performance measures an entity may use that may be relevant to our risk assessment.

Where and how performance measures may be used	Examples of performance measures
As the basis for contractual commitments or incentive compensation arrangements	<ul style="list-style-type: none"> Financial measures - e.g. revenue, net income, EBITDA Period-on-period financial performance analyses Industry-specific financial measures - e.g. Funds from Operations for real estate investment trusts, same-store sales for retailers Non-financial measures - e.g. number of subscribers or users Common ratios in loan agreements - e.g. debt-to-equity, interest coverage Growth rates in financial and non-financial measures
By external parties - e.g. analysts, rating agencies - to review the entity's performance	
By the entity, to monitor its operations that may also	<ul style="list-style-type: none"> Ratios — e.g. accounts receivable and inventory turnover

highlight unexpected results and trends that management investigates and corrects, including correction of misstatements	<ul style="list-style-type: none"> • Specific categories of operating expenses • Comparisons to budgets or forecasts • Segment or divisional operating results • Comparisons to competitors' operating results • Employee performance measures and incentive compensation policies
---	---

Understanding Inherent Risk Factors

International Standards on Auditing: ISA 315.Appendix 2

Appendix 2 Understanding Inherent Risk Factors

(Ref: Para. 12(f), 19(c), A7.A8, A85.A89)

This appendix provides further explanation about the inherent risk factors, as well as matters that the auditor may consider in understanding and applying the inherent risk factors in identifying and assessing the risks of material misstatement at the assertion level.

The Inherent Risk Factors

1. Inherent risk factors are characteristics of events or conditions that affect susceptibility of an assertion about a class of transactions, account balance or disclosure, to misstatement, whether due to fraud or error, and before consideration of controls. Such factors may be qualitative or quantitative, and include complexity, subjectivity, change, uncertainty or susceptibility to misstatement due to management bias or other fraud risk factors⁷¹ insofar as they affect inherent risk. In obtaining the understanding of the entity and its environment, and the applicable financial reporting framework and the entity's accounting policies, in accordance with paragraphs 19(a).(b), the auditor also understands how inherent risk factors affect susceptibility of assertions to misstatement in the preparation of the financial statements.

⁷¹ ISA 240, paragraphs A24-A27

2. Inherent risk factors relating to the preparation of information required by the applicable financial reporting framework (referred to in this paragraph as "required information") include:

- *Complexity*-arises either from the nature of the information or in the way that the required information is prepared, including when such preparation processes are more inherently difficult to apply. For example, complexity may arise:
 - In calculating supplier rebate provisions because it may be necessary to take into account different commercial terms with many different suppliers, or many interrelated commercial terms that are all relevant in calculating the rebates due; or
 - When there are many potential data sources, with different characteristics used in making an accounting estimate, the processing of that data involves many inter-related steps, and the data is therefore inherently more difficult to identify, capture, access, understand or process.
- *Subjectivity*-arises from inherent limitations in the ability to prepare required information in an objective manner, due to limitations in the availability of knowledge or information, such that

management may need to make an election or subjective judgment about the appropriate approach to take and about the resulting information to include in the financial statements. Because of different approaches to preparing the required information, different outcomes could result from appropriately applying the requirements of the applicable financial reporting framework. As limitations in knowledge or data increase, the subjectivity in the judgments that could be made by reasonably knowledgeable and independent individuals, and the diversity in possible outcomes of those judgments, will also increase.

- *Change*-results from events or conditions that, over time, affect the entity's business or the economic, accounting, regulatory, industry or other aspects of the environment in which it operates, when the effects of those events or conditions are reflected in the required information. Such events or conditions may occur during, or between, financial reporting periods. For example, change may result from developments in the requirements of the applicable financial reporting framework, or in the entity and its business model, or in the environment in which the entity operates. Such change may affect management's assumptions and judgments, including as they relate to management's selection of accounting policies or how accounting estimates are made or related disclosures are determined.
- *Uncertainty*-arises when the required information cannot be prepared based only on sufficiently precise and comprehensive data that is verifiable through direct observation. In these circumstances, an approach may need to be taken that applies the available knowledge to prepare the information using sufficiently precise and comprehensive observable data, to the extent available, and reasonable assumptions supported by the most appropriate available data, when it is not. Constraints on the availability of knowledge or data, which are not within the control of management (subject to cost constraints where applicable) are sources of uncertainty and their effect on the preparation of the required information cannot be eliminated. For example, estimation uncertainty arises when the required monetary amount cannot be determined with precision and the outcome of the estimate is not known before the date the financial statements are finalized.
- *Susceptibility to misstatement due to management bias or other fraud risk factors insofar as they affect inherent risk*-susceptibility to management bias results from conditions that create susceptibility to intentional or unintentional failure by management to maintain neutrality in preparing the information. Management bias is often associated with certain conditions that have the potential to give rise to management not maintaining neutrality in exercising judgment (indicators of potential management bias), which could lead to a material misstatement of the information that would be fraudulent if intentional. Such indicators include incentives or pressures insofar as they affect inherent risk (for example, as a result of motivation to achieve a desired result, such as a desired profit target or capital ratio), and opportunity, not to maintain neutrality. Factors relevant to the susceptibility to misstatement due to fraud in the form of fraudulent financial reporting or misappropriation of assets are described in paragraphs A1 to A5 of ISA 240.

3. When complexity is an inherent risk factor, there may be an inherent need for more complex processes in preparing the information, and such processes may be inherently more difficult to apply. As a result, applying them may require specialized skills or knowledge, and may require the use of a management's expert.

4. When management judgment is more subjective, the susceptibility to misstatement due to management bias, whether unintentional or intentional, may also increase. For example, significant management judgment may be involved in making accounting estimates that have been identified as having high estimation uncertainty, and conclusions regarding methods, data and assumptions may reflect unintentional or intentional management bias.

Examples of Events or Conditions that May Give Rise to the Existence of Risks of Material Misstatement

5. The following are examples of events (including transactions) and conditions that may indicate the existence of risks of material misstatement in the financial statements, at the financial statement level or the assertion level. The examples provided by inherent risk factor cover a broad range of events and conditions; however, not all events and conditions are relevant to every audit engagement and the list of examples is not necessarily complete. The events and conditions have been categorized by the inherent risk factor that may have the greatest effect in the circumstances. Importantly, due to the interrelationships among inherent risk factors, the example events and conditions also are likely to be subject to, or affected by, other inherent risk factors to varying degrees.

Relevant Inherent Risk Factor:	Examples of Events or Conditions That May Indicate the Existence of Risks of Material Misstatement at the Assertion Level
Complexity	<p>Regulatory:</p> <ul style="list-style-type: none"> Operations that are subject to a high degree of complex regulation. <p>Business model:</p> <ul style="list-style-type: none"> The existence of complex alliances and joint ventures. <p>Applicable financial reporting framework:</p> <ul style="list-style-type: none"> Accounting measurements that involve complex processes. <p>Transactions:</p> <ul style="list-style-type: none"> Use of off-balance sheet finance, special-purpose entities, and other complex financing arrangements.
Subjectivity	<p>Applicable financial reporting framework:</p> <ul style="list-style-type: none"> A wide range of possible measurement criteria of an accounting estimate. For example, management's recognition of depreciation or construction income and expenses. Management's selection of a valuation technique or model for a non-current asset, such as investment properties.
Change	Economic conditions:

	<ul style="list-style-type: none"> Operations in regions that are economically unstable, for example, countries with significant currency devaluation or highly inflationary economies. <p>Markets:</p> <ul style="list-style-type: none"> Operations exposed to volatile markets, for example, futures trading. <p>Customer loss:</p> <ul style="list-style-type: none"> Going concern and liquidity issues including loss of significant customers. <p>Industry model:</p> <ul style="list-style-type: none"> Changes in the industry in which the entity operates. <p>Business model:</p> <ul style="list-style-type: none"> Changes in the supply chain. Developing or offering new products or services, or moving into new lines of business. <p>Geography:</p> <ul style="list-style-type: none"> Expanding into new locations. <p>Entity structure:</p> <ul style="list-style-type: none"> Changes in the entity such as large acquisitions or reorganizations or other unusual events. Entities or business segments likely to be sold. <p>Human resources competence:</p> <ul style="list-style-type: none"> Changes in key personnel including departure of key executives. <p>IT:</p> <ul style="list-style-type: none"> Changes in the IT environment. Installation of significant new IT systems related to financial reporting. <p>Applicable financial reporting framework:</p> <ul style="list-style-type: none"> Application of new accounting pronouncements. <p>Capital:</p> <ul style="list-style-type: none"> New constraints on the availability of capital and credit. <p>Regulatory:</p> <ul style="list-style-type: none"> Inception of investigations into the entity's operations or financial results by regulatory or government bodies. Impact of new legislation related to environmental protection.
Uncertainty	Reporting:

	<ul style="list-style-type: none"> Events or transactions that involve significant measurement uncertainty, including accounting estimates, and related disclosures. Pending litigation and contingent liabilities, for example, sales warranties, financial guarantees and environmental remediation.
Susceptibility to misstatement due to management bias or other fraud risk factors insofar as they affect inherent risk	<p>Reporting:</p> <ul style="list-style-type: none"> Opportunities for management and employees to engage in fraudulent financial reporting, including omission, or obscuring, of significant information in disclosures. <p>Transactions:</p> <ul style="list-style-type: none"> Significant transactions with related parties. Significant amount of non-routine or non-systematic transactions including intercompany transactions and large revenue transactions at period end. Transactions that are recorded based on management's intent, for example, debt refinancing, assets to be sold and classification of marketable securities.

Other events or conditions that may indicate risks of material misstatement at the financial statement level:

- Lack of personnel with appropriate accounting and financial reporting skills.
- Control deficiencies - particularly in the control environment, risk assessment process and process for monitoring, and especially those not addressed by management.
- Past misstatements, history of errors or a significant amount of adjustments at period end.

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Assess likelihood and magnitude of potential misstatements to determine RMMs [ISA | 565]

What do we do?

Assess the likelihood and magnitude of potential misstatements, including the possibility of multiple misstatements, to determine RMMs and inherent risk

Why do we do this?

We assess the likelihood and magnitude of potential misstatements to:

- Identify risks of material misstatements (RMMs);
- Determine where on the continuum of inherent risk the RMM sits (which informs our design of further audit procedures to respond to the RMM); and

- Assist in the determination of significant risks.

Execute the Audit

Where are we in our risk assessment? [ISA | 565.1300]

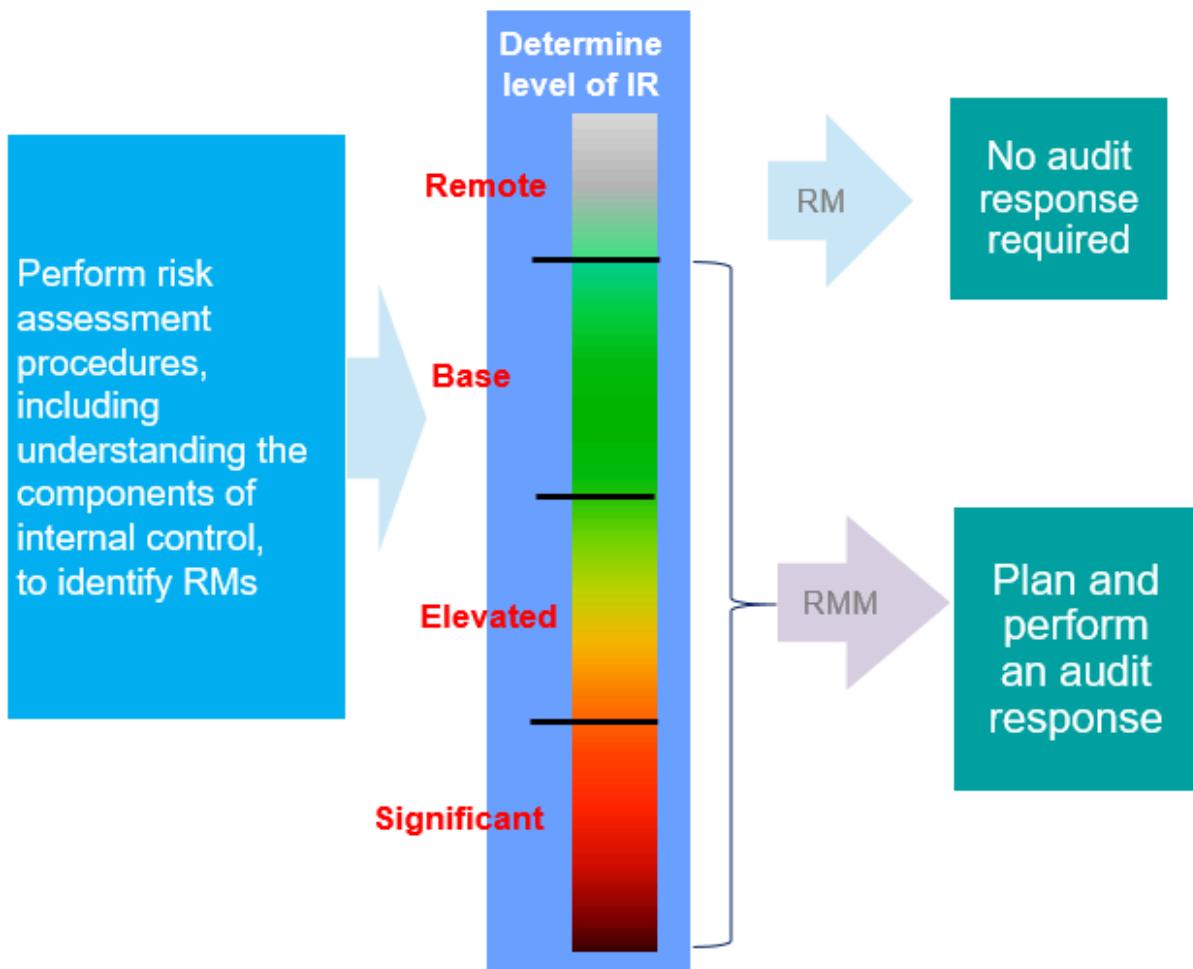


How does assessing likelihood and magnitude of potential misstatements help us determine RMMs and level of inherent risk? [ISA | 565.8701]

Assessing the likelihood and magnitude of potential misstatements helps us gauge where we are on the inherent risk continuum and whether we've reached the level where inherent risk is more than remote for that risk. An RM is simply a risk on the "remote" part of the inherent risk continuum, where no audit response is necessary*.

When the likelihood and magnitude of potential misstatement is more than remote, we assess inherent risk for each RMM at one of three levels - Base, Elevated or Significant, depending on where it is on the continuum (significant risks are closer to the upper end of the continuum).

The following diagram illustrates the inherent risk continuum and how we think about RMs, RMMs and our inherent risk assessment in relation to that continuum:



Not assessing a risk as an RMM has ramifications — it means we don't address it further in our audit*.

* There are certain areas within the financial reporting process where procedures are always performed even if there is no RMM (e.g. disclosures: agree/reconcile information in the disclosure to the underlying accounting records).

How do internal controls affect our assessment of likelihood and magnitude? [ISA | 565.1700]

We don't consider the effects of control activities when we determine which risks are RMMs.

Our understanding of CERAMIC, however, can influence our assessment of inherent risk. When there are deficiencies in CERAMIC, it may highlight an increased chance of material misstatements occurring. For example, when we identify deficiencies related to the entity's ability to attract, develop, and retain competent individuals, there is a higher likelihood of misstatements occurring broadly because unqualified or lower competence individuals are more prone to record transactions incorrectly.

How do we assess likelihood and magnitude? [ISA | 565.8704]

The table below sets out examples of how an engagement team might assess likelihood and magnitude when they determine RMMs and level of inherent risk.

Description of RM and related accounts / disclosures and assertions	Considerations related to likelihood and magnitude of potential misstatement	Assessment of RMM and level of inherent risk
Prepayments are not accurately recorded or do not exist. (Existence of prepaid expenses)	<ul style="list-style-type: none"> • The size of the prepaid expenses account is less than two times performance materiality and has not changed significantly from the prior year, which is consistent with our expectations. • The account comprises a small number of routine prepayments to vendors for materials that the entity expects to consume within 12 months. • The individual balances are homogeneous and not subject to accounting complexities. • There is no risk of aggregation with other non-significant accounts. 	<p>Although the engagement team has identified an RM, they assess that the likelihood and magnitude that a material misstatement may occur is remote given the low number and dollar value of transactions and lack of accounting complexity associated with the risk.</p> <p>The engagement team assess the risk as not an RMM.</p>
Indicators that an asset or cash-generating unit may be impaired are not appropriately identified. (Valuation of PP&E)	<ul style="list-style-type: none"> • The size of the PP&E account is relatively large (40 times performance materiality) and has not changed significantly from the prior year. • All of the PP&E is included within a single long-lived asset group. • The information identified from our inquiries of management indicated no changes in the use of the PP&E. • The favorable interim results of operations reviewed 	<p>Given the more favorable economic conditions and reduced complexity (e.g. not having a significant number of different asset groups), there is a <i>lower</i> likelihood of a material misstatement occurring.</p> <p>However, given the magnitude of the balance of PP&E and susceptibility in recent periods to changes in value, the engagement team concludes that there is still <i>more than a remote</i> chance of a material misstatement occurring.</p>

	<p>in our planning analytical procedures indicate a reduced risk of exposure to losses in this account.</p> <ul style="list-style-type: none"> Asset values have fluctuated in the past and there have been impairments taken in the last three years. 	<p>The engagement team assesses the risk to be an RMM and inherent risk is assessed to be Base.</p>
<p>An inappropriate amount is estimated and recorded for the value of rights of return.</p> <p>Additional risk description: Risk relates to products sold through a new distribution channel. (Existence and Accuracy of revenue and accounts receivable)</p>	<ul style="list-style-type: none"> Based on our risk assessment procedures, we identified that the entity planned to begin selling a new product to resellers in the last quarter of the fiscal year. Previously, the entity had only sold its products directly to end users and these new contracts include unique rights of return. The entity has relatively little experience with product returns and limited data related to these new sales arrangements. Although the product is new, the entity expects its sales volumes to represent approximately 10% of revenue for the year. 	<p>Given the complexity and judgment in determining the estimate for returns, there is an increased chance that a misstatement could occur. Considering the increased likelihood along with the fact that the revenue from the new product is a substantial portion of total revenues, resulting in magnitude of potential misstatement being material, the engagement team concludes that there is more than a remote chance of a material misstatement occurring.</p> <p>The engagement team assesses the risk to be an RMM and considering the degree of complexity in the measurement of the estimate for returns, and the wide range of measurement uncertainty, the inherent risk assessment is Significant.</p>
<p>The disclosure is incomplete, inaccurate, or not fairly presented.</p> <p>Additional risk description: Risk related to the required disclosures of</p>	<ul style="list-style-type: none"> The entity is manufacturer with point-of-sale revenue recognition. Revenue is material to the financial statements and important to its users. There have not been new accounting pronouncements or changes in the entity's accounting policies for 	<p>Given there is no judgment or complexity in the policies, and no changes nor expected changes in the revenue accounting policies disclosures, the engagement team assesses the risk to be an RM.</p>

revenue accounting policies	revenue in the past two years.	
The disclosure is incomplete, inaccurate, or not fairly presented. Additional risk description: Risk relates to the required disclosure of disaggregated revenue amounts. (Presentation of revenue)	<ul style="list-style-type: none"> Revenue is material to the financial statements and important to users of the financial statements. The entity completed an acquisition in the current reporting period, adding a new business line in a geographic region in which the entity has not previously operated. 	<p>Given the magnitude of the balance of revenue and changes in the disclosure from the prior period given the entity's acquisition, the engagement team assesses the risk to be an RMM.</p> <p>As disaggregating revenue amounts does not require judgment, inherent risk is assessed to be Base.</p>

Group Audit | How do we assess RMMs of the group financial statements? [ISA | 565.2200]

As the group auditor, we assess the risks of material misstatement of the group financial statements, whether due to fraud or error, including with respect to the consolidation process by applying the same guidance for assessing RMMs in a stand-alone audit. However, since most assertion-level RMMs of the group financial statements, or group RMMs, will arise in components, we, as the group auditor, will often involve component auditors in risk assessment procedures to assess group RMMs.

Group Audit | Who is responsible for assessing the RMMs of the group financial statements? [ISA | 565.160255]

The lead group auditor takes responsibility for assessing the RMMs of the group financial statements in a group audit.

Group Audit | What does 'take responsibility for' mean? [ISA | 565.160253]

'Take responsibility for' means the lead group auditor may either design and/or perform procedures, tasks, or actions themselves or are permitted to assign the design and/or performance of procedures, tasks or actions to other appropriately skilled or suitably experienced members of the engagement team, including component auditors.

Assigning the design and/or performance of procedures to another member of the engagement team, however, does not relieve the lead group auditor of their responsibility for the overall design and performance of the audit.

Group Audit | Do we assess different RMMs in a group audit? [ISA | 565.11097]

Yes. As the group auditor, we also assess RMMs related to the consolidation process, including sub-consolidations, which are not linked to any specific significant accounts or disclosures. However, we respond to consolidation RMMs similar to assertion-level RMMs (i.e., design substantive procedures and when applicable, identify PRPs and relevant control activities) rather than designing overall responses like we do for financial statement-level RMMs.

Group Audit | Why may RMMs of the group financial statements be assessed differently at components? [ISA | 565.160257]

Examples of when an RMM at the component may be assessed differently than the RMMs of the group financial statements include:

- the component auditor assesses the magnitude of potential misstatements associated with an RMM considering the component performance materiality for the component; however, the potential misstatement to the group financial statements is not considered material or at a magnitude that warrants the same assessment as that at the component; or
- RMMs at the component are identified based on an RMMs that relates to local financial reporting framework which are not RMMs under the financial reporting framework used by the group.

In circumstances where a component auditor has assessed an RMM as either Elevated or Significant that we as the group auditor have not assessed at the same inherent risk level, we document why we consider those RMMs not to be at the same inherent risk level.

For example, suppose that the group auditor has assessed RMMs associated with capitalized software costs as Base because the magnitude to the group financial statements is 2x group performance materiality.

However, a component auditor has assessed RMMs associated with capitalized software costs as Elevated due to the magnitude at the component and the judgment involved in determining the amounts to capitalize. The component auditor communicates this assessment to the group auditor.

The group auditor documents why the RMM is not assessed as Elevated for the group financial statements.

How do we determine whether our assessment of inherent risk for an RMM is Base, Elevated or Significant? [ISA | 565.8705]

In addition to our consideration of inherent risk factors (see question '[What are the inherent risk factors?](#)'), it may be helpful to:

- first determine which risks are closer to the upper end of the inherent risk continuum and are significant risks (see activity '[Determine significant risks](#)'); and
- then assess the remaining risks by evaluating whether they are relatively lower or higher on the inherent risk continuum — i.e. Base or Elevated.

When we are trying to determine whether a risk is Base or Elevated, it may be useful to compare our assessments across non-significant risks.

For example, suppose that:

- the engagement team have assessed risks associated with several smaller and less complex accounts — e.g. prepaid expenses — as Base; and
- they are trying to determine whether a risk associated with a higher-volume, more complex account is Base or Elevated.

The team may find it helpful to consider whether they really believe the lowest level of inherent risk — i.e. Base — makes sense for both types of risks.

Questioning this can help us better determine where the RMM falls on the continuum.

What factors do we consider in assessing likelihood and magnitude and level of inherent risk? [ISA | 565.2000]

We consider:

- Inherent risk factors;
- Significant risk factors (see question '[How do we determine whether any of the identified and assessed RMM are significant risks?](#)'); and
- Estimates risk factors, if applicable (see question '[What are the additional risk factors that we evaluate when identifying significant accounts and disclosures involving accounting estimates?](#)').

We consider each factor for each RM, to gauge whether it is an RMM, and if so where it sits on the inherent risk continuum. When considering these factors, a key consideration is the degree to which the inherent risk factors affect the combination of likelihood of misstatement occurring and magnitude of misstatement. The higher the combination of likelihood and magnitude, the higher the assessment of inherent risk; the lower the combination of likelihood and magnitude, the lower the assessment of inherent risk.

What are the inherent risk factors? [ISA | 565.8706]

The following table describes the inherent risk factors:

Inherent risk factors	Additional description and examples
Factors that affect the susceptibility to misstatement of an assertion about a class of transactions, account balance or disclosure	
<p>Quantitative or qualitative significance, including:</p> <ul style="list-style-type: none"> • Size and composition of the account • Nature of the account or disclosure • Existence of related party transactions in the account • Possibility of significant contingent liabilities arising from the activities reflected in the account or disclosure • Exposure to losses in the account 	<p>Size and composition: As the size of an account increases, so does the potential magnitude of a misstatement in that account or disclosure. Often, this is because in larger account balances, errors that represent a small percentage of the account balance may still exceed materiality. For example, a 2% misstatement in an account that is 60 times materiality exceeds materiality.</p> <p>Understanding the composition of an account helps us evaluate the other factors and determine whether relevant assertions exist for a particular account and whether there is an RMM we haven't yet identified and assessed.</p> <p>For example, if an entity has domestic sales and international sales, the risk for each type may be different. If there are uncertainties about a foreign countries' economic stability, there may be greater risk in their international operations than their domestic operations.</p>

Nature of accounts and disclosures: When we consider the nature, we think about numerous characteristics of an account, disclosure or assertion, including:

- its importance or prominence in the financial statements
- the way it is recorded or presented
- the basic types of transactions that affect it.

These factors, along with others, can affect how likely a material misstatement is to occur for a specific assertion.

For example:

- accrual balances, by their nature, often have more risk of understatement than overstatement
- assertions related to accounting estimates are more likely to contain a material misstatement related to the valuation assertion
- assertion disclosures related to revenue or significant judgments in applying the related revenue accounting policies or principles are important or prominent in the financial statements
- an accounting estimate often involves management making significant judgments about the assumptions to use. These judgments can involve uncertainty, and introduce more potential for human error.

Existence of related party transactions: Related party transactions involve close relationships between parties, so there is more chance that they might involve fraud or be inappropriate, and lack a clear business purpose and not be appropriately disclosed.

These issues may arise because the entity doesn't account for the transaction properly, or because the substance of a related party transaction might be different from its form.

For example, an entity may structure a related party transaction solely to avoid recording and disclosing a liability in the financial statements. The risk to the financial statements increases because the entity and its related parties control both sides of the transaction.

Given this risk, a material misstatement is more likely in an account that includes related party transactions.

Possibility of significant contingent liabilities: The nature of an entity's transactions and business activities could lead to significant contingencies.

For example, selling goods could lead to sales returns or warranty claims on defective products. Or certain fixed assets may exist (such as underground storage tanks containing gasoline) that could lead to asset retirement obligations or environmental liabilities.

Contingent liabilities may be difficult to identify, and judgment may be involved to determine the amount to be recorded or disclosed in the financial statements. Therefore, they may be more likely to contain a material misstatement.

Exposure to losses in the account: The more exposure an account has to losses, the more chance it may contain an error. Factors in the entity's general environment may expose a particular account to losses. We also think about accounts that may have lower recorded balances but a higher exposure to losses.

For example, an entity may record a small legal accrual, but face several lawsuits with potential unfavorable outcomes that expose it to significant losses. This potential for loss may increase the likelihood of material misstatement over the completeness, valuation and presentation assertions for the legal accrual.

Volume of activity, complexity and homogeneity of the individual transactions processed through the account or reflected in the disclosure

Volume : The more transactions processed through a class of transactions, account balance or reflected in a disclosure, the greater the chance that it contains a material misstatement. There is more risk that multiple items could be misstated that could aggregate to a material misstatement.

We consider the volume of transactions in all accounts and disclosures, but we don't dismiss those with smaller balances without carefully considering the volume of transactions.

For example, a cash account may have a zero balance at the period end, but the entity may process a high volume of cash transactions through it during the period. This may be an account with a reasonable possibility of a material misstatement.

Complexity: More complex transactions can suggest more judgment or present a greater opportunity for errors.

	<p>For example, transactions that result from complex calculations often have multiple inputs, each of which may present a possibility for error. Simple calculations with fewer inputs may have a lower chance of error.</p>
	<p>More complex calculations increase the likelihood of material misstatements related to particular assertions — e.g. valuation — of a particular account or disclosure.</p> <p><i>Homogeneity:</i> In certain cases, when transactions are homogeneous, misstatements in one transaction may indicate additional misstatements in others. As such, multiple errors could occur, which could increase the magnitude of any potential misstatement. In this case, the homogeneity may increase the possibility of a material misstatement. Conversely, when transactions lack uniformity in the composition of the items processed in the account or class of transactions may increase susceptibility to misstatement in the related account or disclosure.</p>
Susceptibility to misstatement due to error	<p>Some accounts, disclosures and assertions, by their nature, are more susceptible to misstatement - including those more likely to be affected by human error.</p> <p>This may be due to the types of transactions processed in an account, the nature of the account or disclosure itself, or many other factors.</p> <p>This higher susceptibility to misstatements increases the likelihood that a material misstatement will occur.</p> <p>For example, when substantial doubt about an entity's ability to continue as a going concern is raised but is alleviated by management's plans, the disclosures could be more susceptible to misstatement whether due to error or fraud.</p>
Factors relating to preparation of the information required by the financial reporting framework	
Complexity, including accounting and reporting complexities associated with the account or disclosure	Complexity arises either from the nature of the information or in the way that the required information is prepared, including when such preparation processes are more inherently difficult to apply.

	<p>For example, complexity may arise in calculating supplier rebate provisions because it may be necessary to take into account different commercial terms with many different suppliers, or many interrelated commercial terms that are all relevant in calculating the rebates due.</p> <p>As another example, complexity may arise in developing disclosures for a business combination because several individuals from different departments may be involved and different sources of information from multiple IT systems may be necessary in preparing the disclosures.</p>
	<p>Complex accounting and reporting can often:</p> <ul style="list-style-type: none"> • be more challenging for an entity to evaluate; • involve a greater degree of judgment; and • necessitate a greater degree of skill, knowledge and experience. <p>For example, accounting for income taxes can be complex, especially when an entity operates in multiple jurisdictions.</p>
	<p>Such complexities can make errors or incorrect judgments more prevalent, and increase the likelihood of material misstatement.</p> <p>Complexity may arise from changes in the applicable financial reporting framework that create new disclosure requirements, or changes in the entity's transactions and activities that result in new accounting policies or principles.</p>
Subjectivity (including judgment in the recognition or measurement of financial information related to the risk)	<p>Subjectivity arises from inherent limitations in the ability to prepare necessary information in an objective manner, due to limitations in the availability of knowledge or information, such that management may need to make an election or subjective judgment about the appropriate approach to take and about the resulting information to include in the financial statements.</p> <p>Because of different approaches to preparing the required information, different outcomes could result from appropriately applying the requirements of the applicable financial reporting framework. As limitations in knowledge or data increase, the subjectivity in the judgments that could be made by reasonably knowledgeable and independent individuals, and the diversity in possible outcomes of those judgments, will also increase.</p>

	<p>For example, management's selection of a valuation technique or model for a non-current asset, such as investment properties.</p> <p>Additionally, subjectivity can arise for disclosures that are subjective in relation to their preparation.</p> <p>For example, disclosures related to a lawsuit and related loss contingency could be more susceptible to misstatement given their subjective nature.</p>
<p>Change(s), including changes from the prior period in account/disclosure characteristics</p> <p>Risk relates to recent significant economic, accounting or other developments</p>	<p>Results from events or conditions that, over time, affect the entity's business or the economic, accounting, regulatory, industry or other aspects of the environment in which it operates, when the effects of those events or conditions are reflected in the required information. Such events or conditions may occur during, or between, financial reporting periods.</p> <p>For example, change may result from developments in the requirements of the applicable financial reporting framework, or in the entity and its business model, or in the environment in which the entity operates. Such change may affect management's assumptions and judgments, including as they relate to management's selection of accounting policies or principles or how accounting estimates are made or related disclosures are determined.</p> <p>As another example, rising interest rates may affect management's projected financial information utilized in the valuation of goodwill, including an impact on the discount rates used and projected revenue and expenses. This change in business environment may also have an impact on management's disclosures of judgments applied in performing the annual impairment test.</p>
	<p>Changes from the prior period may indicate that the risks have changed or that entity has entered into new types of transactions with a different risk profile.</p> <p>The more significant the change, the greater the likelihood that a material misstatement could occur.</p>

	<p>For example, an entity may change its mix of investment securities from government treasury securities to private hedge funds - i.e. from Level 1 investments to Level 3 investments.</p> <p>This change involves a new and potentially more complex valuation model. It may increase the likelihood of a material misstatement related to the valuation and presentation assertions.</p>
Uncertainty	<p>Uncertainty arises when the required information cannot be prepared based only on sufficiently precise and comprehensive data that is verifiable through direct observation (e.g. pending litigation).</p> <p>In these circumstances, an approach may need to be taken that applies the available knowledge to prepare the information using sufficiently precise and comprehensive observable data, to the extent available, and reasonable assumptions supported by the most appropriate available data, when it is not. Constraints on the availability of knowledge or data, which are not within the control of management (subject to cost constraints where applicable) are sources of uncertainty and their effect on the preparation of the necessary information cannot be eliminated.</p> <p>For example, estimation uncertainty arises when the required monetary amount cannot be determined with precision and the outcome of the estimate is not known before the date the financial statements are finalized.</p>
Susceptibility to misstatement due to management bias or other fraud risk factors insofar as they affect inherent risk (including significant unusual transactions)	<p>Results from conditions that create susceptibility to intentional or unintentional failure by management to maintain neutrality in preparing the information.</p> <p>For example:</p> <p>Opportunities for management and employees to engage in fraudulent financial reporting, including omission, or obscuring, of significant information in disclosures.</p> <p>Significant amount of non-routine or non-systematic transactions including intercompany transactions and large revenue transactions at period end.</p>

Transactions that are recorded based on management's intent, for example, debt refinancing, assets to be sold and classification of marketable securities.

Management bias is often associated with certain conditions that have the potential to give rise to management not maintaining neutrality in exercising judgment (indicators of potential management bias), which could lead to a material misstatement of the information that would be fraudulent if intentional.

See activity '[Identify fraud risk factors](#)' for additional considerations when considering other fraud risk factors.

We perform risk assessment procedures to obtain an understanding of how these inherent risk factors affect susceptibility of assertions to misstatement and the degree to which they do so, in the preparation of the financial statements in accordance with the applicable financial reporting framework.

It is not expected that an inherent risk factor is selected in the applicable workflow just because it is "relevant", if it does not impact where the risk sits on the inherent risk continuum. For example, where the RM is associated with the transaction (e.g. PPE additions) we would select volume of activity and homogeneity of the transaction, rather than the size and composition of the account as volume of activity and homogeneity factors impact where the risk sits on the inherent risk continuum.

[Will all inherent risk factors be relevant?](#) [ISA | 565.11100]

No. Depending on the specific risk we are assessing, some inherent risk factors may not be relevant or are not impactful to our assessment.

For example, when there are no related party transactions that are associated with a particular risk, that factor is not relevant or important in our assessment.

We focus on the factors that are most relevant to our assessment of whether the risk rises to an RMM and the related level of inherent risk. We also think about the relative significance of each inherent risk factor during our evaluation.

[Does the number of relevant factors impact the level of inherent risk?](#) [ISA | 565.11102]

No. There is not a specific number of factors that are present before something moves from one inherent risk level to another (e.g. base to elevated), because the factors are considered on a continuum and not in a binary manner.

It is often helpful to take a step back and compare the risks aggregated at an account level against other risks from other accounts.

For example, suppose that:

- We have assessed the risks associated with several smaller and less complex accounts, e.g., prepaid expenses, as Base.

- We are trying to determine whether a risk associated with a higher-volume, more complex account is Base or Elevated.

It may be helpful to think about whether the lowest level of inherent risk, (i.e., Base), makes sense for both types of risks.

Furthermore, for a risk to be assessed as higher on the continuum of inherent risk, it does not mean that both the magnitude and likelihood are assessed as high. Rather, it is the intersection of the magnitude and likelihood of the material misstatement on the continuum of inherent risk that will determine whether the assessed inherent risk is higher or lower on the continuum of inherent risk. A higher inherent risk assessment may also arise from different combinations of likelihood and magnitude, for example a higher inherent risk assessment could result from a lower but still reasonable likelihood but a very high magnitude.

[What if the risk is on the threshold between two levels of inherent risk?](#) [ISA | 565.11103]

If, we assess a risk as being on the threshold between two levels of inherent risk — e.g. Base/Elevated or Elevated/Significant — it may be appropriate to 'round up', or pick the higher risk level, documenting our rationale for the decision as part of our assessment of likelihood and magnitude.

Remember: assessing a risk as too low may result in an insufficient audit response and an unacceptable increase in audit risk.

[What if an RMM includes multiple portions of an account balance with varying levels of inherent risk?](#) [ISA | 565.11104]

If this is the case, we may have defined the RMM too broadly. In this situation, it may be appropriate to disaggregate the RMM into separate components that have varying levels of inherent risk and associate a disaggregated RM/RMM to each component. This may mean we create a duplicate RM/RMM. Adding an additional risk description can clarify how the disaggregated RMMs apply to each component.

We then perform our assessment of likelihood and magnitude of potential misstatements for each of the disaggregated RMs we identified. In performing this assessment, we may determine that one or more of the RMs does not rise to the level of an RMM. This concept applies for both accounts and disclosures.

For example, we identify the following RMM: An inappropriate amount is estimated for the net realizable value (NRV) of inventory, or an inaccurate amount is recorded for the lower of cost and NRV.

Raw materials inventory comprises multiple types of raw materials that are subject to different levels of inherent risk - including steel.

If steel prices are volatile, that may increase the risk of steel-based inventory being overvalued.

We assess inherent risk differently for the steel-based raw materials than for the remaining raw materials inventory.

As a result, we break down the risk into two separate risks - one relating to the steel-based raw materials, and the other relating to the remaining raw materials.

This disaggregation leads us to identify and assess one RMM as Significant (the risk relating to steel-based raw materials) and another as Elevated (the risk relating to the remaining raw materials) based on the relevant inherent risk factors.

As another example, we may disaggregate an RM related to the existence of cash and cash equivalent balances between different cash and cash equivalents accounts because management may use them in varying ways in different locations for different purposes (e.g. payroll, accounts payable and expense disbursement, treasury function for interest and dividend receipts, or revenue receipts) and therefore the related inherent risks may vary based on account/location/component because of differing risk profiles.

[What do we do if we have identified the same RMM due to error and due to fraud?](#) [ISA | 565.8702]

If we have identified the same RMM due to error and due to fraud, then we create 2 separate RMMs within the KPMG Clara workflow, and assess them separately. A fraud risk is always a significant risk, but a risk due to error may have a different inherent risk assessment.

We perform procedures to respond to the fraud risk and demonstrate our special audit consideration in response to the related significant risk. These procedures/responses may differ to our response to the RMM due to error (particularly if our CAR assessment is different). By identifying and assessing these RMMs separately, we can appropriately tailor our response to obtain sufficient appropriate audit evidence for both.

[How do we consider whether there is an RMM in aggregate?](#) [ISA | 565.2100]

We assess for each business process and across all business processes if there are any indications that there is an RMM in aggregate within those assertions, transactions, account balances and disclosures that do not have any RMM associated with them. Signs that might indicate that there are reasonable possibilities of RMM in the aggregate include the following:

- identifying multiple risks that relate to the same accounts/disclosures and assertions;
- determining that the combined magnitude of potential misstatements related to the remaining risks is material; or
- identifying multiple risks with similar characteristics, which may indicate several potential misstatements that could aggregate to a material misstatement.

We assess risks in the aggregate in a manner similar to our risk assessment over each risk on an individual basis. That is, when performing this aggregation assessment, we consider the same inherent risk factors (see question '[What factors do we consider in assessing likelihood and magnitude and level of inherent risk?](#)').

When assessing risks in the aggregate across all business processes, we step back and focus on those accounts and disclosures that were not identified as significant and the assertions were not identified as relevant (see question '[How do we identify significant accounts and disclosures and their relevant assertions?](#)').

[What do we do when we have determined that RMs identified represent an RMM when assessed in the aggregate?](#) [ISA | 565.11107]

When we have identified that RMs aggregate to one or more RMMs, we

- change the assessment of RMs to RMMs until the remaining RMs do not aggregate to an RMM, or
- add a custom RMM that identifies the aggregate risk.

[Is there anything we additionally consider when accounting estimates are involved?](#) [ISA | 565.11116]

Yes. We perform the risk assessment procedures related to accounting estimates in the KAEG chapter on estimates (ISA 540, AU-C 540 or AS 2501). We perform certain risk assessment procedures in order to identify and assess RMMs related to accounting estimates, as outlined in '[Perform risk assessment procedures related to accounting estimates](#)'.

[Is there anything additional we consider when the financial reporting process is involved?](#) [ISA | 565.6463]

Yes. 'Risk considerations' are used when available, within the financial reporting process screens in KPMG Clara workflow - i.e. financial statements, cash flows, segment information, disclosures - and may assist us in:

- identifying the risks of misstatement (RMs);
- determining whether the RMs are risks of material misstatement (RMMs); and/or
- designing appropriate audit responses for those assessed as RMMs.

[How do the 'risk considerations' assist us in determining whether the RMs are RMMs?](#) [ISA | 565.6469]

The 'risk considerations' let us see more clearly the individual items that contribute to the corresponding RMs within the financial reporting process, individually or in combination.

As a result, we can appropriately assess the inherent risk for the RMs, by assessing the likelihood and magnitude of potential misstatements and other relevant factors.

We assess inherent risk at the RM level, not at the risk consideration level.

[How do the 'risk considerations' assist us in designing appropriate audit responses?](#) [ISA | 565.6470]

For each RM we assess as an RMM, we design appropriate audit responses taking into account the more detailed information provided by the 'risk considerations'.

Our response is at the RMM level, not the risk consideration level.

[What do we do with financial statement-level RMs?](#) [ISA | 565.6468]

As with other risks, we assess financial statement-level RMs and determine whether there is a possibility of a material misstatement to the financial statements by considering the likelihood and magnitude of potential misstatements.

When determining whether a financial statement-level RM is an RMM, we also consider whether it affects the assessment of RMMs at the assertion level.

If the financial statement-level RM is an RMM, it affects how we conduct our audit broadly and we design and implement overall responses. See activity '[Design and implement overall responses](#)' for information about overall responses.

[What key success factors might help us in our inherent risk assessment?](#) [ISA | 565.11119]

The table below sets out examples of key success factors that can help us when assessing inherent risk.

Key success factor	How it may help
Timely partner and manager involvement	<p>An effective inherent risk assessment relies on the judgments of the engagement team's most senior members at a sufficiently detailed level early in the audit - especially for risks on the thresholds between Base and Elevated, and Elevated and Significant.</p>
Not being anchored in prior-period inherent risk assessments	<p>We use the information obtained through our risk assessment process to form up-to-date inherent risk assessments based on the current period's factors.</p> <p>Prior-period knowledge is helpful, but we combine it with everything we learn during planning and risk assessment in the current period.</p>
Thinking about inherent risk as a continuum	<p>The inherent risk continuum includes varying levels of risk.</p> <p>Thinking about where each RMM falls on that continuum can help us identify whether an account/disclosure contains components, or groups of transactions, with varying degrees of risk that are subject to different processes and controls.</p> <p>This can help us better identify significant accounts or disclosures.</p>
Paying attention to what's documented in our audit file	<p>Fully capturing how we considered the factors in our inherent risk assessment has several benefits:</p> <p>Our inherent risk assessments involve judgment, and so may warrant more persuasive audit evidence and robust documentation.</p> <p>Documenting the basis for our conclusions demonstrates how we applied professional skepticism.</p> <p>The process of documenting our rationale may lead us to rethink our initial conclusion</p>

	and revisit that assessment when it is not appropriate.
Leveraging management's risk assessment process	Reconciling our inherent risk assessments with management's risk assessments can help us evaluate the effectiveness of management's internal control over financial reporting — i.e. the Risk Assessment component.
Holding risk assessment meetings at the right times	We may hold meetings to discuss risk assessment throughout the audit - not just during planning and before issuing the audit opinion. The best ideas may come when we ask people to invest time thinking about risk assessment before these meetings. Risk Assessment and Planning Discussion (RAPD) meetings provide excellent opportunities to discuss risks holistically - but to be most effective, we plan and conduct these at the right times.
Completion of an Accounting Disclosure Checklist (ADC)	Completion of relevant sections of an ADC during risk assessment in connection with each business process assists in understanding disclosures to be expected for the process. The prior period financial statements and related disclosures, and previously completed ADC combined with current year activity, changes within existing business processes and events and circumstances that may require disclosures, all while being mindful to take a 'fresh lens' approach, assists in assessing inherent risk.

Examples

How do we consider the inherent risk factors when assessing RMs around disclosures? [ISA | 565.159465]

Below are examples of how an engagement team considers the inherent risk factors when assessing RMs around disclosures.

Fact Pattern:

RM	Initial risk assessment to identify and assess RMs
<p>Disclosures of significant accounting policies that are an integral part of the financial statements are incomplete, inaccurate or not fairly presented</p> <p>Additional risk description - goodwill and intangible asset accounting policies</p>	<p>Significant accounting policies related to recognition of goodwill and intangible assets for an acquisition are complex and involve judgment. The entity has not been involved in a significant business combination in several years, and the acquisition is material to the financial statements and intended users.</p> <p>Based on these factors, the engagement team has assessed the risk of the accounting policy disclosures is an RMM.</p>
<p>The disclosures is incomplete, inaccurate, or not fairly presented.</p> <p>Additional risk description - revenue note disclosures.</p>	<p>The entity's revenue streams have significant variable consideration that is difficult to identify and measure.</p> <p>Revenue is significant to the users of the intended users and the recognition policy is complex.</p> <p>Based on these factors, the engagement team has assessed the risk of the revenue note disclosures is an RMM.</p>

[What are additional examples of how we determine the inherent risk level?](#) [ISA | 565.11149]

See some examples below on how we determine the inherent risk levels.

Expected credit losses (ECL) allowance

The engagement team identified the following RMM: An inappropriate amount is estimated and recorded for the expected credit losses (ECL) allowance for financial assets or contracts.

Fact Pattern:

The ECL has several factors that are high on the inherent risk continuum:

- The most complex estimate for the entity (factors *complexity* and *subjectivity* are very high on the risk continuum, and possibly *exposure to losses*, *significant accounting*, or *economic factors*, *susceptibility of error*, etc.)
- The most heavily scrutinized by regulators and investors (factors *nature of the account*, *exposure to losses*).

Analysis:

Based on these factors alone, the engagement team assesses the inherent risk as Significant for related RMMs.

Deposits

The engagement team identified the following RMM: Deposits are recorded inappropriately when:

- they are not accurately recorded
- they do not meet the recognition requirements or
- they do not exist.

Fact Pattern:

The only factor that is higher on the risk continuum is volume/amount. All other factors are quite low on the risk continuum (low complexity even on a relative basis to other processes, no judgment, no exposure to losses, no SUTs or related parties, etc.).

Analysis:

Based on this fact pattern, the engagement team assesses the inherent risk of RMMs associated with deposits as Base.

Product Returns

The engagement team identified an RMM related to the rights of return estimate, including the related disclosures.

Fact Pattern:

While volume/amount are lower on the risk continuum, exposure to losses and changes from the prior period are higher on the risk continuum (given certain changes in the entity's revenue contracts and uncertainty in the economic environment).

Analysis:

Based on this fact pattern, the engagement team assesses the inherent risk for both the account and related disclosures as Elevated.

Understanding the Entity's System of Internal Control

International Standards on Auditing: ISA 315.Appendix 3 Appendix 3 Understanding the Entity's System of Internal Control

(Ref: Para. 12(m), 21-26, A90-A181)

1. The entity's system of internal control may be reflected in policy and procedures manuals, systems and forms, and the information embedded therein, and is effected by people. The entity's system of internal control is implemented by management, those charged with governance, and other personnel based on the structure of the entity. The entity's system of internal control can be applied, based on the decisions of management, those charged with governance or other personnel and in the context of legal or regulatory requirements, to the operating model of the entity, the legal entity structure, or a combination of these.
2. This appendix further explains the components of, as well as the limitations of, the entity's system of internal control as set out in paragraphs 12(m), 21-26, and A90-A181, as they relate to a financial statement audit.
3. Included within the entity's system of internal control are aspects that relate to the entity's reporting objectives, including its financial reporting objectives, but it may also include aspects that relate to its operations or compliance objectives, when such aspects are relevant to financial reporting.

Example:

Controls over compliance with laws and regulations may be relevant to financial reporting when such controls are relevant to the entity's preparation of disclosures of contingencies in the financial statements.

Components of the Entity's System of Internal Control

Control Environment

4. The control environment includes the governance and management functions and the attitudes, awareness, and actions of those charged with governance and management concerning the entity's system of internal control, and its importance in the entity. The control environment sets the tone of an organization, influencing the control consciousness of its people, and provides the overall foundation for the operation of the other components of the entity's system of internal control.
5. An entity's control consciousness is influenced by those charged with governance, because one of their roles is to counterbalance pressures on management in relation to financial reporting that may arise from market demands or remuneration schemes. The effectiveness of the design of the control environment in relation to participation by those charged with governance is therefore influenced by such matters as:
 - Their independence from management and their ability to evaluate the actions of management.
 - Whether they understand the entity's business transactions.
 - The extent to which they evaluate whether the financial statements are prepared in accordance with the applicable financial reporting framework, including whether the financial statements include adequate disclosures.
6. The control environment encompasses the following elements:
 - (a) *How management's responsibilities are carried out, such as creating and maintaining the entity's culture and demonstrating management's commitment to integrity and ethical values.* The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical behavior are the product of the entity's ethical and behavioral standards or codes of conduct, how they are communicated (e.g., through policy statements), and how they are reinforced in practice (e.g., through management actions to eliminate

or mitigate incentives or temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts). The communication of entity policies on integrity and ethical values may include the communication of behavioral standards to personnel through policy statements and codes of conduct and by example.

(b) *When those charged with governance are separate from management, how those charged with governance demonstrate independence from management and exercise oversight of the entity's system of internal control.* An entity's control consciousness is influenced by those charged with governance. Considerations may include whether there are sufficient individuals who are independent from management and objective in their evaluations and decision-making; how those charged with governance identify and accept oversight responsibilities and whether those charged with governance retain oversight responsibility for management's design, implementation and conduct of the entity's system of internal control. The importance of the responsibilities of those charged with governance is recognized in codes of practice and other laws and regulations or guidance produced for the benefit of those charged with governance. Other responsibilities of those charged with governance include oversight of the design and effective operation of whistle blower procedures.

(c) *How the entity assigns authority and responsibility in pursuit of its objectives.* This may include considerations about:

- Key areas of authority and responsibility and appropriate lines of reporting;
- Policies relating to appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties; and
- Policies and communications directed at ensuring that all personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

(d) *How the entity attracts, develops, and retains competent individuals in alignment with its objectives.* This includes how the entity ensures the individuals have the knowledge and skills necessary to accomplish the tasks that define the individual's job, such as:

- Standards for recruiting the most qualified individuals - with an emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior.
- Training policies that communicate prospective roles and responsibilities, including practices such as training schools and seminars that illustrate expected levels of performance and behavior; and
- Periodic performance appraisals driving promotions that demonstrate the entity's commitment to the advancement of qualified personnel to higher levels of responsibility.

(e) *How the entity holds individuals accountable for their responsibilities in pursuit of the objectives of the entity's system of internal control.* This may be accomplished through, for example:

- Mechanisms to communicate and hold individuals accountable for performance of controls responsibilities and implement corrective actions as necessary;
- Establishing performance measures, incentives and rewards for those responsible for the entity's system of internal control, including how the measures are evaluated and maintain their relevance;
- How pressures associated with the achievement of control objectives impact the individual's responsibilities and performance measures; and

- How the individuals are disciplined as necessary.

The appropriateness of the above matters will be different for every entity depending on its size, the complexity of its structure and the nature of its activities.

The Entity's Risk Assessment Process

7. The entity's risk assessment process is an iterative process for identifying and analyzing risks to achieving the entity's objectives, and forms the basis for how management or those charged with governance determine the risks to be managed.
8. For financial reporting purposes, the entity's risk assessment process includes how management identifies business risks relevant to the preparation of financial statements in accordance with the entity's applicable financial reporting framework, estimates their significance, assesses the likelihood of their occurrence, and decides upon actions to manage them and the results thereof. For example, the entity's risk assessment process may address how the entity considers the possibility of unrecorded transactions or identifies and analyzes significant estimates recorded in the financial statements.
9. Risks relevant to reliable financial reporting include external and internal events, transactions or circumstances that may occur and adversely affect an entity's ability to initiate, record, process, and report financial information consistent with the assertions of management in the financial statements. Management may initiate plans, programs, or actions to address specific risks or it may decide to assume a risk because of cost or other considerations. Risks can arise or change due to circumstances such as the following:
 - *Changes in operating environment.* Changes in the regulatory, economic or operating environment can result in changes in competitive pressures and significantly different risks.
 - *New personnel.* New personnel may have a different focus on or understanding of the entity's system of internal control.
 - *New or revamped information system.* Significant and rapid changes in the information system can change the risk relating to the entity's system of internal control.
 - *Rapid growth.* Significant and rapid expansion of operations can strain controls and increase the risk of a breakdown in controls.
 - *New technology.* Incorporating new technologies into production processes or the information system may change the risk associated with the entity's system of internal control.
 - *New business models, products, or activities.* Entering into business areas or transactions with which an entity has little experience may introduce new risks associated with the entity's system of internal control.
 - *Corporate restructurings.* Restructurings may be accompanied by staff reductions and changes in supervision and segregation of duties that may change the risk associated with the entity's system internal control.
 - *Expanded foreign operations.* The expansion or acquisition of foreign operations carries new and often unique risks that may affect internal control, for example, additional or changed risks from foreign currency transactions.
 - *New accounting pronouncements.* Adoption of new accounting principles or changing accounting principles may affect risks in preparing financial statements.
 - *Use of IT.* Risks relating to:
 - Maintaining the integrity of data and information processing;

- Risks to the entity business strategy that arise if the entity's IT strategy does not effectively support the entity's business strategy; or
- Changes or interruptions in the entity's IT environment or turnover of IT personnel or when the entity does not make necessary updates to the IT environment or such updates are not timely.

The Entity's Process to Monitor the System of Internal Control

10. The entity's process to monitor the system of internal control is a continual process to evaluate the effectiveness of the entity's system of internal control, and to take necessary remedial actions on a timely basis. The entity's process to monitor the entity's system of internal control may consist of ongoing activities, separate evaluations (conducted periodically), or some combination of the two. Ongoing monitoring activities are often built into the normal recurring activities of an entity and may include regular management and supervisory activities. The entity's process will likely vary in scope and frequency depending on the assessment of the risks by the entity.

11. The objectives and scope of internal audit functions typically include activities designed to evaluate or monitor the effectiveness of the entity's system of internal control.⁷² The entity's process to monitor the entity's system of internal control may include activities such as management's review of whether bank reconciliations are being prepared on a timely basis, internal auditors' evaluation of sales personnel's compliance with the entity's policies on terms of sales contracts, and a legal department's oversight of compliance with the entity's ethical or business practice policies. Monitoring is done also to ensure that controls continue to operate effectively over time. For example, if the timeliness and accuracy of bank reconciliations are not monitored, personnel are likely to stop preparing them.

⁷² ISA 610 (Revised 2013) and Appendix 4 of this ISA provides further guidance related to internal audit.

12. Controls related to the entity's process to monitor the entity's system of internal control, including those that monitor underlying automated controls, may be automated or manual, or a combination of both. For example, an entity may use automated monitoring controls over access to certain technology with automated reports of unusual activity to management, who manually investigate identified anomalies.

13. When distinguishing between a monitoring activity and a control related to the information system, the underlying details of the activity are considered, especially when the activity involves some level of supervisory review. Supervisory reviews are not automatically classified as monitoring activities and it may be a matter of judgment whether a review is classified as a control related to the information system or a monitoring activity. For example, the intent of a monthly completeness control would be to detect and correct errors, where a monitoring activity would ask why errors are occurring and assign management the responsibility of fixing the process to prevent future errors. In simple terms, a control related to the information system responds to a specific risk, whereas a monitoring activity assesses whether controls within each of the five components of the entity's system of internal control are operating as intended.

14. Monitoring activities may include using information from communications from external parties that may indicate problems or highlight areas in need of improvement. Customers implicitly corroborate billing data by paying their invoices or complaining about their charges. In addition, regulators may communicate with the entity concerning matters that affect the functioning of the entity's system of internal control, for example, communications concerning examinations by bank regulatory agencies. Also, management may

consider in performing monitoring activities any communications relating to the entity's system of internal control from external auditors.

The Information System and Communication

15. The information system relevant to the preparation of the financial statements consists of activities and policies, and accounting and supporting records, designed and established to:

- Initiate, record and process entity transactions (as well as to capture, process and disclose information about events and conditions other than transactions) and to maintain accountability for the related assets, liabilities and equity;
- Resolve incorrect processing of transactions, for example, automated suspense files and procedures followed to clear suspense items out on a timely basis;
- Process and account for system overrides or bypasses to controls;
- Incorporate information from transaction processing in the general ledger (e.g., transferring of accumulated transactions from a subsidiary ledger);
- Capture and process information relevant to the preparation of the financial statements for events and conditions other than transactions, such as the depreciation and amortization of assets and changes in the recoverability of assets; and
- Ensure information required to be disclosed by the applicable financial reporting framework is accumulated, recorded, processed, summarized and appropriately reported in the financial statements.

16. An entity's business processes include the activities designed to:

- Develop, purchase, produce, sell and distribute an entity's products and services;
- Ensure compliance with laws and regulations; and
- Record information, including accounting and financial reporting information.

Business processes result in the transactions that are recorded, processed and reported by the information system.

17. The quality of information affects management's ability to make appropriate decisions in managing and controlling the entity's activities and to prepare reliable financial reports.

18. Communication, which involves providing an understanding of individual roles and responsibilities pertaining to the entity's system of internal control, may take such forms as policy manuals, accounting and financial reporting manuals, and memoranda. Communication also can be made electronically, orally, and through the actions of management.

19. Communication by the entity of the financial reporting roles and responsibilities and of significant matters relating to financial reporting involves providing an understanding of individual roles and responsibilities pertaining to the entity's system of internal control relevant to financial reporting. It may include such matters as the extent to which personnel understand how their activities in the information system relate to the work of others and the means of reporting exceptions to an appropriate higher level within the entity.

Control Activities

20. Controls in the control activities component are identified in accordance with paragraph 26. Such controls include information processing controls and general IT controls, both of which may be manual or automated in nature. The greater the extent of automated controls, or controls involving automated

aspects, that management uses and relies on in relation to its financial reporting, the more important it may become for the entity to implement general IT controls that address the continued functioning of the automated aspects of information processing controls. Controls in the control activities component may pertain to the following:

- *Authorization and approvals.* An authorization affirms that a transaction is valid (i.e., it represents an actual economic event or is within an entity's policy). An authorization typically takes the form of an approval by a higher level of management or of verification and a determination if the transaction is valid. For example, a supervisor approves an expense report after reviewing whether the expenses seem reasonable and within policy. An example of an automated approval is when an invoice unit cost is automatically compared with the related purchase order unit cost within a pre-established tolerance level. Invoices within the tolerance level are automatically approved for payment. Those invoices outside the tolerance level are flagged for additional investigation.
- *Reconciliations* - Reconciliations compare two or more data elements. If differences are identified, action is taken to bring the data into agreement. Reconciliations generally address the completeness or accuracy of processing transactions.
- *Verifications* - Verifications compare two or more items with each other or compare an item with a policy, and will likely involve a follow-up action when the two items do not match or the item is not consistent with policy. Verifications generally address the completeness, accuracy, or validity of processing transactions.
- Physical or logical controls, including those that address security of assets against *unauthorized access, acquisition, use or disposal*. Controls that encompass:
 - The physical security of assets, including adequate safeguards such as secured facilities over access to assets and records.
 - The authorization for access to computer programs and data files (i.e., logical access).
 - The periodic counting and comparison with amounts shown on control records (for example, comparing the results of cash, security and inventory counts with accounting records).

The extent to which physical controls intended to prevent theft of assets are relevant to the reliability of financial statement preparation depends on circumstances such as when assets are highly susceptible to misappropriation.

- *Segregation of duties.* Assigning different people the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets. Segregation of duties is intended to reduce the opportunities to allow any person to be in a position to both perpetrate and conceal errors or fraud in the normal course of the person's duties.

For example, a manager authorizing credit sales is not responsible for maintaining accounts receivable records or handling cash receipts. If one person is able to perform all these activities the person could, for example, create a fictitious sale that could go undetected. Similarly, salespersons should not have the ability to modify product price files or commission rates.

Sometimes segregation is not practical, cost effective, or feasible. For example, smaller and less complex entities may lack sufficient resources to achieve ideal segregation, and the cost of hiring additional staff may be prohibitive. In these situations, management may institute alternative controls. In the example above, if the salesperson can modify product price files, a detective

control activity can be put in place to have personnel unrelated to the sales function periodically review whether and under what circumstances the salesperson changed prices.

21. Certain controls may depend on the existence of appropriate supervisory controls established by management or those charged with governance. For example, authorization controls may be delegated under established guidelines, such as investment criteria set by those charged with governance; alternatively, non-routine transactions such as major acquisitions or divestments may require specific high-level approval, including in some cases that of shareholders.

Limitations of Internal Control

22. The entity's system of internal control, no matter how effective, can provide an entity with only reasonable assurance about achieving the entity's financial reporting objectives. The likelihood of their achievement is affected by the inherent limitations of internal control. These include the realities that human judgment in decision-making can be faulty and that breakdowns in the entity's system of internal control can occur because of human error. For example, there may be an error in the design of, or in the change to, a control. Equally, the operation of a control may not be effective, such as where information produced for the purposes of the entity's system of internal control (for example, an exception report) is not effectively used because the individual responsible for reviewing the information does not understand its purpose or fails to take appropriate action.

23. Additionally, controls can be circumvented by the collusion of two or more people or inappropriate management override of controls. For example, management may enter into side agreements with customers that alter the terms and conditions of the entity's standard sales contracts, which may result in improper revenue recognition. Also, edit checks in an IT application that are designed to identify and report transactions that exceed specified credit limits may be overridden or disabled.

24. Further, in designing and implementing controls, management may make judgments on the nature and extent of the controls it chooses to implement, and the nature and extent of the risks it chooses to assume.

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Understand and evaluate the Control Environment component [ISA | 1310]

What do we do?

Obtain an understanding of and evaluate the entity's control environment relevant to the preparation of the financial statements, including the policies and actions of management and those charged with governance concerning the entity's control environment.

Why do we do this?

We obtain an understanding of and evaluate the entity's control environment relevant to the preparation of the financial statements to support our identification and assessment of risks of material misstatement (RMMs).

Execute the Audit

What is the Control Environment? [ISA | 1310.1300]

An entity's Control Environment is the set of controls, processes and structures that provide the basis for carrying out internal control across the entity.

The Control Environment includes:

- the governance and management functions; and
- the attitudes, awareness and actions of those charged with governance and management concerning the entity's system of internal control and its importance to the entity.

The Control Environment sets the tone of an organization, influencing the control consciousness of its people and provides the overall foundation for the operation of the other components of the entity's system of internal control

Does the Control Environment encompass all levels of an entity? [ISA | 1310.11898]

Yes. The Control Environment underpins how ICFR is carried out across the organization and at all levels. So we may assess the Control Environment at levels below the parent or corporate level - e.g. regions, divisions, operating units and functional areas.

Does the Control Environment encompass third-party service providers and business partners? [ISA | 1310.11899]

Yes. The Control Environment also includes third-party service providers and business partners. Although the organization may rely on an outsourced service provider to conduct business processes, policies, and procedures on behalf of the entity, management retains ultimate responsibility for meeting the requirements for an effective system of internal control.

Why is the Control Environment an important component of ICFR? [ISA | 1310.1400]

If we consider the entity's internal control structure as like the structure of a house, the Control Environment is the foundation; thus it is the foundation for ICFR.



Process-level control activities directly affect financial reporting, but often affect only just one particular stream of transactions. In contrast, the Control Environment's effect on ICFR is indirect, yet it may have a pervasive effect on multiple business processes throughout the organization.

Not Integrated Audit | How do we obtain an understanding of the entity's Control Environment? [ISA | 1310.1800]

We obtain an understanding of the entity's Control Environment by:

- understanding, through inquiry, the set of controls, processes and structures that address the following elements/principles:
 - [how the entity demonstrates a commitment to integrity and ethical values](#)
 - [how the board of directors/those charged with governance demonstrates independence and oversight of internal control](#)
 - [structures, reporting lines, and authorities and responsibilities](#)
 - [how the entity demonstrates a commitment to attract, develop, and retain competent individuals](#)
 - [how the entity holds individuals accountable for their internal control responsibilities](#)
- [performing procedures to obtain an understanding of the CERAMIC components:](#)
 - begin by performing inquiries to obtain an understanding of each element/principle within the component.
 - consider whether certain factors apply to determine whether to perform more than inquiry
 - If at least one of the factors apply, design additional procedures to obtain an understanding (i.e. observation and/or inspection)
- Based on our understanding obtained, [evaluating the control environment component](#).

We also [consider how information is being used](#) in our procedures and [determine the appropriate audit procedures to evaluate the reliability of the information](#) used to obtain an understanding.

If we identify a control deficiency, we perform the following:

- evaluate the severity of the control deficiency and assess the impact on our audit; and
- evaluate whether the control deficiency is indicative of a fraud risk factor.
- evaluate whether control deficiencies undermine the other components of the entity's system of internal control.

What do we do if there are unaddressed elements after we obtain an understanding of CERAMIC? [ISA | 1310.8653]

When those charged with governance are not separate from management, it is appropriate for the following elements to be unaddressed:

- Element 2 - Those charged with governance demonstrates independence from management and exercises oversight of the development and performance of internal control.
- Element 11 - The entity communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control between management and those charged with governance.

In all other circumstances, if there are unaddressed elements after we have obtained an understanding of the CERAMIC component, we identify a control deficiency in the related CERAMIC component.

What are the five elements of the Control Environment component? [ISA | 1310.11926]

We obtain an understanding over the following five elements in order to evaluate the Control Environment component of ICFR.

Elements of the Control Environment component	<u>Element 1:</u> The organization demonstrates a commitment to integrity and ethical values. <u>Element 2:</u> When those charged with governance are separate from management, those charged with governance demonstrates independence from management and exercises oversight of the development and performance of internal control. <u>Element 3:</u> Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. <u>Element 4:</u> The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. <u>Element 5:</u>
---	---

The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

How may the Control Environment component for less complex entities be different? [ISA | 1310.2000]

Although the same principles / elements underlying the Control Environment component apply for both simpler and complex organizations; the entity's approach to address the CERAMIC component is likely to differ.

For example, a less complex entity may not have a written code of conduct, but instead, develops a culture that emphasizes the importance of integrity and ethical behavior through oral communication and by management example. Further, compared to a more complex entity, communication may be less structured and easier to achieve in a less complex entity since there may be fewer levels of responsibility and management may be more available and have greater visibility. As such, there is often more direct interaction between management and employees such that the organizational structure, reporting lines, and responsibilities are clear and evident.

A less complex entity's commitment to integrity and ethical values may appear in the variety of policies and procedures it employs or the attitudes, awareness and actions of those charged with governance and management.

Examples

2 Understand and evaluate the risk assessment process [ISA | 1317]

What do we do?

Obtain an understanding of management's risk assessment process and evaluate whether the entity's risk assessment process is appropriate to the entity's circumstances considering the nature and complexity of the entity.

Why do we do this?

Our evaluation of the entity's risk assessment process may assist us in understanding where the entity has identified risks that may occur, and how the entity has responded to those risks. Our evaluation of how the entity identifies its business risks, and how it assesses and addresses those risks assists us in understanding whether the risks faced by the entity have been identified, assessed and addressed as appropriate for the nature and complexity of the entity.

If an entity does not have a risk assessment process that is appropriate for its nature and complexity, it may lead to unidentified / unaddressed risks relevant to its financial reporting objectives, ineffectively designed control activities and an increase in the possibility of a material misstatement in the financial statements.

Our understanding and evaluation of the entity's risk assessment process assists us with identifying and assessing financial statement level and assertion level risks of material misstatement.

Execute the Audit

Why is risk assessment an important component of ICFR? [ISA | 1317.1400]

Risk assessment is an essential component of ICFR because it forms the basis for how management identifies and analyzes risks relevant to its financial reporting objectives and how they determine the risks to be managed. If an entity does not have a risk assessment process that is appropriate for its nature and complexity, it may lead to unidentified / unaddressed risks relevant to its financial reporting objectives, ineffectively designed control activities and an increase in the possibility of a misstatement in the financial statements.

Using our house example, the risk assessment process is the blueprint or map of the house, and is needed to appropriately design the house.



Understanding the entity's risk assessment process, relevant to the preparation of the financial statements, gives us insight into whether the entity is appropriately identifying risks (and have a sound ICFR), which may affect our risk assessments. In addition, it also helps us plan and execute our audit and gives us insight into potential RMMs that we may not have considered.

When does an entity perform its risk assessment process? [ISA | 1317.1600]

An effective risk assessment process is iterative in nature. The four principles / elements within the Risk Assessment component are not always considered sequentially because there is considerable overlap among the principles / elements. Further, as an entity performs and monitors controls, management may identify items that require earlier risk determinations to be reassessed.

How do we obtain an understanding of the entity's risk assessment process? [ISA | 1317.1900]

We obtain an understanding of the entity's risk assessment process by:

- understanding, through inquiry, the processes that address the following elements/principles:
 - [how the entity specifies objectives to identify and assess risks](#)

- [how the entity identifies and analyses risks](#)
- [how the entity considers fraud when assessing risks](#)
- [how the entity identifies and assesses changes that impact internal control](#)
- [performing procedures to obtain an understanding of the CERAMIC components:](#)
 - begin by performing inquiries
 - consider whether certain factors apply to determine whether to perform more than inquiry
 - If at least one of the factors apply, design additional procedures to obtain an understanding (i.e. observation and/or inspection)
- based on the above, [evaluating the entity's risk assessment process](#).

We also [consider how information is being used](#) in our procedures and [determine the appropriate audit procedures to evaluate the reliability of the information](#) used to obtain an understanding.

If we identify a control deficiency in a CERAMIC component(s), [we evaluate the severity of the control deficiency and assess the impact on our evaluation](#).

What do we do if there are unaddressed elements after we obtain an understanding of CERAMIC? [ISA | 1317.8653]

When those charged with governance are not separate from management, it is appropriate for the following elements to be unaddressed:

- Element 2 - Those charged with governance demonstrates independence from management and exercises oversight of the development and performance of internal control.
- Element 11 - The entity communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control between management and those charged with governance.

In all other circumstances, if there are unaddressed elements after we have obtained an understanding of the CERAMIC component, we identify a control deficiency in the related CERAMIC component.

What are the four elements of the Risk Assessment component? [ISA | 1317.1800]

When management has an established risk assessment process, we consider the four elements outlined in the table below when obtaining an understanding of the Risk Assessment component of ICFR.

Elements of the Risk Assessment component	<p>Element 6: The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.</p> <p>Element 7: The organization identifies risks to the achievement of its objectives and analyzes risks as a basis for determining how the risks should be managed.</p> <p>Element 8:</p>
---	--

	<p>The organization considers the potential for fraud in assessing risks to the achievement of objectives.</p> <p>Element 9:</p> <p>The organization identifies and assesses changes that could significantly affect the system of internal control.</p>
--	---

Our understanding includes how the entity's risk assessment process identifies and addresses risks related to [accounting estimates](#).

Why is it important for an entity to consider the potential for fraud? [ISA | 1317.11847]

Every entity faces some risk of fraud from within, but the very nature of fraud makes it difficult to detect. It can also evolve and change over time, which makes fraud prevention or detection even more difficult.

At the same time, as shown by major corporate fraud scandals in nearly every decade of the past century, fraud can have a significant negative effect on an entity's financial reporting process, the reliability of its financial statements, and investor confidence.

[Principle / Element 8](#) highlights the importance of fraud risks to make it clear that an appropriate risk assessment process should specifically consider the vulnerability of the entity to fraudulent activity.

Why is it important for an entity to monitor changes? [ISA | 1317.11848]

Experience suggests that entities control routine business processes well. However, when something new or unusual happens, the system of ICFR is unable to process the new events or transactions in a controlled manner. This, in turn, may lead to material errors in the financial statements and deficiencies in internal control.

Identifying new transactions and events ahead of time through an entity's 'early warning systems' allows the entity time to make the necessary adjustments to the existing system of ICFR.

[Principle / Element 9](#) highlights the importance of considering whether changes result in additional risks, and whether the entity has designed and implemented control activities that appropriately mitigate those additional risks.

How do the auditing standards map to the four elements of the Risk Assessment Process component?

[ISA | 1317.11849]

The following table maps each of the processes that comprise the risk assessment process in the auditing standards to the related elements of the Risk Assessment Process component.

Process	Related Elements
Identifying business risks relevant to financial reporting objectives	<p>Element 6:</p> <p>The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.</p> <p>Element 7:</p>

	<p>The organization identifies risks to the achievement of its objectives and analyzes risks as a basis for determining how the risks should be managed.</p> <p><u>Element 8:</u></p> <p>The organization considers the potential for fraud in assessing risks to the achievement of objectives.</p> <p><u>Element 9:</u></p> <p>The organization identifies and assesses changes that could significantly impact the system of internal control.</p>
Estimating the significance of the risks and assessing the likelihood of their occurrence	<p><u>Element 7:</u></p> <p>The organization identifies risks to the achievement of its objectives and analyzes risks as a basis for determining how the risks should be managed.</p> <p><u>Element 8:</u></p> <p>The organization considers the potential for fraud in assessing risks to the achievement of objectives.</p> <p><u>Element 9:</u></p> <p>The organization identifies and assesses changes that could significantly impact the system of internal control.</p>
Deciding about actions to address those risks	<p><u>Element 7:</u></p> <p>The organization identifies risks to the achievement of its objectives and analyzes risks as a basis for determining how the risks should be managed.</p> <p><u>Element 8:</u></p> <p>The organization considers the potential for fraud in assessing risks to the achievement of objectives.</p> <p><u>Element 9:</u></p>

	The organization identifies and assesses changes that could significantly impact the system of internal control.
--	--

How may the Risk Assessment Process component for smaller, less complex entities be different? [ISA | 1317.2200]

In some less complex, smaller entities, and particularly owner-managed entities, an appropriate risk assessment may be performed through the direct involvement of management or the owner-manager (for example, the manager or owner-manager may routinely devote time to monitoring the activities of competitors and other developments in the market place to identify emerging business risks). The evidence of this risk assessment occurring in these types of entities is often not formally documented. However, discussions we have with management, corroborated by e-mails or other correspondence between management and other personnel, may provide evidence that management is, in fact, performing risk assessment procedures appropriate to the nature and complexity of the entity.

Examples

3 Understand and evaluate monitoring activities

[ISA | 1336]

What do we do?

Obtain an understanding of and evaluate the entity's monitoring activities.

Why do we do this?

Our understanding and evaluation of how the entity monitors the system of internal control relevant to the preparation of the financial statements assists us in understanding whether the other components of the entity's system of internal control are present and functioning, and therefore assists with understanding the other components of the entity's system of internal control. Our understanding and evaluation may also assist us with identifying and assessing financial statement level and assertion level risks of material misstatement.

Execute the Audit

What is a monitoring activity? [ISA | 1336.1300]

Monitoring activities help ascertain whether each of the components of internal control, including controls within each component, is present and functioning as intended.

Management's monitoring activities over internal controls involves assessing the effectiveness of internal control performance over time through ongoing activities, separate evaluations, or a combination of the two and taking necessary remedial actions.

Why are monitoring activities an important component of ICFR? [ISA | 1336.1400]

Using our house example, monitoring activities are similar to the roof of the house. They oversee and protect the other components.



Management's monitoring processes and controls continually check the other ICFR components to identify issues and determine what needs attention. Effective monitoring helps management identify necessary changes to the ICFR system to prevent or detect, on a timely basis, future errors in the financial statements.

The goal of monitoring is to determine both that the system of internal control operated and that it operated effectively.

Monitoring also includes evaluating the severity of identified deficiencies and communicating deficiencies to the appropriate parties.

Without effective monitoring, management do not have a basis to rely on their own ICFR.

[Not Integrated Audit | How do we obtain an understanding of the entity's monitoring activities?](#) [ISA |

1336.1700]

We obtain an understanding of the entity's process to monitor internal controls relevant to financial reporting by:

- understanding, through inquiry, the processes that address the following elements/principles:
 - [how the entity selects, develops, and performs monitoring activities](#)
 - [how the entity addresses internal control deficiencies](#)
- [performing procedures to obtain an understanding of the CERAMIC components:](#)
 - begin by performing inquiries
 - consider whether certain factors apply to determine whether to perform more than inquiry

- If at least one of the factors apply, design additional procedures to obtain an understanding (i.e. observation and/or inspection)
- based on our understanding obtained, evaluating whether the entity's process for monitoring the system of internal control is appropriate to the entity's circumstances, considering the nature and complexity of the entity.

We also consider how information is being used in our procedures and determine the appropriate audit procedures to evaluate the reliability of the information used to obtain an understanding.

In addition, if the entity has an internal audit function, we obtain an understanding of the internal audit function as part of understanding the entity's monitoring activities (refer to the activity 'Obtain an understanding of the IA function').

If we identify a control deficiency in a CERAMIC component(s), we evaluate the severity of the control deficiency and assess the impact on our evaluation.

What do we do if there are unaddressed elements after we obtain an understanding of CERAMIC? [ISA | 1336.8653]

When those charged with governance are not separate from management, it is appropriate for the following elements to be unaddressed:

- Element 2 - Those charged with governance demonstrates independence from management and exercises oversight of the development and performance of internal control.
- Element 11 - The entity communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control between management and those charged with governance.

In all other circumstances, if there are unaddressed elements after we have obtained an understanding of the CERAMIC component, we identify a control deficiency in the related CERAMIC component.

What are the two elements of the Monitoring component? [ISA | 1336.1800]

We consider the two elements outlined in the table below when obtaining an understanding of the Monitoring component of ICFR.

Elements of the Monitoring Component	<u>Element 13:</u> The organization selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
	<u>Element 14:</u> The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action.

How may the Monitoring component for less complex entities be different? [ISA | 1336.1900]

Although the same principles / elements underlying the Monitoring component apply for both small and large organizations; the entity's process to address the CERAMIC component is likely to differ.

In less complex entities, the entity's process to monitor the system of internal control may be accomplished by management's close involvement in the entity's operations and accounting / financial reporting. In these circumstances, monitoring activities are likely to include more ongoing activities that are built into the normal recurring activities of an entity, as opposed to separate evaluations or formal testing of controls by Internal Audit or a similar function.

For example, management's close involvement in the entity's operations may involve regular and supervisory activities such as periodic reviews of the financial statement and related accounting information and/or a review of bank reconciliations, exception reports, or other information which has a role in monitoring the effectiveness of the underlying controls.

Through this close involvement, management may identify variances from expectations or inaccuracies in financial data, leading to the control being corrected. Further, management's actions and follow-up may also evidence how remedial actions are implemented.

Examples

4 Understand and evaluate information and communication [ISA | 1323]

What do we do?

Obtain an understanding of the information system relevant to financial reporting and how the entity communicates roles and responsibilities and significant matters relating to financial reporting and evaluate whether the entity's information system and communication appropriately support the preparation of the entity's financial statements in accordance with the applicable financial reporting framework.

Why do we do this?

We understand the entity's information system and communication because understanding the entity's policies that define the flows of transactions and other aspects of the entity's information processing activities relevant to the preparation of the financial statements, and evaluating whether the component appropriately supports the preparation of the entity's financial statements, supports our identification and assessment of risks of material misstatement at the assertion level.

This understanding and evaluation may also result in the identification of risks of material misstatement at the financial statement level when the results of our procedures are inconsistent with expectations about the entity's system of internal control that may have been set based on information obtained during the engagement acceptance or continuance process.

Execute the Audit

What is information and communication? [ISA | 1323.1300]

The scope of the Information and Communication component of ICFR is broad. It generally comprises people, business processes, activities, transactions, information/data elements and IT.

The information system may be located at the entity, its service organizations or both. It is used to generate relevant, quality information to execute the entity's business objectives - e.g. to produce and sell its products and services and measure its performance - and financial reporting objectives.

Communication, both internal and external, delivers the information the entity needs to carry out day-to-day controls. Communication also helps staff understand their internal control responsibilities and how they help achieve the entity's objectives.

Our understanding of information focuses on the aspects of an entity's information system relevant to financial reporting and ICFR. Even with that narrow focus, this often includes obtaining an understanding of how information flows from:

- the initiation and authorization of individual transactions;
- the occurrence of other events and conditions relevant to financial reporting; and
- how those transactions and other events and conditions are reported in the financial statements and related disclosures within the financial statements.

[How do we obtain an understanding of the Information and Communication component?](#) [ISA | 1323.1500]

We obtain an understanding of the information and communication component by:

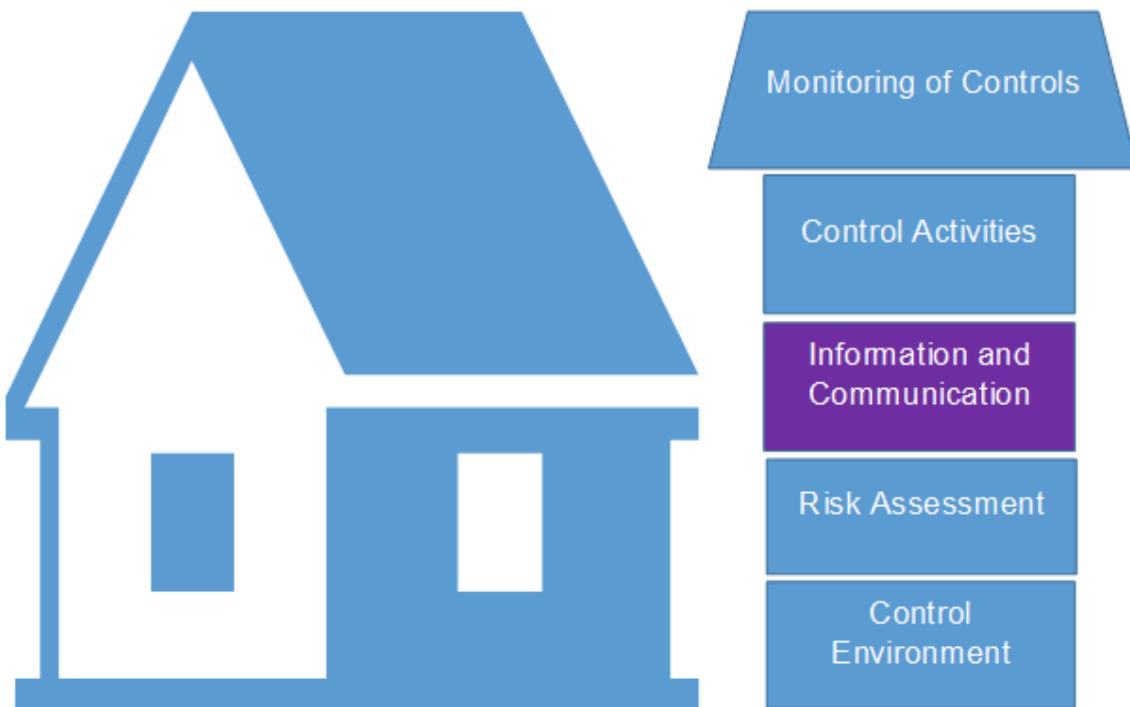
- [understanding and evaluating information](#); and
- [understanding and evaluating communication](#)

We also [consider how information is being used](#) in our procedures and [determine the appropriate audit procedures to evaluate the reliability of the information](#) used to obtain an understanding.

[Why is the Information and Communication component important to ICFR?](#) [ISA | 1323.1400]

An entity's ICFR uses information and communication to achieve its ICFR objectives across all of the ICFR components. If we recall our house example, information and communication are the walls and pipes of the house. Information and communication touch all of the components and act as a conduit for interaction between the components and throughout the entity.

The entity's ICFR could be ineffective if control operators don't receive complete, accurate, appropriate and timely information from both external and internal sources.



Because communication is so pervasive to the entity's overall ICFR, deficiencies can also have implications for our audit approach. For example, if an entity has written accounting policies but does not communicate them consistently across employees, individuals responsible for financial reporting may not appropriately account for transactions in accordance with the applicable financial reporting framework.

As auditors, if we are aware of this deficiency, it is likely to affect our risk assessment - especially as it relates to our identification of RMMs.

Similarly, if the entity does not have processes and controls in place to facilitate communication between its legal and accounting departments about a legal contingency, a higher risk of material misstatement might exist in this area. So, we may plan to respond to it.

Without obtaining an understanding of the entity's communication processes and controls, we may not have all the information we need to appropriately plan and execute our audit.

What are the three elements for the communications portion of the Information and Communications component? [ISA | 1323.1600]

We consider the three elements outlined in the table below when obtaining an understanding and evaluating the communications portion of the Information and Communication component of ICFR.

Elements for communication	<u>Element 10:</u> The organization communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control between people within the entity, including how financial reporting roles and responsibilities are communicated.
----------------------------	---

Element 11:

The organization communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control between management and those charged with governance.

Element 12:

The organization communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control to external parties, such as regulatory bodies.

Examples

5 Understand control activities [ISA | 1340]

What do we do?

Obtain an understanding of control activities that is sufficient to assess the factors that affect the risks of material misstatement and to design further audit procedures.

Why do we do this?

We understand control activities, including evaluating their design and implementation, when we plan to test their operating effectiveness or when we are otherwise evaluating them as a part of risk assessment (e.g. controls over significant risks, journal entries, etc.). We refer to the control activities that we understand as relevant control activities.

Execute the Audit

What are control activities? [ISA | 1340.12185]

Control activities	Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity and at various stages within business processes, and over the technology environment. Specific to financial reporting, control activities are the policies and procedures established to mitigate (either directly or indirectly) risks of material misstatement in the business processes and financial reporting processes.
--------------------	---

Control activities include both process control activities and general IT controls (GITCs). The table below illustrates the distinction between these two types of control activities.

	Control activities	
Types of control activities	Process control activities	General IT controls
Address	PRPs	RAFITS
Nature	Manual or Automated	

These terms are used in KAEG to distinguish how the methodology applies to each type of control activity. However, KAEG may also use the term 'control activities' or 'control' when the type of control activity being addressed is established in the content or is not relevant.

For example, '*The precision of a process control activity is essentially the size of a potential misstatement the control would prevent, or detect and correct, when it operates effectively. So, a control's precision is the maximum size of a misstatement that could be accepted based on the control's design and operation.*'

We only evaluate precision for process control activities, which is made clear in the beginning of the first sentence. The broader term 'control' is used later for convenience as it is shorter and does not detract from the established application of the content.

What are process control activities? [ISA | 1340.8434]

Process control activities relate to the processing of information, in IT systems or other manual processes, that directly address PRPs.

KAEG may refer to process control activities as 'control activities' when it is apparent from the context of content that the control activity occurs in a business process and addresses a PRP.

What are general IT controls? [ISA | 1340.1300]

General IT controls (GICs) are control activities over the entity's IT processes that support the continued effective operation of the IT environment, including:

- the continued effective operation of automated controls, and
- the integrity of data and information within the entity's IT system.

The IT processes are the entity's processes to manage access to programs and data, manage program changes, manage program acquisition and development, and manage computer operations (see activity '[Understand the entity's IT processes](#)' for more information).

The IT environment encompasses the IT systems the entity uses as part of its financial reporting and business processes, including its layers of technology (application, database, operating system and network), the IT processes and the IT organization (see activity '[Understand how the entity uses IT as part of financial reporting](#)' for more information).

GITCs are not expected to directly prevent, or detect and correct, material misstatements on a timely basis, but ineffective GITCs may lead to automated controls that don't operate consistently and effectively, and therefore might not prevent, or detect and correct, a material misstatement on a timely basis.

[What is the difference between a control activity and a process?](#) [ISA | 1340.12186]

We might think about the process as the actual steps necessary to record an amount into the financial records, whereas control activities are the specific actions taken along the way to mitigate risks that are introduced during the process. Said differently - processes are 'how' an entity records transactions and control activities are the different checks performed throughout the process to prevent or detect misstatements that could occur.

[Why do we differentiate process activities from control activities?](#) [ISA | 1340.11409]

Understanding the difference between activities that introduce risks - i.e. process activities - and activities that mitigate risks - i.e. control activities - is a key first step to understanding the process and flow of transactions.

Blurring the lines or misunderstanding the distinction between the process activities and the control activities hinders us from properly understanding the process and flow of transactions. This makes it difficult to appropriately perform our risk assessment procedures.

[What is an example of the differences and relationship between process activities and control activities?](#) [ISA | 1340.11410]

Consider the following example — the credit limit illustrates the differences and relationship between process activities and control activities.

Process activities	Customers place their purchase orders electronically. These orders are captured in the entity's enterprise resource planning (ERP) system and processed for fulfilment.
Identified risk	Customers could exceed their established credit limit.
Control activities to address the identified risk	The entity's ERP system compares the open receivables from the customer plus the submitted purchase order amount to the established customer credit limit. If the total amount of open receivables and purchase orders exceeds the credit limit, the purchase order is not processed further. Each purchase order not processed is followed-up manually.

[Which control activities do we understand and are relevant to the audit?](#) [ISA | 1340.1600]

We obtain an understanding of control activities that are 'relevant to the audit'. 'Control activities relevant to the audit' or 'relevant control activities' have a specific meaning in our methodology. This terminology identifies control activities that we understand and, thus, perform procedures to evaluate their design and implementation. The following are control activities relevant to the audit:

- process control activities that address RMMs:
 - where we plan to take a controls reliance approach;
 - that are significant risks;
 - that are associated with SUTs (refer to activity '[Identify SUTs](#)') or related parties (refer to activity '[Obtain an understanding of related party processes and controls](#)'); or
 - that are associated with journal entries and other adjustments (refer to activity '[Evaluate the design and implementation of control activities over journal entries and other adjustments](#)'); or
 - where we cannot obtain sufficient evidence through substantive testing alone; or
- process control activities:
 - that we are testing over the accuracy and completeness of internal information and the RDE(s) to evaluate the reliability of such information (see activity '[Test management's controls over the accuracy and completeness of internal information](#)'); or
 - that, in our professional judgment, we consider it appropriate to understand in order to enable us to effectively identify and assess the risk of material misstatement and design further audit procedures; and
- general IT controls that address 'relevant RAFITs' associated with 'relevant automated controls' or data integrity risks (refer to question '[Under what circumstances do we obtain an understanding of general IT controls](#)').

[What are examples of control activities that we may decide to understand for risk assessment purposes even though we will not test their operating effectiveness?](#) [ISA | 1340.8436]

We may consider it appropriate to understand certain control activities, including evaluating their design and implementation even though we do not plan to test their operating effectiveness for the purpose of providing an appropriate basis for the identification, assessment of and response to risks of material misstatement. Examples of such controls may include:

- controls that address risks assessed as Elevated that are higher on the spectrum of inherent risk but have not been determined to be a significant risk;
- controls related to reconciling detailed records to the general ledger;
- controls related to accounting estimates; or
- complementary user entity controls, if the entity uses a service organization

[How do we identify and understand relevant process control activities?](#) [ISA | 1340.11412]

There are four steps in identifying and obtaining an understanding of relevant process control activities.

- (1) [Understand business processes and the financial reporting process](#).
- (2) [Identify process risk points](#).
- (3) [Determine which controls are relevant to the audit](#).
- (4) [Evaluate the design and implementation of relevant process control activities](#).

We achieve these four steps through properly planning and executing either (i) a walkthrough or (ii) inquiries and observations or inspections of relevant control documentation to sufficiently evaluate the design and implementation of identified controls.

Remember: we perform the first step (understanding the business process, including our understanding of IT) regardless of whether we obtain an understanding, including evaluate design and implementation, of the process control activity.

Refer to activity '[Understand how the entity has responded to RAFITs](#)' for the steps to identify and obtain an understanding of general IT controls.

[How do we efficiently obtain an understanding of relevant process control activities?](#) [ISA | 1340.11416]

It is efficient to both:

- identify the PRPs and relevant controls; and
- evaluate the design and implementation of those controls

at the same time as obtaining an understanding of the process.

However, in doing this, we also keep in mind two things:

- (1) If we're not careful, we may focus our walkthrough or inquiries and observations or inspections only on identifying PRPs and relevant process control activities, and fail to obtain an adequate understanding of the business process.
- (2) Once we've determined the RMMs, we revisit the PRPs and process control activities we've identified to determine that those RMMs have associated relevant control activities, if applicable.

[What is a process risk point?](#) [ISA | 1340.11420]

A process risk point (PRP) is a point in the entity's process that a misstatement could, individually or in aggregate, yield a material misstatement to the financial statements. We describe the PRP as the 'where' and the 'how' in the entity's process that misstatement could be introduced.

PRPs are likely to be different from one entity to the next because each entity's processes are different. To be able to determine PRPs, we understand the entity's process.

[How and where might PRPs arise in a business process?](#) [ISA | 1340.11421]

PRPs arise throughout a business process or IT system, and include where and how an error could be introduced to data and information used as part of the process, including risks relating to:

- data input;
- data integrity; and
- data extraction and manipulation.

PRPs may also relate to the accuracy of calculations or other data manipulation performed by the IT system.

Every business process is likely to contain multiple PRPs. And every RMM identified also has at least one PRP.

PRPs also include risks of unauthorized acquisition, use or disposition of assets that could result in a material misstatement of the financial statements.

[What is the difference between a risk of misstatement and a process risk point?](#) [ISA | 1340.11422]

Risks of misstatement (RMs) generally stem from the accounting framework, so we expect them to be the same for similar transactions across entities. Process risk points (PRPs) are the specific points where a material misstatement could be introduced by the process.

Risk of material misstatement

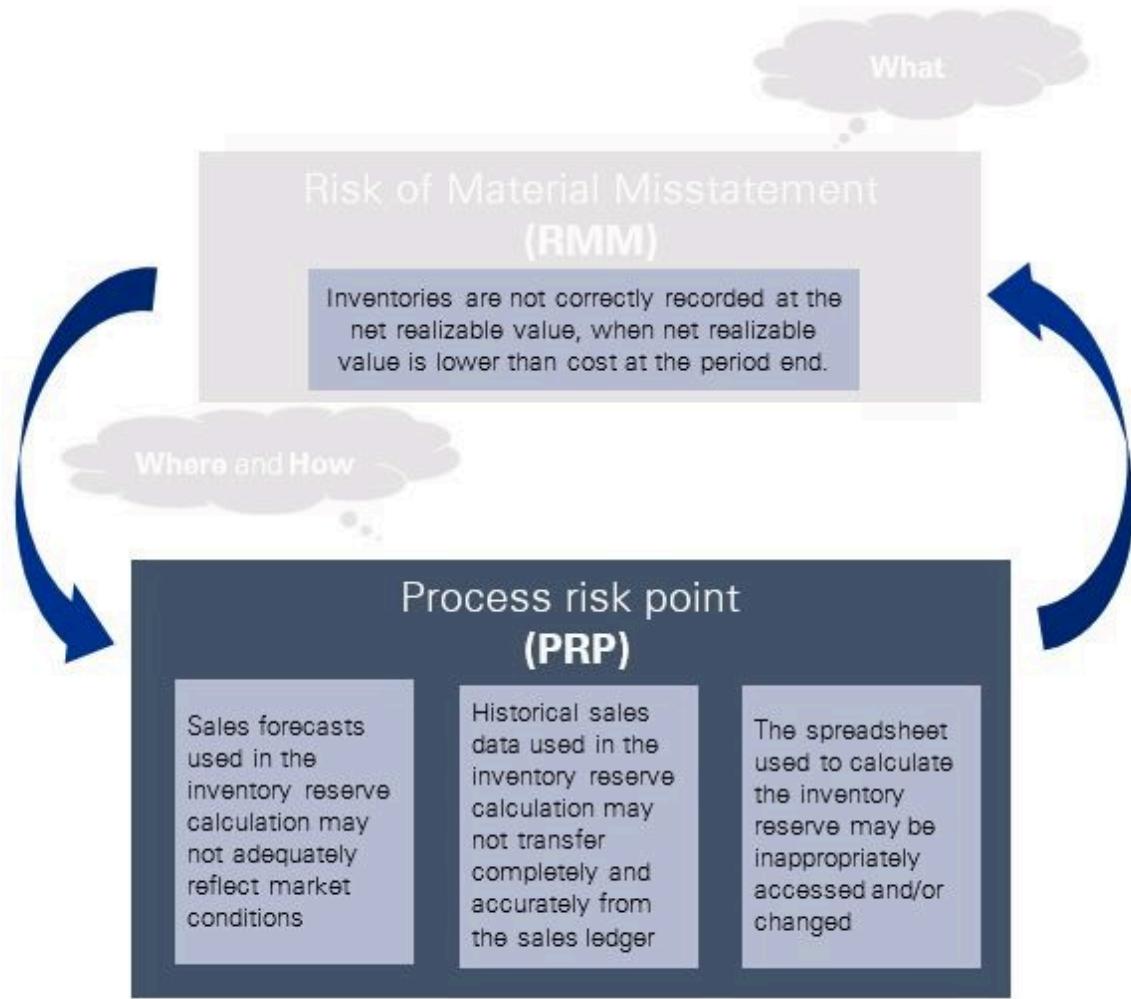
The way an account or disclosure could be misstated, individually or in the aggregate, resulting in a material misstatement

Relevant process risk points

A point in the entity's process that a misstatement could, individually or in the aggregate, yield a material misstatement to the financial statements

[What is the relationship between an RMM and a PRP? \[ISA | 1340.11423\]](#)

The RMM is really the 'what' could be misstated, whereas the PRP are the 'where' and the 'how' in the process an RMM can arise. Therefore each RMM has at least one PRP.



Will every relevant PRP be associated with an RMM? [ISA | 1340.11424]

Yes. Every relevant PRP will be associated with at least one RMM. If we have a PRP without an RMM, we revisit the identification of RMMs.

Can an RMM and a PRP ever be the same thing? [ISA | 1340.11425]

Possibly. This may happen when there is a review control designed to determine whether the accounting criteria is met.

For example, suppose the RMM is that a contract is inappropriately determined to be within or outside the scope of the revenue recognition standard (from the Library "Contracts, or parts of contracts, are not appropriately identified as within or outside the scope of Topic 606/IFRS 15").

The entity's process may be that someone analyzes each contract to determine whether it is within the scope of the revenue recognition standard. There is a PRP that the analysis is incorrect and the person reaches the wrong conclusion. This PRP mirrors the RMM.

However, other PRPs are likely in that process that may also be linked to this RMM. For example, there could be a PRP that all contracts are not sent to Finance for analysis. This type of PRP still

relates to the RMM that a contract is inappropriately determined to be within or outside the scope of the revenue recognition standard, but it is not the same as the RMM.

Other PRPs that are tied to an RMM but are not the same as the RMM might include risks related to the completeness and accuracy of data as it:

- moves through a system;
- is generated into a report;
- is stored in a database; or
- is recorded in the ledger via an automated or manual journal entry.

[Why do we distinguish between RMMs and PRPs?](#) [ISA | 1340.11426]

PRPs are related to the RMMs because an entity's process is designed to account for transactions - i.e. apply appropriate accounting standards given the transaction. However, although they are related, our audit response is different depending on whether we are addressing an RMM or a PRP.

Our substantive procedures are designed to address RMMs, while our control testwork procedures are designed to test the entity's controls that address PRPs.

For example, the RMM might be that a contract does not belong within the scope of the revenue recognition standard.

PRPs, on the other hand, are specific to the entity's process and may include the following:

- not all contracts are sent to the Finance department to be analyzed; or
- the contract is analyzed, but an incorrect conclusion is reached.

Clearly, the RMM and the PRPs are related, but the RMM calls for a different response than the PRPs.

Our substantive procedures to address the RMM could be to sample contracts and analyze them to determine whether they are within the scope of the revenue recognition standard. The attributes of our substantive tests do not include whether all contracts were sent to Finance, or whether they were analyzed by Finance; those are procedures to address the PRPs.

Our control testwork procedures are designed to test the entity's controls that address the PRPs, and therefore focus on whether all contracts were analyzed by Finance and whether the analysis reached an appropriate conclusion.

[How are control activities affected by the other components of ICFR?](#) [ISA | 1340.1801]

Control activities complement the other components of internal control. For example:

- proper design and implementation of control activities are supported by an effective risk assessment;
- determining that the controls operate as intended is supported by monitoring;
- providing control operators with the information to operate controls properly is supported by appropriate levels of information and communication; and
- a robust control environment lays the foundation for an effective system of internal controls.

Because the five ICFR components are distinct but interrelated, deficiencies in one component may affect controls in another, and so may ultimately cause us to change our audit response for other tests of controls or substantive procedures.

[How are monitoring activities different from process control activities?](#) [ISA | 1340.1800]

The key difference between process control activities and monitoring activities relates to their objective and their relationship to the risk of material misstatement of an entity's financial statements.

With process control activities, that relationship is direct: each process control activity's objective is to mitigate a specific risk within a business process that could lead to a material misstatement of the entity's financial statements. We call that risk a process risk point (PRP).

Accordingly, process control activities are designed and operated with a level of precision that allows both management and external auditors to be confident that they would prevent or detect, in a timely manner, a material misstatement to the entity's financial statements.

On the other hand, monitoring activities have only an indirect relationship to the risk of misstatement (RM) of an entity's financial statements. They do not themselves mitigate risks to specific financial statement assertions. Instead, they monitor the continuing appropriateness of the design and operating effectiveness of control activities and controls within other components of ICFR (Control Environment, Risk Assessment, Control Activities, and Information and Communication).

The objective of monitoring activities is to:

- timely identify deficiencies in controls;
- analyze their root causes; and
- design and implement effective remediation plans.

For example, the intent of a monthly completeness control activity would be to detect and correct errors; whereas a monitoring activity would ask why there were errors in the first place and assign management the responsibility of fixing the process to prevent future errors.

Monitoring activities *could* identify a misstatement in the entity's financial statements. But they're more likely to identify instances where control activities did not operate effectively, and where further investigation as to the propriety of financial reporting may be necessary.

When it comes to mitigating the RMMs of an entity's financial statements, the difference in the level of assurance provided by process control activities ('would' level) and monitoring activities ('could' level) has implications for how we rely on their assessment of the entity's ICFR.

Process Control activities	Monitoring activities
<ul style="list-style-type: none"> • Respond to specific risks (PRPs) at the process level 	<ul style="list-style-type: none"> • Monitor the effective operation of control activities and other components of ICFR • Monitor operations to identify unusual trends or anomalies that may warrant investigation
<ul style="list-style-type: none"> • Designed with sufficient precision to prevent, or detect and correct errors 	<ul style="list-style-type: none"> • Could identify errors themselves, but that is not the objective of their design

in financial statement assertions at the 'would' level of assurance

- Designed to identify the cause of errors
- Monitor the remediation of deficiencies

Considerations for Understanding an Entity's Internal Audit Function

International Standards on Auditing: ISA 315.Appendix 4 Appendix 4 Considerations for Understanding an Entity's Internal Audit Function

(Ref: Para 14(a), 24(a)(ii), A25.A28, A118)

This appendix provides further considerations relating to understanding the entity's internal audit function when such a function exists.

Objectives and Scope of the Internal Audit Function

1. The objectives and scope of an internal audit function, the nature of its responsibilities and its status within the organization, including the function's authority and accountability, vary widely and depend on the size, complexity and structure of the entity and the requirements of management and, where applicable, those charged with governance. These matters may be set out in an internal audit charter or terms of reference.
2. The responsibilities of an internal audit function may include performing procedures and evaluating the results to provide assurance to management and those charged with governance regarding the design and effectiveness of risk management, the entity's system of internal control and governance processes. If so, the internal audit function may play an important role in the entity's process to monitor the entity's system of internal control. However, the responsibilities of the internal audit function may be focused on evaluating the economy, efficiency and effectiveness of operations and, if so, the work of the function may not directly relate to the entity's financial reporting.

Inquiries of the Internal Audit Function

3. If an entity has an internal audit function, inquiries of the appropriate individuals within the function may provide information that is useful to the auditor in obtaining an understanding of the entity and its environment, the applicable financial reporting framework and the entity's system of internal control, and in identifying and assessing risks of material misstatement at the financial statement and assertion levels. In performing its work, the internal audit function is likely to have obtained insight into the entity's operations and business risks, and may have findings based on its work, such as identified control deficiencies or risks, that may provide valuable input into the auditor's understanding of the entity and its environment, the applicable financial reporting framework, the entity's system of internal control, the auditor's risk assessments or other aspects of the audit. The auditor's inquiries are therefore made whether or not the auditor expects to use the work of the internal audit function to modify the nature or timing, or reduce the extent, of audit procedures to be performed.⁷³ Inquiries of particular relevance

may be about matters the internal audit function has raised with those charged with governance and the outcomes of the function's own risk assessment process.

73 The relevant requirements are contained in ISA 610 (Revised 2013).

4. If, based on responses to the auditor's inquiries, it appears that there are findings that may be relevant to the entity's financial reporting and the audit of the financial statements, the auditor may consider it appropriate to read related reports of the internal audit function. Examples of reports of the internal audit function that may be relevant include the function's strategy and planning documents and reports that have been prepared for management or those charged with governance describing the findings of the internal audit function's examinations.
5. In addition, in accordance with ISA 240,⁷⁴ if the internal audit function provides information to the auditor regarding any actual, suspected or alleged fraud, the auditor takes this into account in the auditor's identification of risk of material misstatement due to fraud.

74 ISA 240, paragraph 19

6. Appropriate individuals within the internal audit function with whom inquiries are made are those who, in the auditor's judgment, have the appropriate knowledge, experience and authority, such as the chief internal audit executive or, depending on the circumstances, other personnel within the function. The auditor may also consider it appropriate to have periodic meetings with these individuals.

Consideration of the Internal Audit Function in Understanding the Control Environment

7. In understanding the control environment, the auditor may consider how management has responded to the findings and recommendations of the internal audit function regarding identified control deficiencies relevant to the preparation of the financial statements, including whether and how such responses have been implemented, and whether they have been subsequently evaluated by the internal audit function.

Understanding the Role that the Internal Audit Function Plays in the Entity's Process to Monitor the System of Internal Control

8. If the nature of the internal audit function's responsibilities and assurance activities are related to the entity's financial reporting, the auditor may also be able to use the work of the internal audit function to modify the nature or timing, or reduce the extent, of audit procedures to be performed directly by the auditor in obtaining audit evidence. Auditors may be more likely to be able to use the work of an entity's internal audit function when it appears, for example, based on experience in previous audits or the auditor's risk assessment procedures, that the entity has an internal audit function that is adequately and appropriately resourced relative to the complexity of the entity and the nature of its operations, and has a direct reporting relationship to those charged with governance.

9. If, based on the auditor's preliminary understanding of the internal audit function, the auditor expects to use the work of the internal audit function to modify the nature or timing, or reduce the extent, of audit procedures to be performed, ISA 610 (Revised 2013) applies.

10. As is further discussed in ISA 610 (Revised 2013), the activities of an internal audit function are distinct from other monitoring controls that may be relevant to financial reporting, such as reviews of management accounting information that are designed to contribute to how the entity prevents or detects misstatements.

11. Establishing communications with the appropriate individuals within an entity's internal audit function early in the engagement, and maintaining such communications throughout the engagement, can facilitate effective sharing of information. It creates an environment in which the auditor can be informed of significant matters that may come to the attention of the internal audit function when such matters may affect the work of the auditor. ISA 200 discusses the importance of the auditor planning and performing the audit with professional skepticism,⁷⁵ including being alert to information that brings into question the reliability of documents and responses to inquiries to be used as audit evidence. Accordingly, communication with the internal audit function throughout the engagement may provide opportunities for internal auditors to bring such information to the auditor's attention. The auditor is then able to take such information into account in the auditor's identification and assessment of risks of material misstatement.

⁷⁵ ISA 200, paragraph 7

How do we comply with the Standards? [ISA | KAEGLDWC]

1 Not Integrated Audit | Internal Audit | Obtain an understanding of the IA function [ISA | 1126]

What do we do?

IF the entity has an internal audit function THEN obtain an understanding of the function, including by performing inquiries and other procedures

Why do we do this?

When an entity has an internal audit (IA) function, we obtain an understanding of the function and its activities. This understanding helps us:

- identify those activities that are relevant to planning the audit; and
- conclude whether we will use the IA function's work.

Understanding the function's role in monitoring of internal control over financial reporting (ICFR) in particular helps us understand the entity's monitoring activities. It may also provide information that is directly relevant to our identification and assessment of the risks of material misstatement (RMMs).

Execute the Audit

What is an IA function? [ISA | 1126.1300]

An entity's IA function performs assurance and consulting activities to management and those charged with governance that are designed to evaluate and improve the effectiveness of the entity's governance, risk management and internal control processes.

Many public entities have an IA function, often comprising one or more people who perform internal auditing activities within an entity. In some cases, other functions within an entity perform these or similar activities. In other cases, employees may be called 'internal auditors' but do not perform the internal auditing activities described in this chapter. These others are acting in the capacity of the IA function and are assessed in the similar fashion.

Do we obtain an understanding of the IA function, when the function is outsourced to a third-party service provider? [ISA | 1126.1400]

Yes. The function's title and whether the activities are performed by the entity or a third-party service provider do not solely determine whether we can use the function's work. Rather, we consider the nature of the activities and the IA function's competence, objectivity, and whether they apply a systematic and disciplined approach.

In this chapter, references to the work of the IA function include relevant activities of other functions or third-party service providers.

What IA responsibilities and activities are 'relevant to planning the audit'? [ISA | 1126.1500]

The IA responsibilities and activities are relevant to planning the audit when they relate to the entity's financial reporting. When their responsibilities and activities are relevant, we may be able to use the IA function's work to modify the nature or timing of audit procedures we will perform directly, or to reduce their extent.

The IA function can have several responsibilities, some that are relevant to our audit and some that are not. As we obtain our understanding of the IA function, it is helpful for us to focus on those activities that are relevant to our audit.

The table below sets out examples of common IA function responsibilities and activities that may be relevant to our audit.

Work performed by the IA function	Description
Evaluation of internal control	<p>Evaluate the design and implementation of controls, their operation and recommend improvements.</p> <p>For example, the IA function may plan and perform tests or other procedures to provide assurance to management and those charged with governance regarding the design, implementation and operating effectiveness of internal control, including those that are relevant to the audit (i.e. ICFR).</p>
Examination of financial and operating information	<p>Review the means used to identify, recognize, measure, classify and report financial and operating information, and to make specific inquiries into individual items, including detailed testing of transactions, balances and procedures.</p>

Review of compliance with laws and regulations	Review compliance with laws, regulations and other external requirements, and with management policies and directives and other internal requirements.
Perform risk management procedures	Identify and evaluate significant exposures to risk and contribute to the improvement of risk management and internal control. Perform procedures to help the entity to detect fraud.
Assess the governance process	Assess whether the governance process meets the entity's objectives for: <ul style="list-style-type: none">• ethics and values;• performance management and accountability;• effectively communicating risk and control information to appropriate areas of the entity; and• effective communication among those charged with governance, external and internal auditors, and management.

How do we assess whether IA activities are relevant to planning the audit? [ISA | 1126.1600]

Examples of procedures that may help with our assessment include:

- considering knowledge from prior-year audits;
- reviewing how the internal auditors allocate their audit resources to financial or operating areas in response to their risk-assessment process; and
- obtaining detailed information about the scope of IA activities by reading IA reports, the IA function's charter and the IA function's organizational chart.

How do we obtain our understanding of the IA function? [ISA | 1126.1700]

We obtain our understanding of the IA function by performing inquiries. To supplement the inquiries, we may also obtain our understanding by performing other procedures, such as:

- reading the internal audit charter or terms of reference;
- reviewing the internal audit function's audit plan for the period and discussing that plan with appropriate individuals;
- reading internal audit reports or other documents outlining the work performed; and
- reading other documents outlining the work performed by the IA function.

Do we perform inquiries even when we don't intend to use the IA function's work? [ISA | 1126.10469]

Yes. The IA function has likely obtained insight into the entity's operations and risks, and may have findings based on its work -- e.g. control deficiencies, identified risks. These findings may help us understand the entity, assess risk or perform other aspects of the audit. So we make our inquiries whether or not we intend to use the IA function's work.

Do we read IA reports when obtaining an understanding of the IA function? [ISA | 1126.10470]

We may decide to read internal audit reports when:

- our inquiries reveal findings that may be relevant to the entity's financial reporting and our audit, or
- they may provide us more information about the IA function.

Reading reports prepared for management or those charged with governance may help us conduct several areas of our audit, including:

- obtaining detailed information about the scope of IA activities;
- uncovering matters that may inform our risk assessment;
- identifying previously unknown control deficiencies;
- identifying instances of non-compliance with laws and regulations;
- detecting instances of fraud; and
- providing evidence that helps us evaluate the results of the IA function's work.

[Who do we inquire of when obtaining an understanding of the IA function?](#) [ISA | 1126.1800]

We inquire of individuals who have appropriate knowledge, experience and authority - e.g. the head of the IA function, appropriate management and other IA staff. When the entity's governance structure includes an audit committee, we may also inquire of its chair and/or members.

[What do we inquire about when obtaining an understanding of the IA function?](#) [ISA | 1126.1900]

The table below sets out areas we inquire about as we obtain our understanding of the IA function and highlights the purpose of these inquiries.

Area of inquiry	Purpose
The organizational status of the IA function within the entity	<p>Depending on the organizational status of the IA function, the function may be more or less effective.</p> <p>For example, the function may be considered as less effective or even ineffective if it reports to management because this may affect the IA function's objectivity.</p>
The IA function's nature of responsibilities	<p>Learning about the nature of the IA function's responsibilities helps us determine whether the IA function's work is relevant to the audit.</p> <p>For example, the IA function may focus on economic efficiency and operational effectiveness. These responsibilities do not necessarily relate to the entity's financial reporting and so they may not be relevant to the audit.</p>
The IA function's application of internal audit professional standards	<p>Internal audit professional standards (e.g. standards issued by the International Internal Audit Standards Board, Institute of Internal Auditors and General Accounting Office) aim to:</p> <ul style="list-style-type: none"> • impart an understanding of the role and responsibilities of the IA function; • permit measurement of the IA function's performance; and

	<ul style="list-style-type: none"> improve the practice and quality of internal audit's work.
The IA function's audit plan, including the nature, timing and extent of their work	An IA plan may provide insights about, among other things, the IA function's areas of focus, how much time was allocated to the work, and who performed it. This helps us to understand whether the work may be relevant to our audit and form initial views about how it could be used to modify our audit procedures.
The IA function's access to records and whether there are limits on the scope for their activities	Limits imposed by management or those charged with governance on the IA function's access to documents and other sources of information relevant to its activities and/or on the function's scope may indicate that the function is less effective.

When do we make inquiries to gain an understanding of the IA function? [ISA | 1126.2000]

We make inquiries to gain an understanding of the IA function during risk assessment and audit planning. We update this understanding throughout the audit.

How can the IA function's work help us in our audit? [ISA | 1126.2100]

The IA function's work can provide information about the entity that is helpful during risk assessment and audit planning. In some cases, their work may allow us to modify the nature or timing of audit procedures we perform, or reduce their extent.

The table below sets out examples of how the work of the IA function may affect our audit approach.

IA function's work	Impact on our approach
Preparation of reports detailing work they have performed	Reviewing these reports may help us identify matters that could influence our risk assessment and audit plan
Review, assess and monitor controls	When we use the procedures performed by the internal auditors in this area, we may gain useful information about the entity's internal controls and possibly reduce the nature, timing, and/or extent of the procedures necessarily to test controls
Flowcharting procedures performed by entity	Reviewing these flowcharts may provide us with information about the entity's business processes and the design of relevant controls
Work performed over a number of locations	We may be able to reduce the number of locations where we perform audit procedures

Considerations for Understanding Information Technology (IT)

International Standards on Auditing: ISA 315.Appendix 5 Appendix 5 Considerations for Understanding Information Technology (IT)

(Ref: Para. 25(a), 26(b).(c), A94, A166.A172)

This appendix provides further matters that the auditor may consider in understanding the entity's use of IT in its system of internal control.

Understanding the Entity's Use of Information Technology in the Components of the Entity's System of Internal Control

1. An entity's system of internal control contains manual elements and automated elements (i.e., manual and automated controls and other resources used in the entity's system of internal control). An entity's mix of manual and automated elements varies with the nature and complexity of the entity's use of IT. An entity's use of IT affects the manner in which the information relevant to the preparation of the financial statements in accordance with the applicable financial reporting framework is processed, stored and communicated, and therefore affects the manner in which the entity's system of internal control is designed and implemented. Each component of the entity's system of internal control may use some extent of IT.

Generally, IT benefits an entity's system of internal control by enabling an entity to:

- Consistently apply predefined business rules and perform complex calculations in processing large volumes of transactions or data;
- Enhance the timeliness, availability and accuracy of information;
- Facilitate the additional analysis of information;
- Enhance the ability to monitor the performance of the entity's activities and its policies and procedures;
- Reduce the risk that controls will be circumvented; and
- Enhance the ability to achieve effective segregation of duties by implementing security controls in IT applications, databases and operating systems.

2. The characteristics of manual or automated elements are relevant to the auditor's identification and assessment of the risks of material misstatement, and further audit procedures based thereon. Automated controls may be more reliable than manual controls because they cannot be as easily bypassed, ignored, or overridden, and they are also less prone to simple errors and mistakes. Automated controls may be more effective than manual controls in the following circumstances:

- High volume of recurring transactions, or in situations where errors that can be anticipated or predicted can be prevented, or detected and corrected, through automation.
- Controls where the specific ways to perform the control can be adequately designed and automated.

Understanding the Entity's Use of Information Technology in the Information System (Ref: Para. 25(a))

3. The entity's information system may include the use of manual and automated elements, which also affect the manner in which transactions are initiated, recorded, processed, and reported. In particular, procedures to initiate, record, process and report transactions may be enforced through the IT applications used by the entity, and how the entity has configured those applications. In addition, records in the form of digital information may replace or supplement records in the form of paper documents.

4. In obtaining an understanding of the IT environment relevant to the flows of transactions and information processing in the information system, the auditor gathers information about the nature and characteristics of the IT applications used, as well as the supporting IT infrastructure and IT. The following table includes examples of matters that the auditor may consider in obtaining the understanding of the IT environment and includes examples of typical characteristics of IT environments based on the complexity of IT applications used in the entity's information system. However, such characteristics are directional and may differ depending on the nature of the specific IT applications in use by an entity.

	Examples of typical characteristics of:		
	Non-complex commercial software	Mid-size and moderately complex commercial software or IT applications	Large or complex IT applications (e.g., ERP systems)
Matters related to extent of automation and use of data:			
<ul style="list-style-type: none"> • The extent of automated procedures for processing, and the complexity of those procedures, including, whether there is highly automated, paperless processing. 	N/A	N/A	Extensive and often complex automated procedures

<ul style="list-style-type: none"> The extent of the entity's reliance on system-generated reports in the processing of information. 	Simple automated report logic	Simple relevant automated report logic	Complex automated report logic; Report-writer software
<ul style="list-style-type: none"> How data is input (i.e., manual input, customer or vendor input, or file load). 	Manual data inputs	Small number of data inputs or simple interfaces	Large number of data inputs or complex interfaces
<ul style="list-style-type: none"> How IT facilitates communication between applications, databases or other aspects of the IT environment, internally and externally, as appropriate, through system interfaces. 	No automated interfaces (manual inputs only)	Small number of data inputs or simple interfaces	Large number of data inputs or complex interfaces
<ul style="list-style-type: none"> The volume and complexity of data in digital form being processed by the information system, including whether accounting records or other information are stored in 	Low volume of data or simple data that is able to be verified manually; Data available locally	Low volume of data or simple data	Large volume of data or complex data; Data warehouses; ⁷⁶ Use of internal or external IT service providers (e.g., third-party storage or hosting of data)

digital form and the location of stored data.			
Matters related to the IT applications and IT infrastructure:			
<ul style="list-style-type: none"> The type of application (e.g., a commercial application with little or no customization, or a highly-customized or highly-integrated application that may have been purchased and customized, or developed in-house). 	Purchased application with little or no customization	Purchased application or simple legacy or low-end ERP applications with little or no customization	Custom developed applications or more complex ERPs with significant customization
<ul style="list-style-type: none"> The complexity of the nature of the IT applications and the underlying IT infrastructure. 	Small, simple laptop or client server-based solution	Mature and stable mainframe, small or simple client server, software as a service cloud	Complex mainframe, large or complex client server, web-facing, infrastructure as a service cloud
<ul style="list-style-type: none"> Whether there is third-party hosting or outsourcing of IT. 	If outsourced, competent, mature, proven provider (e.g., cloud provider)	If outsourced, competent, mature, proven provider (e.g., cloud provider)	Competent, mature proven provider for certain applications and new or start-up provider for others
<ul style="list-style-type: none"> Whether the entity is using emerging technologies that affect 	No use of emerging technologies	Limited use of emerging technologies in some applications	Mixed use of emerging technologies across platforms

its financial reporting.			
Matters related to IT processes:			
<ul style="list-style-type: none"> The personnel involved in maintaining the IT environment (the number and skill level of the IT support resources that manage security and changes to the IT environment). 	Few personnel with limited IT knowledge to process vendor upgrades and manage access	Limited personnel with IT skills / dedicated to IT	Dedicated IT departments with skilled personnel, including programming skills
<ul style="list-style-type: none"> The complexity of processes to manage access rights. 	Single individual with administrative access manages access rights	Few individuals with administrative access manage access rights	Complex processes managed by IT department for access rights
<ul style="list-style-type: none"> The complexity of the security over the IT environment, including vulnerability of the IT applications, databases, and other aspects of the IT environment to cyber risks, particularly when there are web-based transactions or transactions involving 	Simple on-premise access with no external web-facing elements	Some web-based applications with primarily simple, role-based security	Multiple platforms with web-based access and complex security models

external interfaces.			
<ul style="list-style-type: none"> Whether program changes have been made to the manner in which information is processed, and the extent of such changes during the period. 	Commercial software with no source code installed	Some commercial applications with no source code and other mature applications with a small number or simple changes; traditional systems development lifecycle	New or large number or complex changes, several development cycles each year
<ul style="list-style-type: none"> The extent of change within the IT environment (e.g., new aspects of the IT environment or significant changes in the IT applications or the underlying IT infrastructure). 	Changes limited to version upgrades of commercial software	Changes consist of commercial software upgrades, ERP version upgrades, or legacy enhancements	New or large number or complex changes, several development cycles each year, heavy ERP customization
<ul style="list-style-type: none"> Whether there was a major data conversion during the period and, if so, the nature and significance of the changes made, and how the conversion was undertaken. 	Software upgrades provided by vendor; No data conversion features for upgrade	Minor version upgrades for commercial software applications with limited data being converted	Major version upgrade, new release, platform change

76 A data warehouse is generally described as a central repository of integrated data from one or more disparate sources (such as multiple databases) from which reports may be generated or that may be used by the entity for other data analysis activities. A report-writer is an IT application that is used to extract data from one or more sources (such as a data warehouse, a database or an IT application) and present the data in a specified format.

Emerging Technologies

5. Entities may use emerging technologies (e.g., blockchain, robotics or artificial intelligence) because such technologies may present specific opportunities to increase operational efficiencies or enhance financial reporting. When emerging technologies are used in the entity's information system relevant to the preparation of the financial statements, the auditor may include such technologies in the identification of IT applications and other aspects of the IT environment that are subject to risks arising from the use of IT. While emerging technologies may be seen to be more sophisticated or more complex compared to existing technologies, the auditor's responsibilities in relation to IT applications and identified general IT controls in accordance with paragraph 26(b).(c) remain unchanged.

Scalability

6. Obtaining an understanding of the entity's IT environment may be more easily accomplished for a less complex entity that uses commercial software and when the entity does not have access to the source code to make any program changes. Such entities may not have dedicated IT resources but may have a person assigned in an administrator role for the purpose of granting employee access or installing vendor-provided updates to the IT applications. Specific matters that the auditor may consider in understanding the nature of a commercial accounting software package, which may be the single IT application used by a less complex entity in its information system, may include:

- The extent to which the software is well established and has a reputation for reliability;
- The extent to which it is possible for the entity to modify the source code of the software to include additional modules (i.e., add-ons) to the base software, or to make direct changes to data;
- The nature and extent of modifications that have been made to the software. Although an entity may not be able to modify the source code of the software, many software packages allow for configuration (e.g., setting or amending reporting parameters). These do not usually involve modifications to source code; however, the auditor may consider the extent to which the entity is able to configure the software when considering the completeness and accuracy of information produced by the software that is used as audit evidence; and
- The extent to which data related to the preparation of the financial statements can be directly accessed (i.e., direct access to the database without using the IT application) and the volume of data that is processed. The greater the volume of data, the more likely the entity may need controls that address maintaining the integrity of the data, which may include general IT controls over unauthorized access and changes to the data.

7. Complex IT environments may include highly-customized or highly-integrated IT applications and may therefore require more effort to understand. Financial reporting processes or IT applications may be integrated with other IT applications. Such integration may involve IT applications that are used in the entity's business operations and that provide information to the IT applications relevant to the flows of transactions and information processing in the entity's information system. In such circumstances, certain IT applications used in the entity's business operations may also be relevant to the preparation of the financial statements. Complex IT environments also may require dedicated IT departments that have structured IT processes supported by personnel that have software development and IT environment

maintenance skills. In other cases, an entity may use internal or external service providers to manage certain aspects of, or IT processes within, its IT environment (e.g., third-party hosting).

Identifying IT Applications that are Subject to Risks Arising from the use of IT

8. Through understanding the nature and complexity of the entity's IT environment, including the nature and extent of information processing controls, the auditor may determine which IT applications the entity is relying upon to accurately process and maintain the integrity of financial information. The identification of IT applications on which the entity relies may affect the auditor's decision to test the automated controls within such IT applications, assuming that such automated controls address identified risks of material misstatement. Conversely, if the entity is not relying on an IT application, the automated controls within such IT application are unlikely to be appropriate or sufficiently precise for purposes of operating effectiveness tests. Automated controls that may be identified in accordance with paragraph 26(b) may include, for example, automated calculations or input, processing and output controls, such as a three-way match of a purchase order, vendor shipping document, and vendor invoice. When automated controls are identified by the auditor and the auditor determines through the understanding of the IT environment that the entity is relying on the IT application that includes those automated controls, it may be more likely for the auditor to identify the IT application as one that is subject to risks arising from the use of IT.

9. In considering whether the IT applications for which the auditor has identified automated controls are subject to risks arising from the use of IT, the auditor is likely to consider whether, and the extent to which, the entity may have access to source code that enables management to make program changes to such controls or the IT applications. The extent to which the entity makes program or configuration changes and the extent to which the IT processes over such changes are formalized may also be relevant considerations. The auditor is also likely to consider the risk of inappropriate access or changes to data.

10. System-generated reports that the auditor may intend to use as audit evidence may include, for example, a trade receivable aging report or an inventory valuation report. For such reports, the auditor may obtain audit evidence about the completeness and accuracy of the reports by substantively testing the inputs and outputs of the report. In other cases, the auditor may plan to test the operating effectiveness of the controls over the preparation and maintenance of the report, in which case the IT application from which it is produced is likely to be subject to risks arising from the use of IT. In addition to testing the completeness and accuracy of the report, the auditor may plan to test the operating effectiveness of general IT controls that address risks related to inappropriate or unauthorized program changes to, or data changes in, the report.

11. Some IT applications may include report-writing functionality within them while some entities may also utilize separate report-writing applications (i.e., report-writers). In such cases, the auditor may need to determine the sources of system-generated reports (i.e., the application that prepares the report and the data sources used by the report) to determine the IT applications subject to risks arising from the use of IT.

12. The data sources used by IT applications may be databases that, for example, can only be accessed through the IT application or by IT personnel with database administration privileges. In other cases, the data source may be a data warehouse that may itself be considered to be an IT application subject to risks arising from the use of IT.

13. The auditor may have identified a risk for which substantive procedures alone are not sufficient because of the entity's use of highly-automated and paperless processing of transactions, which may involve multiple integrated IT applications. In such circumstances, the controls identified by the auditor are likely to include automated controls. Further, the entity may be relying on general IT controls to maintain the integrity of the transactions processed and other information used in processing. In such cases, the IT applications involved in the processing and the storage of the information are likely subject to risks arising from the use of IT.

End-User Computing

14. Although audit evidence may also come in the form of system-generated output that is used in a calculation performed in an end-user computing tool (e.g., spreadsheet software or simple databases), such tools are not typically identified as IT applications in the context of paragraph 26(b). Designing and implementing controls around access and change to end-user computing tools may be challenging, and such controls are rarely equivalent to, or as effective as, general IT controls. Rather, the auditor may consider a combination of information processing controls, taking into account the purpose and complexity of the end-user computing involved, such as:

- Information processing controls over the initiation and processing of the source data, including relevant automated or interface controls to the point from which the data is extracted (i.e., the data warehouse);
- Controls to check that the logic is functioning as intended, for example, controls which 'prove' the extraction of data, such as reconciling the report to the data from which it was derived, comparing the individual data from the report to the source and vice versa, and controls which check the formulas or macros; or
- Use of validation software tools, which systematically check formulas or macros, such as spreadsheet integrity tools.

Scalability

15. The entity's ability to maintain the integrity of information stored and processed in the information system may vary based on the complexity and volume of the related transactions and other information. The greater the complexity and volume of data that supports a significant class of transactions, account balance or disclosure, the less likely it may become for the entity to maintain integrity of that information through information processing controls alone (e.g., input and output controls or review controls). It also becomes less likely that the auditor will be able to obtain audit evidence about the completeness and accuracy of such information through substantive testing alone when such information is used as audit evidence. In some circumstances, when volume and complexity of transactions are lower, management may have an information processing control that is sufficient to verify the accuracy and completeness of the data (e.g., individual sales orders processed and billed may be reconciled to the hard copy originally entered into the IT application). When the entity relies on general IT controls to maintain the integrity of certain information used by IT applications, the auditor may determine that the IT applications that maintain that information are subject to risks arising from the use of IT.

Example characteristics of an IT application that is likely not subject to risks arising from IT	Example characteristics of an IT application that is likely subject to risks arising from IT

<ul style="list-style-type: none"> • Standalone applications. • The volume of data (transactions) is not significant. • The application's functionality is not complex. • Each transaction is supported by original hard copy documentation. 	<ul style="list-style-type: none"> • Applications are interfaced. • The volume of data (transactions) is significant. • The application's functionality is complex as: <ul style="list-style-type: none"> - The application automatically initiates transactions; and - There are a variety of complex calculations underlying automated entries.
<p>IT application is likely not subject to risks arising from IT because:</p> <ul style="list-style-type: none"> • The volume of data is not significant and therefore management is not relying upon general IT controls to process or maintain the data. • Management does not rely on automated controls or other automated functionality. The auditor has not identified automated controls in accordance with paragraph 26(a). • Although management uses system-generated reports in their controls, it does not rely on these reports. Instead, it reconciles the reports back to the hard copy documentation and verifies the calculations in the reports. • The auditor will directly test information produced by the entity used as audit evidence. 	<p>IT application is likely subject to risks arising from IT because:</p> <ul style="list-style-type: none"> • Management relies on an application system to process or maintain data as the volume of data is significant. • Management relies upon the application system to perform certain automated controls that the auditor has also identified.

Other Aspects of the IT Environment that Are Subject to Risks Arising from the Use of IT

16. When the auditor identifies IT applications that are subject to risks arising from the use of IT, other aspects of the IT environment are also typically subject to risks arising from the use of IT. The IT infrastructure includes the databases, operating system, and network. Databases store the data used by IT applications and may consist of many interrelated data tables. Data in databases may also be accessed directly through database management systems by IT or other personnel with database administration privileges. The operating system is responsible for managing communications between hardware, IT applications, and other software used in the network. As such, IT applications and databases may be directly accessed through the operating system. A network is used in the IT

infrastructure to transmit data and to share information, resources and services through a common communications link. The network also typically establishes a layer of logical security (enabled through the operating system) for access to the underlying resources.

17. When IT applications are identified by the auditor to be subject to risks arising from IT, the database(s) that stores the data processed by an identified IT application is typically also identified. Similarly, because an IT application's ability to operate is often dependent on the operating system and IT applications and databases may be directly accessed from the operating system, the operating system is typically subject to risks arising from the use of IT. The network may be identified when it is a central point of access to the identified IT applications and related databases or when an IT application interacts with vendors or external parties through the internet, or when web-facing IT applications are identified by the auditor.

Identifying Risks Arising from the Use of IT and General IT Controls

18. Examples of risks arising from the use of IT include risks related to inappropriate reliance on IT applications that are inaccurately processing data, processing inaccurate data, or both, such as

- Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or non-existent transactions, or inaccurate recording of transactions. Particular risks may arise where multiple users access a common database.
- The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties.
- Unauthorized changes to data in master files.
- Unauthorized changes to IT applications or other aspects of the IT environment.
- Failure to make necessary changes to IT applications or other aspects of the IT environment.
- Inappropriate manual intervention.
- Potential loss of data or inability to access data as required.

19. The auditor's consideration of unauthorized access may include risks related to cybersecurity risks. Such risks may not necessarily affect financial reporting, as an entity's IT environment may also include IT applications and related data that address operational or compliance needs. It is important to note that cyber incidents usually first occur through the perimeter and internal network layers, which tend to be further removed from the IT application, database and operating systems that affect the preparation of the financial statements. Accordingly, if information about a security breach has been identified, the auditor ordinarily considers the extent to which such a breach had the potential to affect financial reporting. If financial reporting may be affected, the auditor may decide to understand, and test the related controls to determine the possible impact or scope of potential misstatements in the financial statements or may determine that the entity has provided adequate disclosures in relation to such security breach.

20. In addition, laws and regulations that may have a direct or indirect effect on the entity's financial statements may include data protection legislation. Considering an entity's compliance with such laws or regulations, in accordance with ISA 250 (Revised),⁷⁷ may involve understanding the entity's IT processes and general IT controls that the entity has implemented to address the relevant laws or regulations.

77 ISA 250 (Revised)

21. General IT controls are implemented to address risks arising from the use of IT. Accordingly, the auditor uses the understanding obtained about the identified IT applications and other aspects of the IT

environment and the applicable risks arising from the use of IT in determining the general IT controls to identify. In some cases, an entity may use common IT processes across its IT environment or across certain IT applications, in which case common risks arising from the use of IT and common general IT controls may be identified.

22. In general, a greater number of general IT controls related to IT applications and databases are likely to be identified than for other aspects of the IT environment. This is because these aspects are the most closely concerned with the information processing and storage of information in the entity's information system. In identifying general IT controls, the auditor may consider controls over actions of both end users and of the entity's IT personnel or IT service providers.

23. Appendix 6 provides further explanation of the nature of the general IT controls typically implemented for different aspects of the IT environment. In addition, examples of general IT controls for different IT processes are provided.

How do we comply with the Standards? [ISA | KAEGHDWC]

1 Understand how the entity uses IT as part of financial reporting [ISA | 1325]

What do we do?

Obtain an understanding of how the entity uses IT and how IT affects the entity's flow of transactions and the financial statements by understanding the IT environment.

Why do we do this?

Understanding how the entity uses IT as part of financial reporting provides information that's useful when:

- determining whether the entity highly depends on IT processing,
- identifying and assessing risks of material misstatement (RMMs),
- obtaining an understanding of business processes, including process risk points (PRPs) and relevant automated process control activities,
- identifying the relevant IT layers, risks arising from IT (RAFITs) and relevant general IT controls (GITCs),
- identifying information we plan to use in the audit, and
- designing substantive audit procedures.

Execute the Audit

How do entities use IT systems? [ISA | 1325.1400]

Entities often use IT systems extensively within their information systems and in business processes to help them:

- manage and operate their business;
- maintain their financial records;

- and report financial results both internally and externally.

Entities may choose to automate certain processes using IT systems - including control activities to mitigate risks - to enhance efficiency and effectiveness. Automation may be particularly common when processing and reporting larger volumes of transactions, or when processing and aggregating information or data elements is not feasible without using IT systems.

A wide range of software may be part of an entity's financial reporting IT systems, including ERP systems that integrate multiple layers of technology. Common ERP software vendors include Microsoft, Oracle and SAP. In addition, many entities develop custom software to meet their specific needs or outsource IT services to service organizations, such as cloud computing (see question "[What additional considerations are there if the entity outsources cloud computing?](#)" and sub-questions for more information).

[How might service-organization-managed services affect business processes?](#) [ISA | 1325.10452]

Using service-organization-managed services may have a pervasive effect on the flow of an entity's transactions in one or many business processes. Some of these service organizations may not produce service auditor reports, which can make obtaining an understanding of the entity's information system challenging.

Using service organizations may also result in unique risks because the entity has given up control of some or all of its IT systems, while retaining responsibility for its information systems and ICFR.

In view of the wide variety of outsourced services offered and potential structures, understanding how the entity uses IT and its effect on the financial statements, and identifying and testing general IT controls, can be difficult. Using specific team members (STMs) with expertise in IT (IT Audit STMs) to help us obtain an understanding can be beneficial.

[Who do we involve in obtaining an understanding of an entity's use of IT?](#) [ISA | 1325.2100]

When obtaining an understanding of the entity's use of IT, we determine whether to involve specific team members (STMs) with expertise in IT (IT Audit STMs). See activity '[Involve specific team members with expertise in Tax and IT as appropriate](#)' for information on:

- when we involve IT Audit depending on the type of entity we are auditing,
- when we may involve IT Audit, and
- how we involve IT Audit in our audit, including what are some common areas where IT Audit is involved.

Even if we involve IT Audit, we remain responsible for obtaining an understanding of the entity's use of IT as part of financial reporting.

[How do we obtain an understanding of how the entity uses IT as part of financial reporting?](#) [ISA | 1325.2200]

Obtaining an understanding of how the entity uses IT as part of financial reporting involves obtaining an understanding of an entity's overall IT environment, which includes:

- [understanding the IT systems the entity uses as part of its financial reporting and business processes relevant to the preparation of the financial statements](#), including the various layers of technology that make up the IT system (applications, databases, operating systems and networks);
- [understanding the entity's IT processes to manage the IT environment](#);

- [understanding the entity's IT organization](#); and
- [understanding cybersecurity risks and incidents](#).

Additionally, as part of obtaining an understanding of the entity's business processes and financial reporting process relevant to the preparation of the financial statements, we also obtain and/or confirm our understanding of how IT affects the entity's flow of transactions, accounting records and disclosures related to each process (see activity "[Understand business processes](#)" and sub-activities for further information).

[How may the complexity of the entity's IT environment impact our understanding of the entity's use of IT?](#)

[ISA | 1325.8676]

While the use of IT may be significant in entities with less complex IT environments, extensive descriptions of accounting and IT procedures, sophisticated accounting records, or written policies may not be available. Understanding the entity's IT environment may be easier and it may be more dependent on inquiry than on review of documentation.

When an entity has greater complexity in its IT environment, it is likely that we involve specific team members with expertise in IT in identifying the IT systems and other aspects of the IT environment, determining the related risks arising from IT, and identifying general IT controls. Such involvement is likely to be essential and may be more extensive for complex IT environments. Refer to the activity "[Involve specific team members with expertise in Tax and IT as appropriate](#)" for further information on when to involve IT Audit.

The extent of our understanding of the IT processes varies with the nature and the circumstances of the entity and its IT environment. The complexity of the IT environment may also impact the extent to which the entity has general IT controls in place, as well as the number of IT system layers that are subject to risks arising from IT.

[What do we document when we obtain an understanding of how the entity uses IT as part of financial reporting?](#) [ISA | 1325.10455]

We document:

- the key elements of our understanding,
- the risk assessment procedures performed, and
- the sources of information from which our understanding was obtained.

Examples

[What procedures might we perform to obtain an understanding of how the entity uses IT as part of financial reporting?](#) [ISA | 1325.3000]

Fact pattern:

When obtaining an understanding of how the entity uses IT as part of financial reporting, the engagement team decides to perform a combination of inquiry and inspection procedures.

Analysis

Example procedures that the engagement team may perform to obtain an understanding of the entity's IT systems IT processes and IT organization include:

- Inquiry of management (CIO/ IT director/ Head of IT/ IT manager) to obtain an understanding of matters such as:
 - the structure of IT governance;
 - an overview of the entity's IT infrastructure;
 - how IT is used to support financial reporting/ business processes that impact financial reporting;
 - relevant IT systems used for financial and business operations, including the various layers of technology that make up the IT system (applications, databases, operating systems and networks);
 - how systems interface/transfer data;
 - the extent of end-user computing in financial reporting;
 - recently implemented and new or upcoming IT projects;
 - significant upgrades or changes to relevant layers of technology;
 - management's assessment of significant IT risks;
 - the extent of reliance on centralized services, including shared service centers, and/or third-party service providers;
 - the use of any report writers, data warehouses, utility tools or ticketing tools in the processing of financial data or implementation/operation of automated controls;
 - the use of any Robotic Process Automation (RPA) and if used, its level of sophistication; and
 - the entity's IT processes to manage:
 - access to programs and data
 - program changes
 - program acquisition and development (e.g. Agile development or a more traditional approach)
 - computer operations.
- Inspection of documentation, when available, such as:
 - IT organization chart;
 - Description of IT processes to manage:
 - access to programs and data
 - program changes
 - program acquisition & development
 - computer operations;
 - Cybersecurity risk assessment;
 - IT governance / steering group meeting minutes;
 - service organization contract(s) relating to IT;
 - recent internal audit report(s) relating to IT ; and
 - evaluation report(s) (or other relevant documentation) describing the outcome of IT system(s) implemented or upgraded/ changed in the period.
- Inquiry of management (CEO/ COO/ CFO/ Head of Accounting) to obtain an understanding of matters such as:
 - the dependency of financial reporting/ business processes that impact financial reporting on the use of IT;

- the extent of end-user computing in financial reporting;
- recently completed and currently ongoing IT projects and known/ expected impact on the financial reporting process/ business operations;
- any recent or ongoing IT issues that impact the financial reporting process/ business operations; and
- any envisioned changes to IT that impact business processes and financial reporting.

What matters might we consider when obtaining an understanding of a less complex IT environment? [ISA | 1325.8677]

Fact pattern:

An entity's use of IT as part of financial reporting consists of a single commercial accounting software.

Analysis

Obtaining an understanding of an entity's use of IT may be more easily accomplished in a less complex IT environment that uses an "off-the-shelf" single commercial accounting software (e.g. QuickBooks). Matters that the engagement team may consider in understanding the nature of a single commercial accounting software may include:

- The nature and extent of modifications that have been made to the software (e.g., setting or amending reporting parameters);
- The extent to which it is possible for the entity to modify the source code of the software to include additional modules (i.e., add-ons) to the base software, or to make direct changes to data;
- The extent to which data related to the preparation of the financial statements can be directly accessed (i.e., direct access to the database without using the IT application) and the volume of data that is processed; and
- The extent to which the software is well established and has a reputation for reliability.

1.1 Understand the entity's IT systems [ISA | 7589]

What do we do?

Obtain an understanding of the IT systems the entity uses as part of its financial reporting and business processes relevant to the preparation of the financial statements.

Why do we do this?

We obtain an understanding of the IT systems the entity uses as part of its financial reporting and business processes relevant to the preparation of the financial statements in order to understand how the entity uses IT and how IT affects the entity's flow of transactions and the financial statements.

Execute the audit

How do we obtain an understanding of the IT systems used by the entity? [ISA | 7589.10383]

For each IT system used by the entity as part of its financial reporting and business processes relevant to the preparation of the financial statements, we obtain at a minimum an understanding of the elements that are set out in the table below.

Element	Description
Name of IT system	<p>The name of the IT system the entity uses, including:</p> <ul style="list-style-type: none"> • whether it was purchased from an outside vendor or developed internally; and • the name of the vendor (if applicable).
Purpose of the IT system	<p>A description of how the entity uses the IT system as part of its financial reporting and business processes.</p>
Processes using the IT system	<p>A list of the accounting and financial reporting processes that use the IT system.</p>
Components using the IT system	<p>If applicable, a list of the entity's components (subsidiaries, divisions or locations) that use the IT system.</p>
Layers of technology within the IT system	<p>For each layer of technology that comprise the IT system - i.e. application layer, database layer, operating system layer and network layer:</p> <ul style="list-style-type: none"> • Title and version • Significant upgrades <p>Description of any significant upgrades to the IT layer/system during the period. For example:</p> <ul style="list-style-type: none"> - the implementation of a new IT layer/system; - upgrades to the existing IT layer/system; - upgrades to layers of the IT system, such as the underlying database for the application; or - upgrades to the operating system that the database runs on. <ul style="list-style-type: none"> • Extent of customization and/or changes <p>Whether the IT layer/system has been customized and the nature of the customization, and whether significant changes have been made.</p> <ul style="list-style-type: none"> • Extent of outsourcing <p>Whether the IT layer/system has been outsourced, and the nature of the outsourcing - e.g. an outsourced data center that hosts the entity's IT system, or an outsourced Cloud-based IT system.</p>

	Note: The same database layer may support more than one IT application and, therefore, be part of more than one IT system. Also, the operating system may support more than one IT application and database.
--	--

We may also prepare or include an IT systems diagram (ISD) or other documentation as part of our understanding.

Additionally, the entity may use emerging technologies (e.g., robotic process automation (RPA), blockchain, or artificial intelligence) because such technologies may present specific opportunities to increase operational efficiencies or enhance financial reporting. When emerging technologies are used in the entity's information system relevant to the preparation of the financial statements, we may include such technologies in our understanding of the entity's IT systems and the layers of technology.

[What are IT systems diagrams?](#) [ISA | 7589.10384]

An IT systems diagram (ISD) is a graphical depiction of the IT systems an entity uses- including the layers of technology within those systems.

[Why are ISDs useful when obtaining an understanding of an entity's use of IT systems?](#) [ISA | 7589.10385]

An ISD helps us to simplify our understanding of the entity's IT systems and the layers of technology within those systems. Understanding the layers of technology that make up an IT system can become complex - especially when the entity uses multiple IT systems that comprise many different layers of technology.

This simplified understanding may help us:

- evaluate whether we have a sufficient understanding of the entity's use of IT systems; and
- identify risk arising from the entity's use of IT that could affect the continued effective operation of automated controls or the integrity of data and information residing within those systems.

[Can an ISD be used to document our understanding of the flow of data and information through IT systems?](#) [ISA | 7589.10386]

No, because ISDs show the relationships between layers of IT, not the flow of data or transactions through the IT system or through a business process.

While the ISD helps us understand the IT systems and the layers of technology within those IT systems, we capture and document the flow of data and information as part of our understanding of the business processes (see activity '[Understand business processes](#)' for more information).

[What are the layers of technology that comprise an IT system?](#) [ISA | 7589.10387]

IT systems are comprised of four types of layers of technology (also referred to as IT system layers or IT layers), which are the application, database, operating system and network layers (the last three layers may be collectively referred to as IT infrastructure). Each of these layers of technology may present risks arising from IT (RAFITS) to be controlled by management so that:

- automated controls operate and function effectively; or
- the integrity of data and information sourced from an entity's IT system is maintained.

The table below provides a description of each of the layers of technology.

Layer	Description
Application	<p>Applications are the layers of IT systems designed to perform one or many functions, tasks or activities - often to capture, process or extract data. Applications often include an interface accessed by an end-user.</p> <p>An IT application is a program or a set of programs that is used in the initiation, processing, recording and reporting of transactions or information. Examples of the application layer of an IT system include:</p> <ul style="list-style-type: none"> • ERP systems, such as SAP and Oracle; • report writers, • emerging technologies, such as robotic process automation (RPA), artificial intelligence; and • transaction-processing systems, such as a CRM or billing system.
Database	<p>Databases are the layers of IT systems that organize a collection of data or information so that it can be easily accessed, managed and updated. This includes data warehouses, which are separate applications that we consider as a database layer.</p> <p>SQL Server and Oracle DB, as well as stand-alone data repositories and data warehouses, are examples of the database layer of an IT system. Technologies such as MS SQL Server may be used by an entity for multiple IT systems to access information in the database.</p>
Operating system	<p>Operating systems are the layers of IT systems that control the basic operation of a computer and provide a software platform on which to run other software, such as applications and databases.</p> <p>The operating system generally works behind the scenes and is usually not manipulated directly by the end user.</p> <p>UNIX, LINUX, Microsoft Windows and MacOS are examples of the operating system layer of an IT system.</p>
Network	<p>Networks are the layers of IT systems that transport information or data between computers, either within an organization or between organizations.</p> <p>Access to IT applications may be restricted to users on a particular network - e.g. users cannot access an IT application outside of a local area network (LAN) or virtual private network (VPN).</p> <p>Wide area networks (WANs), LANs and VPNs are examples of the network layer of an IT system.</p>

Why do we understand the layers of technology that comprise an IT system? [ISA | 7589.10388]

We understand the layers of technology that comprise an IT system because:

- Data and information related to transactions and other events and conditions relevant to an entity's financial reporting may flow through multiple IT systems and the layers of technology within those systems.
- An entity may also design and implement automated controls within any layer of technology in an IT system. Thus, [risks arising from IT](#) (RAFITS) may exist in some or all of the layers of technology that make up an IT system.
- Not all layers of technology may be relevant to our audit, so understanding the layers helps us determine the specific layers that impact our audit approach.

What are report writers? [ISA | 7589.10389]

Report writers are a specific type of application whose function is to extract information or data, often from a database or data warehouse, and present that information or data in a specified format such as a report.

Entities often use these application layers as part of their financial reporting and business processes to produce data and information used in the operation of controls.

Report writers include:

- separate report writer applications;
- report writer functionality integrated into another IT application (e.g. within an ERP system); or
- report writer functionality integrated into an end-user computing environment (e.g. within Microsoft Excel).

What is robotic process automation (RPA)? [ISA | 7589.10390]

Robotic process automation (RPA), also referred to as 'robotics' or 'bots', is an emerging type of application used to automate manual tasks within a workflow. These tasks are generally repetitive, low judgment, and high-volume in nature and are often associated with processes that follow explicit or predictable rules and prescriptive steps. Bots may rely on end-users to trigger the activity (i.e. attended bots) or run independently, enabling work to be scheduled or completed continuously (i.e. unattended bots).

What is a data warehouse? [ISA | 7589.10391]

Data warehouses are separate applications that are database layers used as a central repository to accumulate and integrate data and information from a wide range of sources, e.g. multiple databases or other IT systems used in financial reporting and business processes, from which reports may be generated or that may be used by the entity for other data analysis activities. Data warehouses are often the source of data and information used in the operation of controls.

How do we identify report writers, RPA and data warehouses used in an entity's financial reporting and business processes? [ISA | 7589.10392]

We identify report writers, RPA and data warehouses when we obtain an understanding of the business processes - specifically, when we carefully consider and understand how the data is transferred to the report writer/data warehouse, where it is stored and how it is manipulated, extracted and reported.

Examples

What is included in our understanding of an entity's IT systems? [ISA | 7589.10393]

Fact pattern:

Consider an entity (Daisy Inc.) that uses:

- Hyperion for the consolidation process;
- Oracle Financials for the general ledger and sales and purchases processes; and
- Oracle HR for the HR/payroll process.

Each application is hosted in the entity's Boston data center.

Oracle Financials and Oracle HR run on a Unix A|X operating system and Oracle Database and are supported by the local IT group in Boston.

Hyperion runs on a Windows 10 operating system and SQL Server 2019 database and is supported by the IT group in the entity's corporate office in New York.

The consolidation application, Hyperion, was upgraded from Hyperion Enterprise to Hyperion Financial Management (HFM) in February of the current period. This was a major upgrade, which required replacing hardware, converting data, and installing and configuring new servers - including upgrading the operating systems to Windows 10 and upgrading the databases to SQL Server 2019.

Analysis:

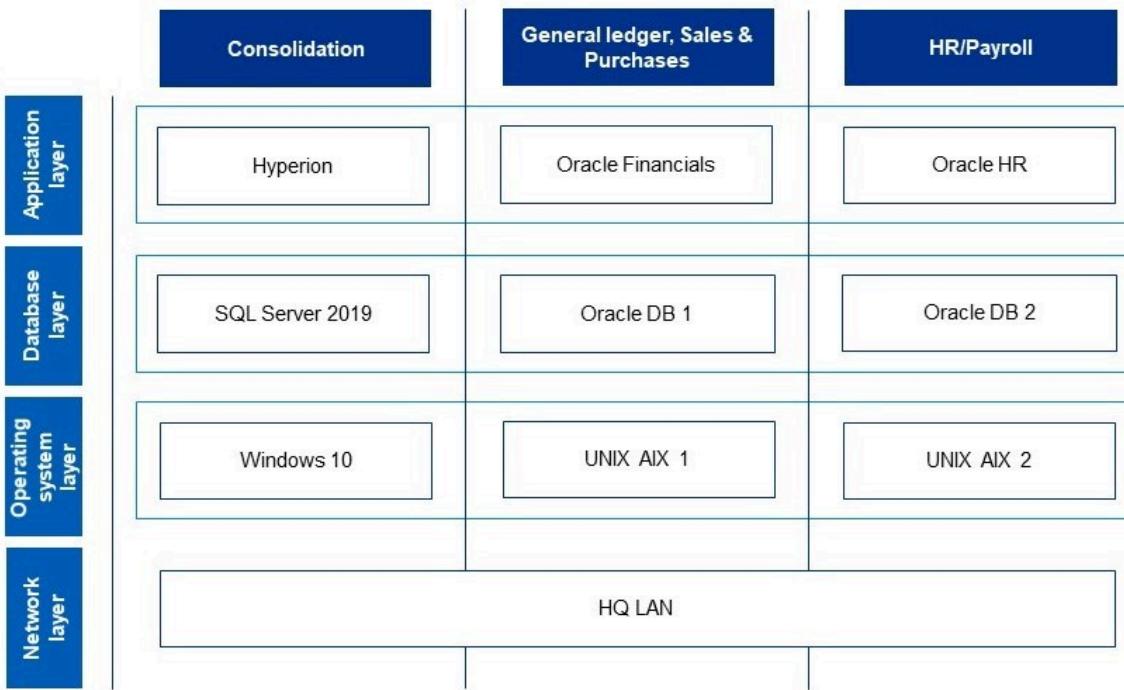
The engagement team identified three IT systems the entity uses as part of its financial reporting and business processes relevant to the preparation of the financial statements: Hyperion, Oracle Financials and Oracle HR.

The engagement team's understanding of the entity's IT systems included the following for the Hyperion system (Note: the engagement team also obtained an understanding of the Oracle Financials and Oracle HR systems, but this is not shown in this example):

Name of IT system	Hyperion
Purpose of the IT system	Used for the entity's financial reporting from components and for the entity's consolidated financial information
Processes using the IT system	Consolidation
Components using the IT system	All components
Layers of technology within the IT system	Application layer <ul style="list-style-type: none"> • Title and version: Hyperion Financial Management (HFM) • Significant upgrades: upgraded from Hyperion Enterprise to Hyperion Financial Management (HFM) in February of the

	<p>current period. This was a major upgrade, which required replacing hardware, converting data, and installing and configuring new servers.</p> <ul style="list-style-type: none"> • Extent of customization and/or changes: None • Extent of outsourcing: None • Other relevant information: None
	<p>Database layer</p> <ul style="list-style-type: none"> • Title and version: SQL Server 2019 (15.0.2000.5) • Significant upgrades: as part of upgrading Hyperion, the database was upgraded from SQL Server 2014 to SQL Server 2019 in February of the current period • Extent of customization and/or changes: None • Extent of outsourcing: None • Other relevant information: None
	<p>Operating system layer</p> <ul style="list-style-type: none"> • Title and version: Windows 10 • Significant upgrades: as part of upgrading Hyperion, the operating system was upgraded from Windows 2003 to Windows 10 in February of the current period • Extent of customization and/or changes: None • Extent of outsourcing: None • Other relevant information: None
	<p>Network layer</p> <ul style="list-style-type: none"> • Title and version: HQ LAN • Significant upgrades: N/A • Extent of customization and/or changes: None • Extent of outsourcing: None • Other relevant information: None

They also include the following ISD, capturing certain key elements of all three IT systems:



1.2 Understand the entity's IT processes [ISA | 7842]

What do we do?

Obtain an understanding of the entity's IT processes to manage access to programs and data, program changes, program acquisition and development and computer operations.

Why do we do this?

We obtain an understanding of the entity's IT processes in order to understand how the entity uses IT and how IT affects the entity's flow of transactions and the financial statements. Our understanding may help us to identify relevant risks arising from IT (RAFITS) and the general IT controls (GITCs) that address them.

Execute the audit

What does our understanding of the entity's IT processes include? [ISA | 7842.8689]

Obtaining an understanding of the entity's IT processes includes understanding the process to:

- manage access to programs and data;
- manage program changes or changes to IT systems;
- acquire or develop new IT systems; and
- manage computer operations.

The table below provides example considerations that may be applicable when obtaining an understanding of the entity's IT processes.

IT process	Example considerations
Access to programs and data	<ul style="list-style-type: none"> The process to manage access to programs and data (authentication/authorization, provisioning, de-provisioning, privileged access, user access reviews, physical access) The complexity of the process to manage access rights Whether the entity uses any tools to support the process (e.g. identity access management (IAM), workflow tools to support the approval process, password vaults to secure shared passwords, etc.)
Program changes	<ul style="list-style-type: none"> The process to manage program changes or changes to IT systems (authorization, development, testing, and approval, migration to the production environment including configuration and emergency changes) The complexity and formalization of the change process Whether the entity uses any tools to support the change management process (e.g. workflow tools, code migration tools, etc.)
Program acquisition and development	<ul style="list-style-type: none"> The process to acquire or develop new IT systems (design, development, testing, approval, implementation, and data migration) The development methodology (e.g. agile or traditional) The complexity and formalization of the acquisition and development process The nature and significance of major data conversion, if one occurred, and how the conversion was undertaken (e.g. software upgrade provided by vendor, major version upgrade, new release, platform change, etc.)
Computer operations	<ul style="list-style-type: none"> The process to manage computer operations (job scheduling, job monitoring, backup and recovery, and incident/problem management) Whether the entity uses any tools to backup data related to relevant financial systems, tools used for incident and problem management, and/or tools used to manage job scheduling activities.

Understanding the nature and complexity of IT processes in place may assist in determining which IT systems the entity is relying upon to process and maintain the integrity of information in the entity's IT environment.

What might we consider when assessing the complexity of IT processes? [ISA | 7842.8690]

The table below sets out example considerations when assessing the complexity of IT processes.

IT process	Example complexity considerations
------------	-----------------------------------

Access to programs and data	The complexity of the process to manage access rights may vary from a less complex IT process with informal policies and procedures, centralized security administration function, and/or a single individual dedicated to supporting security administration to a more complex IT process with formally documented policies and procedures, a decentralized security administration function and a larger number of individuals dedicated to supporting security administration and monitoring.
Program changes	The complexity of the program change process may vary from a less complex IT process over changes to a commercial application with little or no customization to a more complex program change process over highly customized or highly integrated applications.
Program acquisition and development	The complexity of the program acquisition and development process may vary from a less complex IT process over the acquisition of purchased commercial applications with no ability to customize to a more complex process over entity-developed applications with significant customizations and conversions of system data from legacy systems to new systems.
Computer operations	The complexity of the computer operations process may vary from a less complex IT process over informal computer operations with few scheduled jobs and no policies or procedures to a formal computer operations function with many scheduled jobs with varying frequency and formal policies and procedures.

Examples

What is included in our understanding of an entity's IT processes? [ISA | 7842.8691]

Fact pattern 1:

Consider an entity that:

- Has a moderately complex IT environment
- Uses Hyperion for consolidation and part of the period-end financial reporting process; Oracle Financials for the general ledger and sales and purchases processes; and Oracle HR for the HR/payroll process
- Uses ServiceNow to support the access to programs and data and program change processes

Analysis:

The engagement team's understanding of the entity's IT processes included the following:

IT process	Description

Access to programs and data	<p>The entity adopted a formal security policy that provides guidance for information security within the organization. The security policy includes aspects of the IT environment relevant to financial reporting applications such as password policies, procedures to request and revoke access, etc.</p> <p>Passwords are used for authentication to the entity's financial systems based on the entity's information security policy. The entity established password rules including minimum length, password change interval, complexity, use of recycled password, etc.</p> <p>The process to provision access, including privileged access, to the entity's financial systems is initiated when a user's manager submits an online access request form via ServiceNow. The user's manager completes the form to indicate the user's role/responsibilities and the system(s) and access permissions requested for the new user. The form is submitted to the IT department, where a designated IT security administrator will review the form and process the request.</p> <p>The process to de-provision access to the entity's financial systems is initiated when the HR department changes the employee status to 'terminated' in the Oracle HR system. Once the status is changed, the terminated employee's Oracle user account is automatically disabled. Changing the employee status to 'terminated' also triggers the automatic creation of a ServiceNow ticket. The ticket is assigned to the IT security administrator to confirm that access to all systems is disabled.</p> <p>On a quarterly basis, the entity performs a user access review. The IT security administrator generates system security reports showing the access permissions of users and submit the reports to the business owners for review. The business owners review the users access rights and submit requests for access changes as necessary. The IT security administrator will then process the requests.</p> <p>The entity uses electronic key cards to restrict physical access to the data center. The process to obtain physical access to the data center requires that the employee complete and submit a request form to Operations Management personnel for approval. Upon approval, a designated security administrator will grant the employee physical access to the data center.</p>
Program changes	<p>The entity has a formal change management policy. All changes, including configuration changes, require approval and testing. Prior to migration to production, changes are reviewed and approved by both business and IT managers. The entity uses an automated workflow to capture the change request and approval process.</p> <p>The process to migrate changes to production is initiated when the final approvals for testing indicate the change was successfully tested in the quality assurance (QA) environment and is ready for migration into the production</p>

	<p>(PROD) environment. Designated system administrators responsible for migrating changes, which are separate from developers, will then migrate the change from the QA environment to the PROD environment.</p> <p>Emergency changes follows a similar process, however emergency changes are flagged as high priority and the request, approval, testing are expedited.</p>
Program acquisition and development	<p>Requests for new system acquisitions or development are forwarded to Steering Committee for review and approval. Major system acquisitions require the approval of the Board of Directors.</p> <p>Once approved, the entity follows the established policies and procedures over new system acquisitions/developments including defining requirements, design, development, testing, and data conversion/migration.</p> <p>*Note: When there are significant program acquisitions or developments, additional documentation of the specific aspects of those processes would be included here.</p>
Computer operations	<p>The entity uses utility tools to support batch job scheduling, processing, and monitoring. The Computer Operations team is responsible for monitoring batch jobs and notifying relevant teams as necessary to resolve any job failures.</p> <p>The entity uses a cloud backup service to back up their business-critical data and applications on cloud servers. Data backups are restored periodically and tested for data recoverability.</p>

Fact pattern 2:

Consider an entity that:

- Has a less complex IT environment
- Uses ABC system, a single commercial accounting software application

Analysis:

The engagement team's understanding of the entity's IT processes included the following:

IT process	Description
Access to programs and data	<p>The entity has informal process and procedures in place to manage access to ABC system. The IT Manager has security administrative responsibility to administer access to the system.</p> <p>The process to provision access is initiated when HR notifies the IT Manager of a new hire. HR completes an access request form to request access based on the new hire's job responsibility. The IT Manager will then provision access as requested and email the new hire the new user ID and password. The user is required to change the password upon initial logon. The entity also</p>

	<p>has password rules in place including minimum password length, password expiration, and complexity requirements.</p> <p>The process to de-provision access is initiated when HR notifies the IT Manager of an employee termination. Upon notification of termination, the IT Manager will revoke the terminated employees' access.</p> <p>The server room that houses ABC system is secured through use of a key fob. The entity uses a physical security software to program the key fobs to unlock entry to doors based on employee need. The process to obtain access to the server room is initiated when an employee fills out a physical access request form and submits it to the IT Manager for review and approval. Upon approval, the IT Manager will program the employee's key fob to access the server room.</p>
Program changes	<p>The entity does not perform any programming/development nor does the entity have access to ABC system source code. The entity has an informal and less complex change management process in place whereby changes are limited to software patches, releases, and updates. These types of changes are generally initiated by the vendor. If the vendor has an update, they notify the entity that a new update is available. The entity is then responsible for reviewing the release notes and determining whether they want to apply the update. If the entity determines that they will apply the update, they will download the update from the vendor's website to the entity's test environment and perform end user testing. Once testing is completed and the change is approved for production, entity management with system administrative privileges will install the software update in the production environment.</p>
Program acquisition and development	<p>The entity does not develop any new IT systems. It has an informal process to acquire new systems. If the business determines a need to acquire a new system, it is discussed during the weekly Senior Management meetings. If Senior Management agrees to acquire a new system, they will coordinate with the IT Manager to perform research and identify potential vendors. Once a system is identified, they will then coordinate with the vendor to implement the new IT system.</p> <p>The vendor assisting with the implementation has a project plan in place that includes data migration. The entity validates data migrated from the legacy system to the new system.</p>
Computer operations	<p>Job scheduling, job processing, and job monitoring are not applicable given the entity's use of a single commercial accounting software. All transactions are updated in real-time.</p> <p>The entity has an informal process in place to backup data. The entity runs backup jobs to perform incremental daily and weekly backups. Full backups run</p>

monthly. The backed-up data is stored at an offsite secured location. The entity performs periodic data restorations as requested by end users.

What is included in our understanding of an entity's IT processes when we determine GITCs are ineffective and we do not test automated controls? [ISA | 7842.8907]

Fact pattern:

Consider an entity that:

- Has a less complex IT environment
- Uses System A, a single commercial accounting software application
- GITCs are not always formalized and documented
- The engagement team identified GITC deficiencies in the previous audit

The engagement team's understanding of the entity's IT processes included the following:

IT process	Description
Access to programs and data	<p>The IT Manager and the Accounting Manager (as a backup) have security administrative responsibility to administer access to the system. The prior year deficiency related to the privileged access GITC was not remediated in the current year¹.</p> <p>The process to provision access is initiated when the Accounting department identifies a new user that needs access. Generally, the Accounting Manager sends a request either verbally or via email to the IT Manager requesting a new user account. The emails are not always retained².</p> <p>The user is required to change the password upon initial logon. The entity has password rules in place for minimum password length, password expiration, and complexity requirements.</p> <p>The process to de-provision access occurs when the IT Manager is notified of an employee resignation or termination. Upon notification of termination, the IT Manager will revoke the terminated employees' access. The IT Manager indicated that he does not always retain documentation to evidence the timely removal of access².</p> <p>There is no data processing Center, as the system is maintained on the cloud.</p>
<p>Footnotes</p> <p>¹ KPMG identifies this as a deficiency</p> <p>² Since the entity has a less complex IT environment and uses a single commercial accounting software application, GITCs may not always be formalized and documented, which in this case is considered appropriate for the size and complexity of the entity and its IT environment.</p>	

Remember: When documenting our understanding of IT processes, we obtain an understanding for all four IT processes even if we identify a deficiency in one process. In this example, only one row was completed to illustrate example documentation when a deficiency is identified.

Analysis

As a result of the GITC deficiencies identified during the engagement team's understanding of the IT Processes, the engagement team concluded that they cannot rely on the related automated control(s). The engagement team decided to test manual controls related to the same assertion and risk of material misstatement.

1.3 Understand the entity's IT organization [ISA | 7591]

What do we do?

Obtain an understanding of the entity's IT organization.

Why do we do this?

We obtain an understanding of the entity's IT organization in order to understand how the entity uses IT and how IT affects the entity's flow of transactions and the financial statements.

Execute the audit

How do we obtain an understanding of the entity's IT organization? [ISA | 7591.10426]

Obtaining an understanding of the entity's IT organization includes understanding:

- key members of the IT organization, including their names, titles, and locations where they are based. We may also obtain an understanding of the number and skill level of the IT personnel;
- whether certain key functions of the IT organization have been outsourced, including the functions outsourced to external parties and service organizations; and
- the use of any centralized IT services, including shared services centers, to perform IT related processes for multiple IT systems and/or their related layers of technology.

1.4 Understand cybersecurity risks and incidents [ISA | 7592]

What do we do?

Obtain an understanding of management's cybersecurity risk assessment process when obtaining an understanding of how the entity uses IT as part of financial reporting AND consider whether cybersecurity risks or incidents lead us to identifying a risk of material misstatement (RMM) AND, if applicable, involve specific team members with expertise in IT.

Why do we do this?

The risk of a cybersecurity incident is faced by any company. Cybersecurity incidents often have negative consequences for the entity, including:

- lost revenues;
- litigation costs and potential regulatory fines;
- remediation costs related to stolen information, intellectual property, system repairs and incentives given to maintain relationships with customers or business partners;
- increased cybersecurity protection costs, e.g. insurance premiums;
- diminished investor confidence; and
- reputational or brand damage.

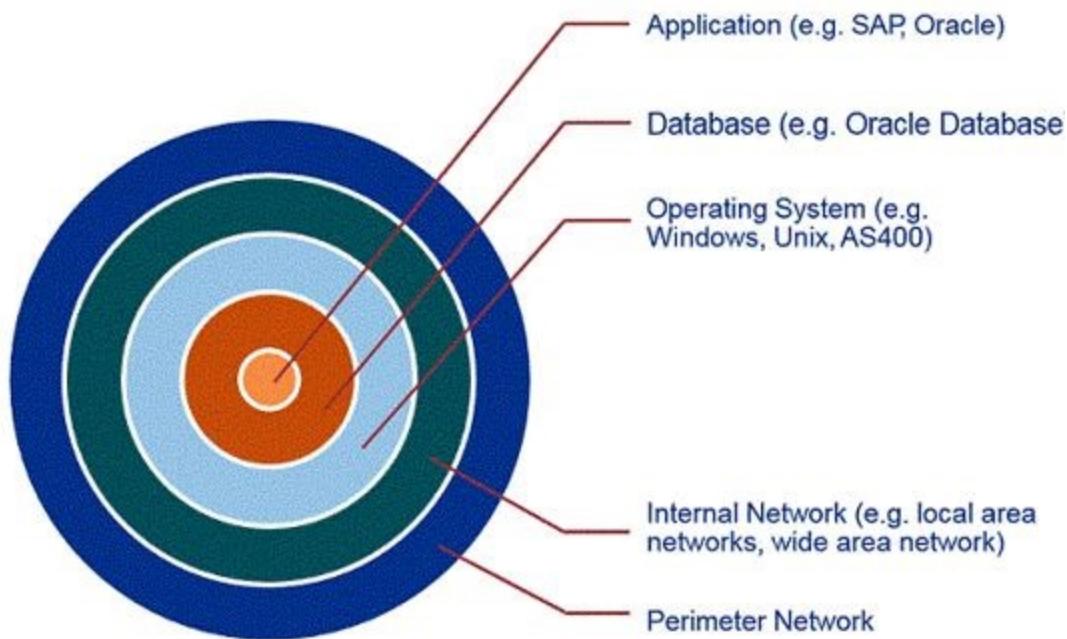
Consequently, when we obtain an understanding of how the entity uses IT and how IT affects the financial statements, we also consider cybersecurity risks and incidents because they may lead us to identifying RMMs, either at the financial statement level or at the assertion level, and may impact our audit approach.

Execute the audit

What are cybersecurity risks and incidents? [ISA | 7592.10437]

Cybersecurity risks relate to unauthorized access to IT systems. Cybersecurity incidents are intentional attacks or unintentional events whereby unauthorized users gain access to IT systems to disrupt operations, corrupt data, steal sensitive information or cause denial of service on websites.

The following diagram depicts the typical access path to an IT system.



Cybersecurity incidents usually first occur through the perimeter and internal networks. Depending on the entity's business environment, security around the internal and perimeter network may not pose risks to financial and non-financial data relevant to the audit. However, network access may or may not be relevant to the audit for entities that permit access to operating systems, databases, and applications through single sign-on protocols at the operating system layer. An example of a cybersecurity incident at the internal or perimeter network is when a computer virus sent as an email attachment or downloaded from a website infects systems on an entity's network.

Do we obtain an understanding of how management responds to cybersecurity risks for all entities? [ISA | 7592.10438]

Yes, we obtain an understanding of how management responds to cybersecurity risks and consider the occurrence of cybersecurity incident(s) for all audits, taking into consideration the nature of the entity's business, customer and vendor base, reliance on automated business processes and other relevant factors.

For example, cybersecurity risks may be more relevant to entities:

- with significant consumer focus and interaction, such as those with high volumes of credit card transactions;
- that retain large amounts of personally identifiable information (PII) (e.g. financial services, insurance, healthcare and retail organizations);
- that have significant intellectual property, such as software developers or pharmaceutical companies;
- with high volumes of transactional data, such as telecommunication providers or financial institutions; or
- with highly automated business processes which may become disrupted during a cybersecurity incident.

Are cybersecurity risks also relevant for third-party service organizations used by the entity? [ISA | 7592.10439]

Yes. When we obtain an understanding of how management responds to cybersecurity risks, we also consider risks related to third-party service organizations that are relevant to the audit.

We may consider the business environment and the nature of services provided by the third-party service organization in determining whether we perform additional procedures to address any cybersecurity risks arising from the third party.

What does obtaining an understanding of management's cybersecurity risk assessment include? [ISA | 7592.10440]

Management is responsible for evaluating the risk of cybersecurity incidents and cyber-related frauds (e.g. business email compromise (BEC) scams and other spoofing techniques) across all aspects of the entity's business operations, including financial reporting and compliance with relevant laws and regulations, and establishing processes, structures, and safeguards to mitigate those risks.

We are not responsible for evaluating cybersecurity risks across an entity's entire IT environment or providing assurances on the adequacy of safeguards and controls established to address cybersecurity risks or the entity's ability to withstand a cybersecurity incident. We are also not responsible for concluding on the appropriateness of the entity's actions in response to cybersecurity risks or to actual cybersecurity incidents. Care should be taken to avoid overstating our responsibilities and the scope of our work when discussing the results of the audit with management and audit committees.

However, we obtain an understanding of management's cybersecurity risk assessment process, which includes:

- evaluating the risks of material misstatement (RMMs) to an entity's financial statements resulting from, among other things, unauthorized access to financial reporting systems, including IT applications, databases, and operating systems.
- obtaining an understanding of a cybersecurity incident if one occurs and evaluating its effect on our audit approach. We evaluate management's assessment of the incident's effect on the amounts and disclosures in the financial statements and the entity's ICFR (see question '[What procedures may we perform if a cybersecurity incident comes to our attention during the course of the audit?](#)').

In obtaining an understanding of management's cybersecurity risk assessment, we inquire of those within the entity that are primarily responsible and knowledgeable about cybersecurity matters and risks about management's risk assessment process related to cybersecurity risks and incidents.

Inquiries we make include:

- How does the entity's risk assessment process evaluate cybersecurity risks across the entity? How does the entity analyze and assess the significance of the risks to financial reporting? How do they manage the risk across the entity?
- How has the entity assessed its internal accounting controls in light of risks arising from cyber-related frauds (e.g. BEC scams, spoofing, phishing etc.)?
- How does the entity identify, assess and respond to risks related to attacks perpetrated through BEC scams or spoofing or phishing routines?
- How would the entity be aware, on a timely basis, if its IT applications, databases, operating systems and/or network had been subject to a cybersecurity incident that could impact the integrity of information used in the financial reporting process?
- Has a cybersecurity incident occurred within the entity during the period or in prior periods that impacts the current period?

[What are BEC scams, spoofing or phishing?](#) [ISA | 7592.8655]

In a "business email compromise" (BEC), also known as "email account compromise" (EAC), scams or spoofing/phishing routines, bad actors send an email message that appears to come from a known source, making it appear as if it's a legitimate request in the course of the business, with the aim of getting otherwise confidential or proprietary information from the entity, or getting personal information to perpetuate fraud for financial gain.

[What are some of the entity's processes we may consider when understanding management's cybersecurity risk assessment?](#) [ISA | 7592.8656]

Examples of the processes being employed by the entity as part of management's cybersecurity risk assessment that we may consider are:

Process	Description
Security evaluations	<p>IT performs periodic network vulnerability assessments to:</p> <ul style="list-style-type: none"> scan, investigate, analyze, and report on any security vulnerabilities discovered on public, internet-facing devices; and

- give the entity's management appropriate mitigation strategies to address those discovered vulnerabilities.

Security software	The entity installs security software to help protect it from web-based threats - including spyware, viruses, and phishing attacks. In addition, the entity uses virtual private networks and email encryption to prevent unauthorized disclosure of information.
Personnel training	Personnel are required to complete security training upon hire, which focuses on IT security and access communications. Security policies and procedures are available throughout the year via the Employee Handbook, located on the HR portal. All employees are required to complete an annual security 'refresh' training.
Network monitoring	The entity uses various software tools across the organization to monitor network access. These include vulnerability scanners, packet sniffers, intrusion detection systems (IDS), vulnerability exploitation devices, packet crafting tools, and firewall monitoring devices.
Corporate cybersecurity incident response team (CIRT)	The entity sets up a CIRT as part of its cyber intrusion protection program (CIPP), which monitors threats and/or breaches of data on a real-time basis. In particular, the CIRT identifies, assesses, evaluates, and takes actions to mitigate data breaches or other types of unauthorized cyber intrusion. Often management would organize their cybersecurity activities in a Security Operations Center.
Cyber governance	The entity incorporates cyber governance in its corporate governance regime - e.g. to receive reports on cybersecurity activities regularly. Alternatively, on a quarterly basis, the Board of Directors is briefed on findings and concerns relating to the entity's CIPP, as well as other measures taken by management to mitigate cybersecurity risks.
Business continuity plan	The business continuity plan includes a documented and tested plan to deal with cybersecurity incidents if the organization does not have a separate cybersecurity incident response plan that is tested by the CIRT.
Service organizations	The entity has a process to consider the impact of cybersecurity risks on service organizations relied upon in connection with their internal control over financial reporting and depending on the nature of the services provided.

Verification controls	The entity has various controls that verify changes to bank account information or vendor payment information (e.g. routing numbers, vendor names, etc.) to authenticate the validity of the changes.
-----------------------	---

Under what circumstances do we involve specific team members with expertise in IT? [ISA | 7592.10441]

If a cybersecurity incident at any layer comes to our attention during the course of our audit, or if we identify cybersecurity risks that lead us to the identification of an RMM, we involve specific team members with expertise in IT to help us with our response to the incident and/or RMM, including the identification of process risk points (PRPs) and process control activities and related general IT controls when applicable.

Further guidance may be sought from the firm's cybersecurity specialists, or DPP, if deemed appropriate.

What if a cybersecurity incident and/or cybersecurity risk gives rise to an RMM? [ISA | 7592.8659]

If we determine that a cybersecurity incident and/or cybersecurity risk gives rise to an RMM, we:

- Identify the RMM,
- Revise our approach to testing relevant control activities, including relevant automated process control activities and GITCs, as a result of the identified RMM, and/or
- Determine the additional substantive procedures to be performed to address the potential financial statement implications (as a result of the cybersecurity incident and/or risk), such as contingent or known liabilities related to possible noncompliance with laws and regulations.

Under what circumstances may a cybersecurity risk give rise to an RMM? [ISA | 7592.8658]

Although it is more likely that we identify an RMM as a result of a cybersecurity incident since the incident can have a significant impact on our audit approach and on the entity's financial statements, in certain circumstances we may identify an RMM as a result of a cybersecurity risk without a cybersecurity incident having occurred. For example, if, as a result of our inquiries to management about their risk assessment process related to cybersecurity risks and incidents, it becomes clear to us that management does not have a risk assessment process or controls in place to prevent and/or detect cybersecurity incidents on a timely basis, such that there is a reasonable possibility of an undetected cybersecurity incident that would have a material effect on the financial statements, including those that may occur at a service organization relevant to the audit.

What procedures may we perform if a cybersecurity incident comes to our attention during the course of the audit? [ISA | 7592.8661]

If a cybersecurity incident, including cyber-related frauds perpetrated through BEC scams, spoofing or phishing techniques, occurs, we evaluate the impact of the incident on our audit and on the entity's financial statements. When evaluating the impact on our audit approach, we may consider taking the following actions:

- Obtain an understanding of the nature, magnitude, and duration of the cybersecurity incident, including what internal and perimeter networks or IT applications, databases, and operating systems were compromised, and any impact on the financial information.

- Determine whether any control deficiencies have been identified as a result of a cybersecurity incident and evaluate them in accordance with the activity '[Identify and evaluate control deficiencies](#)'.
- Reassess whether continued reliance on automated control activities is warranted and if so, whether to test additional process control activities or GITCs. Consider the layers of technology that may have been impacted by the cybersecurity incident and its impact to the RAFITs that are relevant to the effective operation of automated controls or the integrity of information.
- Reassess the risk of material misstatement. Consider whether additional substantive testing is necessary, e.g. over liabilities for compensation and remediation, litigation costs, and regulatory fines/penalties.
- Consider the financial accounting and reporting implications related to a cybersecurity incident. For example:
 - An entity that has experienced a cybersecurity incident may incur both direct and indirect losses that require recognition and/or disclosure in the financial statements, such as those derived from claims asserted against the entity, fines or penalties levied by governmental agencies, incentives to affected customers to maintain the business relationship, or a decline in expected future cash flows as a result of reputational and brand damage that may impact the fair value of assets.
 - Financial statement disclosures related to cybersecurity risks and incidents required by the applicable financial reporting framework or other laws and regulations.
 - Evaluate management's assessment of the incident's effect on the amounts and disclosures in the financial statements - e.g. related contingent liabilities and claims suffered as a result of the actual incident, the impact on cash flows (which may trigger impairment), and the adequacy of disclosures.

Considerations for Understanding General IT Controls

International Standards on Auditing: ISA 315.Appendix 6 Appendix 6 Considerations for Understanding General IT Controls

(Ref: Para. 25(c)(ii), A173.A174)

This appendix provides further matters that the auditor may consider in understanding general IT controls.

1. The nature of the general IT controls typically implemented for each of the aspects of the IT environment:

(a) Applications

General IT controls at the IT application layer will correlate to the nature and extent of application functionality and the access paths allowed in the technology. For example, more controls will be relevant for highly-integrated IT applications with complex security options than a legacy IT

application supporting a small number of account balances with access methods only through transactions.

(b) Database

General IT controls at the database layer typically address risks arising from the use of IT related to unauthorized updates to financial reporting information in the database through direct database access or execution of a script or program.

(c) Operating system

General IT controls at the operating system layer typically address risks arising from the use of IT related to administrative access, which can facilitate the override of other controls. This includes actions such as compromising other user's credentials, adding new, unauthorized users, loading malware or executing scripts or other unauthorized programs.

(d) Network

General IT controls at the network layer typically address risks arising from the use of IT related to network segmentation, remote access, and authentication. Network controls may be relevant when an entity has web-facing applications used in financial reporting. Network controls are also may be relevant when the entity has significant business partner relationships or third-party outsourcing, which may increase data transmissions and the need for remote access.

2. Examples of general IT controls that may exist, organized by IT process include:

(a) Process to manage access:

Authentication

Controls that ensure a user accessing the IT application or other aspect of the IT environment is using the user's own log-in credentials (i.e., the user is not using another user's credentials).

Authorization

Controls that allow users to access the information necessary for their job responsibilities and nothing further, which facilitates appropriate segregation of duties.

Provisioning

Controls to authorize new users and modifications to existing users' access privileges.

Deprovisioning

Controls to remove user access upon termination or transfer.

Privileged access

Controls over administrative or powerful users' access.

User access reviews

Controls to recertify or evaluate user access for ongoing authorization over time.

Security configuration controls

Each technology generally has key configuration settings that help restrict access to the environment.

Physical access

Controls over physical access to the data center and hardware, as such access may be used to override other controls.

(b) Process to manage program or other changes to the IT environment:

Change management process

Controls over the process to design, program, test and migrate changes to a production (i.e., end user) environment.

Segregation of duties over change migration

Controls that segregate access to make and migrate changes to a production environment.

Systems development or acquisition or implementation

Controls over initial IT application development or implementation (or in relation to other aspects of the IT environment).

Data conversion

Controls over the conversion of data during development, implementation or upgrades to the IT environment.

(c) Process to manage IT operations

Job scheduling

Controls over access to schedule and initiate jobs or programs that may affect financial reporting.

Job monitoring

Controls to monitor financial reporting jobs or programs for successful execution.

Backup and recovery

Controls to ensure backups of financial reporting data occur as planned and that such data is available and able to be accessed for timely recovery in the event of an outage or attack.

Intrusion detection

Controls to monitor for vulnerabilities and or intrusions in the IT environment.

The table below illustrates examples of general IT controls to address examples of risks arising from the use of IT, including for different IT applications based on their nature.

Process	Risks	Controls	IT Applications		
IT Process	Example Risks Arising from the Use of IT	Example General IT Controls	Non-complex commercial software - Applicable (yes / no)	Mid-size and moderately complex commercial software or IT applications	Large or complex IT applications (e.g., ERP systems) - Applicable (yes / no)

				- Applicable (yes / no)	
Manage Access	User-access privileges: Users have access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties.	Management approves the nature and extent of user-access privileges for new and modified user access, including standard application profiles/roles, critical financial reporting transactions, and segregation of duties	Yes - instead of user access reviews noted below	Yes	Yes
	Access for terminated or transferred users is removed or modified in a timely manner	Yes - instead of user access reviews below	Yes	Yes	
	User access is periodically reviewed	Yes - instead of provisioning/Deprovisioning controls above	Yes – for certain applications	Yes	

		Segregation of duties is monitored and conflicting access is either removed or mapped to mitigating controls, which are documented and tested	N/A - no system enabled segregation	Yes – for certain applications	Yes
		Privileged-level access (e.g., configuration, data and security administrators) is authorized and appropriately restricted	Yes - likely at IT application layer only	Yes – at IT application and certain layers of IT environment for platform	Yes – at all layers of IT environment for platform
Manage Access	Direct data access: Inappropriate changes are made directly to financial data through means other than application transactions.	Access to application data files or database objects/tables/data is limited to authorized personnel, based on their job responsibilities and assigned role, and such access is	N/A	Yes – for certain applications and databases	Yes

		approved by management			
Manage Access	System settings: Systems are not adequately configured or updated to restrict system access to properly authorized and appropriate users.	Access is authenticated through unique user IDs and passwords or other methods as a mechanism for validating that users are authorized to gain access to the system. Password parameters meet company or industry standards (e.g., password minimum length and complexity, expiration, account lockout)	Yes - password authentication only	Yes - mix of password and multi-factor authentication	Yes
	The key attributes of the security configuration are appropriately implemented	N/A - no technical security configurations exist	Yes – for certain applications and databases		Yes

Manage Change	<p>Application changes:</p> <p>Inappropriate changes are made to application systems or programs that contain relevant automated controls (i.e., configurable settings, automated algorithms, automated calculations, and automated data extraction) or report logic.</p>	Application changes are appropriately tested and approved before being moved into the production environment	N/A – would verify no source code installed	Yes – for non-commercial software	Yes
		Access to implement changes into the application production environment is appropriately restricted and segregated from the development environment	N/A	Yes for non-commercial software	Yes
Manage Change	Database changes:	Database changes are	N/A - no database	Yes – for non-	Yes

	Inappropriate changes are made to the database structure and relationships between the data.	appropriately tested and approved before being moved into the production environment	changes made at entity	commercial software	
Manage Change	System software changes: Inappropriate changes are made to system software (e.g., operating system, network, change-management software, access-control software).	System software changes are appropriately tested and approved before being moved to production	N/A - no system software changes are made at entity	Yes	Yes
Manage Change	Data conversion: Data converted from legacy systems or previous versions introduces data errors if the conversion transfers incomplete, redundant,	Management approves the results of the conversion of data (e.g., balancing and reconciliation activities) from the old application system or data structure	N/A - Addressed through manual controls	Yes	Yes

	obsolete, or inaccurate data.	to the new application system or data structure and monitors that the conversion is performed in accordance with established conversion policies and procedures			
IT Operations	Network: The network does not adequately prevent unauthorized users from gaining inappropriate access to information systems.	Access is authenticated through unique user IDs and passwords or other methods as a mechanism for validating that users are authorized to gain access to the system. Password parameters meet company or professional policies and standards (e.g., password minimum)	N/A - no separate network authentication method exists	Yes	Yes

	length and complexity, expiration, account lockout)			
	Network is architected to segment web-facing applications from the internal network, where ICFR relevant applications are accessed	N/A - no network segmentation employed	Yes – with judgment	Yes – with judgment
	On a periodic basis, vulnerability scans of the network perimeter are performed by the network management team, which also investigates potential vulnerabilities	N/A	Yes – with judgment	Yes – with judgment
	On a periodic basis, alerts are generated to provide	N/A	Yes – with judgment	Yes – with judgment

		notification of threats identified by the intrusion detection systems. These threats are investigated by the network management team			
		Controls are implemented to restrict Virtual Private Network (VPN) access to authorized and appropriate users	N/A - no VPN	Yes – with judgment	Yes – with judgment
IT Operations	Data backup and recovery: Financial data cannot be recovered or accessed in a timely manner when there is a loss of data.	Financial data is backed up on a regular basis according to an established schedule and frequency	N/A - relying on manual backups by finance team	Yes	Yes
IT Operations	Job scheduling: Production	Only authorized users have	N/A - no batch jobs	Yes – for certain applications	Yes

	systems, programs, or jobs result in inaccurate, incomplete, or unauthorized processing of data.	access to update the batch jobs (including interface jobs) in the job scheduling software			
	Critical systems, programs, or jobs are monitored, and processing errors are corrected to ensure successful completion.	N/A - no job monitoring	Yes – for certain applications	Yes	

How do we comply with the Standards?

[ISA | KAEGHDWC]

1 Understand how the entity has responded to RAFITs

What do we do?

Obtain an understanding of how the entity has responded to risks arising from IT.

Why do we do this?

Risks arising from IT (RAFITs) pose a risk to the continued effective operation of automated controls as well as to the integrity of data and information within IT systems. Therefore, we understand how the entity has responded to RAFITs when we identify and evaluate the design and implementation of automated controls or we take a controls approach to evaluate the reliability of data and information within IT systems.

Execute the Audit

How do we obtain an understanding of how the entity has responded to RAFITs? [ISA | 1355.1400]

We obtain an understanding of how the entity has responded to RAFITs by:

- identifying the relevant layers of technology and risks arising from IT (RAFITs); and
- identifying and evaluating the design and implementation of relevant general IT controls (GITCs).

1.1 Identify relevant layers of technology and RAFITs [ISA | 1354]

What do we do?

Identify the layers of technology and risks arising from IT that are relevant to the effective operation of automated controls or the integrity of data and information within the IT system.

Why do we do this?

Identifying the relevant layers of technology (application, database, operating system, or network) helps us identify the relevant RAFITs within those layers, which in turn helps us identify the GITCs that address those RAFITs.

Execute the Audit

What are the layers of technology that comprise an IT system? [ISA | 1354.10387]

IT systems are comprised of four types of layers of technology (also referred to as IT system layers or IT layers), which are the application, database, operating system and network layers (the last three layers may be collectively referred to as IT infrastructure). Each of these layers of technology may present risks arising from IT (RAFITs) to be controlled by management so that:

- automated controls operate and function effectively; or
- the integrity of data and information sourced from an entity's IT system is maintained.

The table below provides a description of each of the layers of technology.

Layer	Description
Application	<p>Applications are the layers of IT systems designed to perform one or many functions, tasks or activities - often to capture, process or extract data. Applications often include an interface accessed by an end-user.</p> <p>An IT application is a program or a set of programs that is used in the initiation, processing, recording and reporting of transactions or information. Examples of the application layer of an IT system include:</p> <ul style="list-style-type: none"> • ERP systems, such as SAP and Oracle; • report writers, • emerging technologies, such as robotic process automation (RPA), artificial intelligence; and • transaction-processing systems, such as a CRM or billing system.

Database	Databases are the layers of IT systems that organize a collection of data or information so that it can be easily accessed, managed and updated. This includes data warehouses, which are separate applications that we consider as a database layer. SQL Server and Oracle DB, as well as stand-alone data repositories and data warehouses, are examples of the database layer of an IT system. Technologies such as MS SQL Server may be used by an entity for multiple IT systems to access information in the database.
Operating system	Operating systems are the layers of IT systems that control the basic operation of a computer and provide a software platform on which to run other software, such as applications and databases. The operating system generally works behind the scenes and is usually not manipulated directly by the end user. UNIX, LINUX, Microsoft Windows and MacOS are examples of the operating system layer of an IT system.
Network	Networks are the layers of IT systems that transport information or data between computers, either within an organization or between organizations. Access to IT applications may be restricted to users on a particular network - e.g. users cannot access an IT application outside of a local area network (LAN) or virtual private network (VPN). Wide area networks (WANs), LANs and VPNs are examples of the network layer of an IT system.

When is a layer of technology relevant? [ISA | 1354.8678]

A layer of technology is relevant when there is one or more relevant RAFITs within that layer of technology.

What is a RAFIT? [ISA | 1354.1300]

A RAFIT represents the susceptibility of automated controls to ineffective design or operation, or risks to the integrity of information in the entity's information system, due to ineffective design or operation of general IT controls. In other words, a RAFIT represents any condition that could affect the effective operation of automated controls or the integrity of data and information within an entity's IT system.

How is a PRP different from a RAFIT? [ISA | 1354.10538]

The table below shows the main differences between PRPs and RAFITs:

	Process risk point (PRP)	Risk arising from IT (RAFIT)

Addressed by:	Process control activities	General IT controls
Identified:	When we obtain an understanding of business processes and the financial reporting process and we plan to evaluate the design and implementation of process control activities	<ul style="list-style-type: none"> - After identifying automated controls that we intend to evaluate design and implementation of (including automated process control activities that address PRPs), or - When evaluating the reliability of internal information by testing management's controls and we decide to address the data integrity risk within the IT system through testing GITCs
Defined as:	Point in the entity's process that a misstatement could, individually or in aggregate, yield a material misstatement to the financial statements. We describe the PRP as the 'where' and the 'how' in the entity's process that misstatement could be introduced	The susceptibility of automated controls to ineffective design or operation, or risks to the integrity of information in the entity's information system, due to ineffective design or operation of general IT controls. In other words, a RAFIT represents any condition that could affect the effective operation of automated controls or the integrity of data and information within an entity's IT system.

What is a relevant RAFIT? [ISA | 1354.8680]

A "relevant RAFIT" is a RAFIT where there is a "reasonable possibility" that the RAFIT could prevent the effective operation of the related automated control and/or integrity of data within the IT system. 'Reasonable possibility' means a more than remote possibility and it is therefore a low threshold.

Do we always identify a relevant RAFIT in each IT process? [ISA | 1354.8681]

No. Not all IT processes affect the effective operation of automated controls or the integrity of data and information within an IT system.

For example, program development may not affect the effective operation of automated controls or the integrity of data and information if the entity did not develop or acquire a new IT system in the current period.

Similarly, IT risks in the computer operations process related to backup and recovery may not affect the effective operation of automated controls or the integrity of data and information.

What is the complete list of RAFITs? [ISA | 1354.8682]

The complete list of RAFITs for each IT process is set out in the table below.

IT process	Risks arising from IT (RAFITS)
Access to programs and data	<p>1.1 APD - Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data.</p> <p>1.2 APD - Logical access permissions (new or modified) are granted to users and accounts (including shared or generic accounts) that are inappropriate (i.e., unauthorized or not commensurate with job responsibilities).</p> <p>1.3 APD - Logical access permissions are not revoked in a timely manner.</p> <p>1.4 APD - Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities).</p> <p>1.5 APD - Physical access to facilities housing IT systems and/or electronic media is unauthorized or not commensurate with job responsibilities.</p>
Program changes	<p>2.1 PC - Changes to IT programs were inappropriate (i.e., unapproved or do not function as intended).</p> <p>2.2 PC - Changes to IT configurations were inappropriate (i.e., unapproved or do not function as intended).</p> <p>2.3 PC - Logical access to implement changes to IT system program or configurations into the production environment is inappropriate (i.e., unauthorized or not commensurate with job responsibilities).</p>
Program acquisition and development	<p>3.1 PD - IT system developments (new components or significant changes) are unapproved or do not function as intended.</p> <p>3.2 PD - Incomplete, redundant, obsolete or inaccurate data is migrated to the production environment of acquired, newly developed or existing IT systems.</p>
Computer operations	<p>4.1 CO - System jobs, processes, and/or programs do not function as intended, resulting in incomplete, inaccurate, untimely or unauthorized processing of data.</p> <p>4.2 CO - Logical access to make changes to system jobs, processes, and/or programs is unauthorized or not commensurate with job responsibilities.</p>

	4.3 CO - Financial data backups are not able to be recovered in a timely manner.
--	--

[Can we identify a RAFIT that is not in the list of RAFITs? \[ISA | 1354.8683\]](#)

No. RAFITs are finite and we have captured a complete list of RAFITs at the appropriate level of granularity.

[Under what circumstances do we identify relevant layers of technology and RAFITs? \[ISA | 1354.1400\]](#)

We identify relevant layers of technology and RAFITs when we:

- plan to rely on and test the operating effectiveness of automated control activities,
- evaluate the design and implementation of automated control activities, even though we do not plan to test their operating effectiveness (e.g., when we evaluate the design and implementation of an automated process control activity that addresses a significant risk or over journal entries). However, when GITCs are a) informal and, therefore, unable to be evaluated for design and implementation or b) expected to be ineffective (i.e. resulting in a control deficiency), we may document our understanding of relevant layers of technology, RAFITs and GITCs in summary as part of our understanding of the IT environment rather than identifying the individual layers of technology, RAFITS and GITCs for each automated control activity, or
- decide to address the data integrity risk within the entity's IT system through testing GITCs, when testing management's controls over the accuracy and completeness of internal information to evaluate the reliability of such information.

[How may we document our understanding of relevant layers of technology, RAFITs and GITCs in summary as part of our understanding of the IT environment? \[ISA | 1354.8899\]](#)

When we evaluate the design and implementation of automated control activities but we do not plan to test their operating effectiveness, and GITCs are a) informal and, therefore, unable to be evaluated for design and implementation or b) expected to be ineffective (i.e. resulting in a control deficiency), we may document our understanding of relevant layers of technology, RAFITs and GITCs in summary as part of our understanding of the entity's IT processes within our understanding of the IT environment.

For example, consider an entity with the following circumstances:

- Has a less complex IT environment
- Uses System A, a single commercial accounting software application
- GITCs are not always formalized and documented
- We identified GITC deficiencies in the previous audit
- We have evaluated the design and implementation of an automated control that addresses a significant risk, but we do not plan to rely on the operating effectiveness of that control

Our understanding of the entity's IT processes may include the following:

IT process	Description
Access to programs and data	The IT Manager and the Accounting Manager (as a backup) have security administrative responsibility to administer access to the system. The prior year deficiency related to the privileged access GITC was not remediated in the current

	<p>year¹. RAFITs related to access to programs and data in system A are considered relevant to automated controls and they are addressed by the following steps in the process.</p> <p>The process to provision access is initiated when the Accounting department identifies a new user that needs access. Generally, the Accounting Manager sends a request either verbally or via email to the IT Manager requesting a new user account. The emails are not always retained².</p> <p>The user is required to change the password upon initial logon. The entity has password rules in place for minimum password length, password expiration, and complexity requirements.</p> <p>The process to de-provision access occurs when the IT Manager is notified of an employee resignation or termination. Upon notification of termination, the IT Manager will revoke the terminated employees' access. The IT Manager indicated that he does not always retain documentation to evidence the timely removal of access².</p> <p>There is no data processing Center, as the system is maintained on the cloud.</p>
<p>Footnotes</p> <p>¹ KPMG identifies this as a deficiency</p> <p>² Since the entity has a less complex IT environment and uses a single commercial accounting software application, GITCs may not always be formalized and documented, which in this case is considered appropriate for the size and complexity of the entity and its IT environment.</p>	

Remember: When documenting our understanding of IT processes, we obtain an understanding for all four IT processes even if we identify a deficiency in one process. In this example, only one row was completed to illustrate example documentation when a deficiency is identified.

How do we identify relevant layers of technology and RAFITs? [ISA | 1354.1500]

To identify relevant layers of technology and RAFITs, we identify:

- The layer of technology where the automated control operates or where the data and information within an IT system exists;
- The layers of technology that are relevant to the effective operation of automated controls or the integrity of data and information within an IT system; and
- the RAFITs within those layers of technology where there is a "reasonable possibility" that the RAFIT could prevent the effective operation of automated controls or the integrity of data and information within an IT system.

We identify the relevant layers of technology and RAFITs concurrently. Even though we start by thinking about what layers of technology are applicable to the automated control or integrity of data within an IT system, we cannot determine that they are relevant if we don't identify one or more relevant RAFITs. In order to assess whether a layer of technology may be relevant, we think about qualitative factors such as where the automated control operates or where the data resides (see

question "[What factors may we think about when identifying relevant layers of technology?](#)" for example factors).

In order to assess whether there is a "reasonable possibility" that the RAFIT could prevent the effective operation of the related automated control and/or integrity of data within the IT system, we think about qualitative factors such as the entity's ability to make code changes or configuration changes (see question "[What factors may we think about when determining when a RAFIT is relevant?](#)" for example factors).

[Can multiple 'layers of technology' be relevant? \[ISA | 1354.8685\]](#)

Yes. Although automated controls are programmed into a particular layer of technology within an IT system, and information we plan to rely on is obtained from the database layer, the RAFITs that are relevant to the effective operation of automated controls and the integrity of data and information can exist in multiple layers of technology that make up an IT system.

[Can an automated control have no relevant layers of technology? \[ISA | 1354.8686\]](#)

A layer of technology is relevant when there is one or more relevant RAFITs within that layer of technology. In the unlikely circumstances when we don't identify any relevant RAFITs for an automated control, we won't have any relevant layers of technology.

For example, we may not identify any relevant layers of technology when we determine it is appropriate to test the operating effectiveness of an automated process control activity throughout the period (see activity '[Test automated process control activities throughout the period, if appropriate](#)').

[What factors may we think about when identifying relevant layers of technology? \[ISA | 1354.8687\]](#)

We start by identifying the layers of technology that are likely to contain RAFITs. For each of those layers, we consider if there are any relevant RAFITs. This enables us to identify the relevant layers of technology and RAFITs.

When the application layer is relevant, the database(s) that stores the data processed by the automated control is typically also relevant. Similarly, because an IT system's ability to operate is often dependent on the operating system and IT applications and databases may be directly accessed from the operating system, the operating system is typically relevant.

The network layer may be identified when an IT system interacts with vendors or external parties through the internet. Generally, RAFITs on the network layer are related to network segmentation/remote access and are not relevant to automated controls. The network layer may be relevant when an entity has web-facing applications used in financial reporting and we identify cybersecurity risks that lead to the identification of an RMM. As part of obtaining an understanding of management's cybersecurity risk assessment, we inquire about how the entity's management evaluates and manages cybersecurity risks across the entity at the network layer. See question "[What does obtaining an understanding of management's cybersecurity risk assessment include?](#)" for more information

To determine if the layer of technology is relevant, we think about the RAFITs and layers of technology factors in parallel. The table below sets out example factors that we may think about when determining whether a layer of technology is relevant.

IT layer factors	Example considerations
------------------	------------------------

The layer in which the automated control operates	An edit check automated process control activity is coded to flag sales transactions for inclusion on an exception report based on a configured dollar threshold flag. The automated process control activity is configured at the application layer and the flag is stored within the database layer . In this scenario, the application and database layers would likely be relevant.
Where the data resides	Relevant data elements (RDEs) presented on the accounts receivable (AR) aging report are stored in the database layer. In this scenario, the database layer would likely be relevant to the integrity of the data.
Where the source code (e.g. stored procedures) is maintained	An automated control relies on stored procedures in a database , where access to deploy a change consists of modifying the stored procedure directly in the database. In this scenario, the database layer would likely be relevant.
Where and how users access the functionality subject to system access controls	For an automated access process control activity to restrict access to change the vendor master file, users can access the functionality through the application layer . In this scenario, the application layer would likely be relevant.
Where the data, subject to the functionality being restricted, can be updated and/or modified	Consider what layer(s) of technology the data subject to the functionality is stored. The vendor master data is stored in the vendor master file database . In this scenario, the database layer would likely be relevant.
Whether special user privileges in other layers of technology can access the data	Accounts at the operating system layer have special privileges to make updates to the vendor master file in a way that would impact the ongoing operation of the automated process control activity. For example, in a Unix operating system, the root account has special privileges, including the ability to make direct updates to the vendor master file, bypassing application layer security. In this scenario, the operating system layer would likely be relevant.

[What factors may we think about when determining when a RAFIT is relevant? \[ISA | 1354.8688\]](#)

The table below sets out example factors, scenarios and considerations that we may think about when determining when a RAFIT is relevant.

RAFIT factors	Example scenarios	Example considerations
<p>Whether the entity has access to make code changes</p> <p>Refer to the question "What are automated controls?" and sub-questions for more information on coded and configured automated controls.</p>	<p>An entity has access to make code changes at the operating system layer. For a coded automated control where changes are migrated from the operating system layer quality assurance environment to the production environment, the following RAFITs at the operating system layer would likely be relevant:</p> <ul style="list-style-type: none"> • 2.3 PC: Logical access to implement changes to IT system program or configurations into the production environment is inappropriate (i.e., unauthorized or not commensurate with job responsibilities). • 1.1 APD: Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data. • 1.3 APD: Logical access permissions are not revoked in a timely manner. • 1.4 APD: Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities). 	<p>When an entity has access to modify code, typically there are risks related to unauthorized privileged access, incompatible job responsibilities (i.e. segregation of duties), and authentication in relation to the layer where the code can be changed. Because generally only privileged users are able to make code changes, we focus on RAFITs related to privileged user access (1.4 APD), supported by identification and authentication mechanisms (1.1 APD) and the specific access to be able to promote such changes (2.3 PC). Risks related to end users making code changes are considered remote, so 1.2 APD is not likely a relevant RAFIT. 1.3 APD may be likely, to the extent it relates to removal of privileged accounts.</p>
<p>Whether the entity has access to make configuration changes</p>	<p>An entity has access to make configuration changes at the application layer. For a configured automated control where configuration changes are implemented directly in the application layer, the following RAFITs at the application layer would likely be relevant:</p> <ul style="list-style-type: none"> • 2.3 PC: Logical access to implement changes to IT system program or configurations into the production environment is inappropriate (i.e., unauthorized or not commensurate with job responsibilities). 	<p>This factor is relevant to situations where the entity has access to modify configurable settings for IT systems where automated controls reside. When an entity has access to modify configurable settings, similar to situations where the entity has access to modify code, there is a risk that individuals or privileged users could make configuration changes in production</p>

	<ul style="list-style-type: none"> • 1.1 APD: Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data. • 1.3 APD: Logical access permissions are not revoked in a timely manner. • 1.4 APD: Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities). 	<p>without going through the appropriate configuration change management process.</p> <p>The RAFITs related to privileged users (1.4 APD), promotion to production (2.3 PC) supported by identification and authentication mechanisms (1.1 APD) and the specific access to change configurations are likely relevant (2.3 PC). 1.3 APD may be likely relevant, to the extent it relates to removal of privileged accounts. The likelihood end users would be able to do this is considered remote, so 1.2 APD is not likely a relevant RAFIT.</p>
Process to approve and test source code changes to production	<p>Changes to a coded automated process control activity are performed in-house. The entity's change management process requires business and IT management approvals before initiating the change as well as testing of the change prior to migration to production. In this scenario, the following RAFIT at the application layer would likely be relevant:</p> <ul style="list-style-type: none"> • 2.1 PC: Changes to IT programs were inappropriate (i.e., unapproved or do not function as intended). 	<p>This factor is relevant to situations where code changes are made to IT systems where automated controls reside and the process the entity has implemented to approve and test those changes. This may include IT systems that are developed in-house, outsourced to a third party, or purchased from a vendor.</p> <p>When changes are made to IT systems, typically there are risks related to implementing unapproved program changes and program changes not functioning as intended (2.1 PC). In addition to these risks, please see the 'Whether the entity has access to make code changes' factor for additional considerations.</p> <p>Note this factor is focused on risks related to the approval</p>

		and testing of source code changes and is separate from the factor that considers the risks related to logical access to implement changes to IT system programs into the production environment (2.3 PC)
<p>Process to approve and test configuration changes to production</p> <p>This factor will also be relevant when the entity does not have direct access to source code but is responsible for evaluating updates and upgrades provided by the vendor before installing on the live environment.</p>	<p>Changes to application configurations associated with an automated control are performed at the application layer. The entity's configuration change process requires business management approvals before initiating the change as well as testing of the change prior to applying the change to production. In this scenario, the following RAFIT at the application layer would likely be relevant:</p> <ul style="list-style-type: none"> • 2.2 PC: Changes to IT configurations were inappropriate (i.e., unapproved or do not function as intended). 	<p>This factor is relevant to situations where configurations changes are made to IT systems where automated controls reside and the process the entity has implemented to approve and test those changes. This may include IT systems that are developed in-house, outsourced to a third party, or purchased from a vendor.</p> <p>When configuration changes are made to IT systems, typically there are risks related to implementing unapproved configuration changes and configuration changes not functioning as intended (2.2 PC). In addition to these risks, please see the 'Whether the entity has access to make configuration changes' factor for additional considerations.</p> <p>Note this factor is focused on risks related to the approval and testing of configuration changes and is separate from the factor that considers the risks related to logical access to implement configurations into the production environment (2.3 PC).</p>

User type	<p>An entity grants regular business end users access to the application layer functionality that allows changes to the vendor master file. In this scenario, the following RAFITs at the application layer would likely be relevant:</p> <ul style="list-style-type: none"> • 1.1 APD: Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data. • 1.2 APD: Logical access permissions are granted (new or modified) to users and accounts (including shared or generic accounts) that are inappropriate (i.e., unauthorized or not commensurate with job responsibilities). • 1.3 APD: Logical access permissions are not revoked in a timely manner. • 1.4 APD: Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities). <p>As another example, database administrators have direct access to make changes to the vendor master file. In this scenario, the following RAFITs at the database layer would likely be relevant:</p> <ul style="list-style-type: none"> • 1.1 APD: Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data. • 1.2 APD: Logical access permissions are granted (new or modified) to users and accounts (including shared or generic accounts) that are inappropriate (i.e., unauthorized or not commensurate with job responsibilities). 	<p>This factor is relevant when testing system access controls. We consider the type of user (e.g. regular business end user, system administrator, database administrator, system accounts, shared accounts, etc.) at each layer of technology, that has access to the functionality or data subject to the automated control.</p> <p>This means that risks related to inappropriate end user access (1.1 APD - 1.3 APD) as well as those related to privileged user access (1.4 APD) are likely relevant.</p> <p>We expect these RAFITs to be relevant to system access controls in all relevant layers of technology in which the access is granted.</p>
------------------	---	---

	<ul style="list-style-type: none"> • 1.3 APD: Logical access permissions are not revoked in a timely manner. • 1.4 APD: Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities). 	
How access to functions / transactions is restricted*	<p>To manage access to functions / transactions, an entity uses security groups to assign user privileges / access rights at the application layer. The following RAFITs at the application layer would likely be relevant:</p> <ul style="list-style-type: none"> • 2.2 PC: Changes to IT configurations were inappropriate (i.e., unapproved or do not function as intended). • 2.3 PC: Logical access to implement changes to IT system program or configurations into the production environment is inappropriate (i.e., unauthorized or not commensurate with job responsibilities). • 1.1 APD: Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data. • 1.2 APD: Logical access permissions are granted (new or modified) to users and accounts (including shared or generic accounts) that are inappropriate (i.e., unauthorized or not commensurate with job responsibilities). • 1.3 APD: Logical access permissions are not revoked in a timely manner. • 1.4 APD: Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., 	<p>This factor is relevant when testing system access controls. We consider how the system access control is designed to restrict access to functions (e.g. change vendor master file) and whether security groups, roles, or profiles are used.</p> <p>We also consider the risks related to changing the security groups, roles or profiles. Since security groups, roles or profiles are generally configured into the system and not hard coded, RAFITs 2.2 PC and 2.3 PC are likely relevant. Risks related to inappropriate end user access (1.1 APD - 1.3 APD) as well as those related to privileged user access (1.4 APD) are also likely relevant as it relates to this factor.</p> <p>We expect these RAFITs to be relevant to system access controls in all relevant layers of technology in which the access is granted.</p>

	unauthorized or not commensurate with job responsibilities).	
Physical access	An entity uses an open console where changes to the system can be made. In instances where physical security risks exist, the following RAFIT would likely be relevant: <ul style="list-style-type: none"> • 1.5 APD: Physical access to facilities housing IT systems and/or electronic media is unauthorized or not commensurate with job responsibilities. 	We consider the risk that unauthorised changes can be made by individuals with access to the console.
Dependency on scheduled jobs	An entity relies on an automated system calculation control that calculates depreciation. This system calculation automatically runs based on a monthly scheduled job configured in the job scheduling application. In this example, the following RAFITs at the application layer would likely be relevant: <ul style="list-style-type: none"> • 4.1 CO: System jobs, processes, and/or programs do not function as intended, resulting in incomplete, inaccurate, untimely or unauthorized processing of data. • 4.2 CO: Logical access to make changes to system jobs, processes, and/or programs is unauthorized or not commensurate with job responsibilities. • 1.1 APD: Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data. • 1.4 APD: Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities). • 2.1 PC: Changes to IT programs were inappropriate (i.e., unapproved or do not function as intended). 	We consider risks associated with inaccurate, incomplete, untimely processing of system jobs, or unauthorized changes, including batch jobs and interfaces (e.g. risk of unauthorized program execution, deviations from scheduled processing, etc.) When the effective operation of the control activity is dependent on running at a specific point in a process or at a specific time, risks related to scheduled jobs are relevant (4.1 CO). Computer operations risks can themselves be caused by inappropriate access or inappropriate changes to the job scheduler (4.2 CO), which then means that PC and APD risks can also affect the control activity. As the job scheduler is generally both coded and configured, both 2.1 PC and 2.2 PC may be relevant, depending on how the schedule is set up. 2.3 PC is likely relevant as it relates to

	<ul style="list-style-type: none"> 2.2 PC: Changes to IT configurations were inappropriate (i.e., unapproved or do not function as intended). 2.3 PC: Logical access to implement changes to IT system program or configurations into the production environment is inappropriate (i.e., unauthorized or not commensurate with job responsibilities). 	<p>the ability to implement any change in the scheduler.</p> <p>The risk of an end user being able to access or make changes to the job scheduler is generally remote, so 1.2 APD and 1.3 APD are not likely relevant. 1.4 APD supported by 1.1 APD would likely be relevant RAFITs as it relates to this example.</p>
Dependency on backup and recovery of programs and data	<p>An entity relies on an automated interface control that transmits data from System A to System B. The interface runs automatically based on a monthly scheduled job. If there were issues with the transmission of data from System A's database to System B's database such that data was partially transmitted, the automated control activity relies on the backup and recovery of data to recover the data and re-run the interface for completeness. In this scenario, the following RAFIT at the database layer would likely be relevant:</p> <ul style="list-style-type: none"> 4.3 CO: Financial data backups are not able to be recovered in a timely manner. 	<p>This criterion is specifically directed at determining if this RAFIT is relevant, so no other RAFITs are considered here.</p>
Occurrence of data migration	<p>An entity migrates data from their legacy system to a newly acquired system. The following RAFIT at the database layer would likely be relevant:</p> <ul style="list-style-type: none"> 3.2 PD: Incomplete, redundant, obsolete or inaccurate data is migrated to the production environment of acquired, newly developed or existing IT systems. 	<p>When data is migrated from one system to another during the period, this creates the risk that such data will be corrupted, lost or does not migrate over completely or accurately. Such migrations may occur when systems are upgraded, replaced or merged.</p>
<p>*Note that access refers to the ability to make changes, it does not include "read only access"</p>		

How may the complexity of the entity's IT environment impact our identification of relevant RAFITs and GITCs? [ISA | 1354.8679]

The extent of our understanding of the IT processes varies with the nature and the circumstances of the entity and its IT environment. The complexity of the IT environment may also impact the extent to which the entity has GITCs in place, as well as the number of layers of technology that include relevant RAFITs.

For example:

- An entity that uses commercial software and does not have access to the source code to make any program changes is unlikely to have a process for program changes, but may have a process or procedures to configure the software (e.g., the chart of accounts, reporting parameters or thresholds). In addition, the entity may have a process or procedures to manage access to the application (e.g., a designated individual with administrative access to the commercial software). In such circumstances, the entity is unlikely to have or need formalized GITCs.
- In contrast, a larger entity may rely on IT to a great extent and the IT environment may involve multiple layers of technology and the IT processes to manage the IT environment may be complex (e.g., a dedicated IT department exists that develops and implements program changes and manages access rights), including that the entity has implemented formalized GITCs over its IT processes.
- When management is not relying on automated process control activities or GITCs to process transactions or maintain the data, and we have not identified any automated process control activities (or any that depend on GITCs), we may plan to directly test any information used as audit evidence involving IT and may not identify any layers of technology that include relevant RAFITs.
- When management relies on a layer of technology to process or maintain data and the volume of data is significant, and management relies upon the layer of technology to perform automated controls that we have also identified, the layer of technology is likely to include relevant RAFITs.

Examples

How do we identify relevant layers of technology and RAFITs related to automated controls and the GITCs that address them? [\[ISA | 1354.1801\]](#)

Fact pattern 1

Consider an entity that:

- Has a less complex IT environment comprised of an IT manager and two system administrators.
- Uses ABC system, a single commercial accounting software application.

As part of obtaining an understanding of the financial reporting process, the engagement team identifies several PRPs related to journal entries and relevant process control activities that address those PRPs. Among those, the engagement team identifies the following PRP and relevant automated process control activity that addresses the PRP:

Process risk point (PRP)	Incorrect or inappropriate journal entries are entered if users can self approve journals they enter.
Automated process control activity	AC-1: The ABC system is coded to prevent the preparer of a journal entry from approving the same journal entry.

Additionally, in obtaining an understanding of the IT systems, IT processes, and the evaluation of the design of the automated process control activity, the engagement team noted the following:

- The automated process control activity operates at the application layer and operates by comparing the unique user IDs of both the preparer and the reviewer of the same journal entry.
- The functionality comes delivered with the ABC system.
- The entity cannot change the functionality of the ABC system.
- ABC system source code is maintained by the vendor and the entity does not have access to make changes to the source code.
- New releases of ABC system are delivered by the vendor. The entity is responsible for evaluating whether new releases meet their business needs.
- New releases are implemented on the operating system by a system administrator. Actions performed at the operating system layer would not impact how journal entries are prevented from being prepared and approved by the same individual or the ongoing effectiveness of the automated process control activity.

Analysis 1

For the relevant automated process control activity that addresses the PRP, the engagement team identifies:

- the layer of technology where the automated process control activity operates and the layers of technology that are relevant to the effective operation of the automated process control activity;
- the RAFITs within those layers of technology where there is a "reasonable possibility" that the RAFIT could prevent the effective operation of the automated process control activity; and
- the GITCs that address the relevant RAFITs;

as set out in the table below.

AC1: The ABC system is coded to prevent the preparer of a journal entry from approving the same journal entry.			
IT system	Layer of technology	RAFIT	GITC
ABC system	Application	2.1 PC - Changes to IT programs were inappropriate (i.e., unapproved or do not function as intended).	GITC-2.1PC-1 - Changes to IT system programs are approved by the business/IT prior to implementation

			into the production environment.
			GITC-2.1PC-2 - Changes to IT system programs are tested and approved in accordance with the organization's change management policy.
Layer/RAFIT analysis: RAFIT 2.1 PC is deemed relevant on the application layer since this is the layer where the automated process control activity operates. No RAFITs related to access to programs and data have been deemed relevant as the automated process control activity is based on the system coding that determines that the preparer and the approver of the same journal entry are different, regardless of the type of user permissions they have. However, the engagement team determined there is a reasonable possibility that unapproved changes and untested changes on the application layer could affect the effective operation of the automated process control activity.			

Fact pattern 2

Consider an entity that:

- Has a less complex IT environment comprised of an IT manager and two system administrators.
- Uses ABC system, a single commercial accounting software application.

As part of obtaining an understanding of the order-to-cash process, the engagement team identifies several PRPs and relevant process control activities that address those PRPs. Among those, the engagement team identifies the following PRP and relevant automated process control activity that addresses the PRP:

Process risk point (PRP)	Inaccurate data is entered into the customer master file resulting in incorrect recording of sales.
Automated process control activity	AC-2: Access to change the customer master file is restricted to authorized personnel

Additionally, in obtaining an understanding of the IT systems, IT processes, and the evaluation of the design of the automated process control activity, the engagement team noted the following:

- The automated process control activity operates at the application layer.
- The customer master file resides within an SQL server database.

- Additions and modifications to the customer master file are performed by users within the accounts receivable department by accessing the ABC system application. Users are assigned a specific permission (i.e. direct access) to allow additions and modifications.
- The system administrators have privileged access to the ABC system application and SQL server database.
- From the engagement team's understanding of the IT processes, there was no turnover in the system administrators group from the prior period

Analysis 2

For the relevant automated process control activity that addresses the PRP, the engagement team identifies:

- the layer of technology where the automated process control activity operates and the layers of technology that are relevant to the effective operation of the automated process control activity;
- the RAFITs within those layers of technology where there is a "reasonable possibility" that the RAFIT could prevent the effective operation of the automated process control activity; and
- the GITCs that address the relevant RAFITs;

as set out in the table below.

AC-2: Access to change the customer master file is restricted to authorized personnel.			
IT system	Layer of technology	RAFIT	GITC
ABC system	Application	1.1 APD - Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data.	GITC-1.1APD-1 - Access is authenticated through unique user IDs and passwords as a mechanism for validating that users are authorized to gain access to the system. Password parameters meet company or industry standards (e.g., password minimum length and complexity, expiration, account lockout).
		1.2 APD - Logical access permissions	GITC-1.2APD-1 - Management

		are granted (new or modified) to users and accounts (including shared or generic accounts) that are inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	approves the nature and extent of user access privileges for new and modified user access, including standard application profiles/roles, and critical financial reporting transactions.
		1.3 APD - Logical access permissions are not revoked in a timely manner.	GITC-1.3APD-1 - Access for terminated or transferred users is removed or modified in a timely manner.
		1.4 APD - Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	GITC-1.4APD-1 - Every quarter, the IT managers periodically review user access of privileged users to determine whether user access is appropriately restricted.
Layer/RAFIT analysis: RAFITs 1.1 APD1 - 1.4 APD on the application layer were deemed relevant since the automated process control activity operates at the application layer and based on the category of the automated control (system access).			
SQL server database	Database	1.1 APD - Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data.	GITC-1.1APD-1 - Access is authenticated through unique user IDs and passwords as a mechanism for validating that users are authorized to gain access to the

			system. Password parameters meet company or industry standards (e.g., password minimum length and complexity, expiration, account lockout).
		1.4 APD - Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	GITC-1.4APD-1 - Every quarter, the IT managers periodically review user access of privileged users to determine whether user access is appropriately restricted.
Layer/RAFIT analysis: RAFITs 1.1 APD and 1.4 APD on the database layer were deemed relevant since the customer master file data resides within an SQL server database and the system administrators have privileged access to the SQL server database. In addition to adding and modifying the customer master file through the ABC system application, an individual with system administrator privileges to the SQL server database can also add or modify the customer master file data. 1.2 APD and 1.3 APD are not relevant to the database layer because business users (i.e. those who are not system administrators) make changes to the customer master file directly through the application layer rather than the database layer.			

Fact pattern 3

Consider an entity that:

- Has a more complex IT environment comprised of a CIO, application managers, system administrators, developers, and database administrators.
- Uses Oracle as its enterprise resource planning (ERP) system. The Oracle ERP uses an Oracle database and runs on a Unix operating system.
- The entity customized the Oracle ERP to meet the needs of the business and has access to modify the source code.

As part of obtaining an understanding of the financial reporting process, the engagement team identifies several PRPs related to journal entries and relevant process control activities that address

those PRPs. Among those, the engagement team identifies the following PRP and relevant automated process control activity that addresses the PRP:

Process risk point (PRP)	Incorrect or inappropriate journal entries are entered into Oracle ERP if users can self approve journals they enter
Automated process control activity	AC-1: The Oracle ERP system is configured to prevent the preparer of a journal entry from approving the same journal entry.

Additionally, in obtaining an understanding of the IT systems, IT processes, and the evaluation of the design of the automated process control activity, the engagement team noted the following:

- The automated process control activity operates at the application layer.
- The entity can require the preparer of a journal entry to be different from the approver by changing the Journal Workflow System setting to "enable" within the application. The setting is stored within the Oracle database.
- Privileged users on the application have elevated access, including access to change the configuration.
- Users with access to the database settings can also change the configuration setting.
- The functionality of the automated process control activity comes delivered with the Oracle ERP system.
- The automated process control activity can be changed via code or configurations.
- Oracle ERP system source code is maintained by the entity and the entity has access to make changes to the source code.
- Changes to code are implemented on the operating system and the entity restricts developer access to the operating system. Developer access to the operating system layer could impact the functionality and the ongoing effectiveness of the automated process control activity.
- Business users are not granted access to operating systems or databases.
- The automated process control activity is not reliant on a job scheduling tool or other computer operations processes.

Analysis 3

For the relevant automated process control activity that addresses the PRP, the engagement team identifies:

- the layer of technology where the automated process control activity operates and the layers of technology that are relevant to the effective operation of the automated process control activity;
- the RAFITs within those layers of technology where there is a "reasonable possibility" that the RAFIT could prevent the effective operation of the automated process control activity; and
- the GITCs that address the relevant RAFITs;

as set out in the table below.

AC1: The Oracle ERP system is configured to prevent the preparer of a journal entry from approving the same journal entry.

IT system	Layer of technology	RAFIT	GITC
Oracle ERP	Application	2.1 PC - Changes to IT programs were inappropriate (i.e., unapproved or do not function as intended).	GITC-2.1PC-1 - Changes to IT system programs are approved by the business/IT prior to implementation into the production environment.
			GITC-2.1PC-3 - Changes to IT system programs are tested prior to implementation into the production environment.
		2.2 PC - Changes to IT configurations were inappropriate (i.e., unapproved or do not function as intended).	GITC-2.2PC-1 - Changes to IT system configurations are approved by the business prior to implementation into the production environment.
			GITC-2.2PC-2 - Changes to IT system configurations are tested prior to implementation into the production environment.
		2.3 PC - Logical access to implement changes to IT system program	GITC-2.3PC-1 - Access to implement changes into the production

		<p>or configurations into the production environment is inappropriate (i.e., unauthorized or not commensurate with job responsibilities).</p>	<p>environment for the Oracle application, including configuration changes, is authorized and restricted for use only by designated system administrators, and segregated from the development environment.</p>
		<p>GITC-1.3APD-2</p> <ul style="list-style-type: none"> - On a quarterly basis, management reviews access permissions assigned to users. Any access modifications identified are evaluated and corrective action is taken. 	
		<p>1.1 APD - Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data.</p>	<p>GITC-1.1APD-1</p> <ul style="list-style-type: none"> - Access is authenticated through unique user IDs and passwords as a mechanism for validating that users are authorized to gain access to the system. Password parameters meet company or industry standards (e.g., password minimum length and complexity,

			expiration, account lockout).
	1.2 APD - Logical access permissions are granted (new or modified) to users and accounts (including shared or generic accounts) that are inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	GITC-1.2APD-1 - Management approves the nature and extent of user access privileges for new and modified user access, including standard application profiles/roles, and critical financial reporting transactions.	
		GITC-1.3APD-2 - On a quarterly basis, management reviews access permissions assigned to users. Any access modifications identified are evaluated and corrective action is taken.	
	1.3 APD - Logical access permissions are not revoked in a timely manner.	GITC-1.3APD-1 - Access for terminated or transferred users is removed or modified in a timely manner.	
	1.4 APD - Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is	GITC-1.4APD-2 - Privileged-level access (e.g., configuration, data and security administrators) in the Oracle application is	

		inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	authorized and appropriately restricted for use by designated IT system administrators.
GITC-1.3APD-2 - On a quarterly basis, management reviews access permissions assigned to users. Any access modifications identified are evaluated and corrective action is taken.			

Layer/RAFIT analysis: RAFITs 2.1 PC - 2.3 PC on the application layer were deemed relevant based on the following considerations:

- The automated process control activity operates at the application layer
- The entity configures the journal entries to require a separate approver from the preparer within the application and the settings are stored within the Oracle database.
- Privileged users on the application have elevated access, including access to change the configuration.
- Oracle ERP system source code is maintained by the entity and the entity has access to make changes to the source code

RAFITs 1.1 APD to 1.4 APD on the application layer were deemed relevant based on the following considerations:

- The automated process control activity operates at the application layer
- The entity has access to enable the configuration (e.g. journal workflow) to require the preparer of a journal entry to be different from the approver by changing the system setting to "enable" within the application.
- Privileged users on the application have elevated access, including access to change the configuration.

Unix	Operating System	1.1 APD - Identification and authentication mechanisms are not implemented	GITC-1.1APD-1 - Access is authenticated through unique user IDs and passwords
------	------------------	---	---

		<p>to restrict logical access to IT systems and data.</p>	<p>as a mechanism for validating that users are authorized to gain access to the system. Password parameters meet company or industry standards (e.g., password minimum length and complexity, expiration, account lockout).</p>
		<p>1.3 APD - Logical access permissions are not revoked in a timely manner.</p>	<p>GITC-1.3APD-1 - Access for terminated or transferred users is removed or modified in a timely manner.</p>
		<p>1.4 APD - Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not commensurate with job responsibilities).</p>	<p>GITC-1.4APD-2 - Privileged-level access (e.g., configuration, data and security administrators) in the Unix operating system is authorized and appropriately restricted for use by designated IT system administrators.</p>
			<p>GITC-1.3APD-2 - On a quarterly basis, management reviews access permissions assigned to users. Any access modifications identified are</p>

			evaluated and corrective action is taken.
	2.3 PC - Logical access to implement changes to IT system program or configurations into the production environment is inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	GITC-2.3PC-1 - Access to implement changes into the production environment for the Unix operating system, including configuration changes, is authorized and restricted for use only by designated system administrators, and segregated from the development environment.	
		GITC-1.3APD-2 - On a quarterly basis, management reviews access permissions assigned to users. Any access modifications identified are evaluated and corrective action is taken.	

Layer/RAFIT analysis: RAFITs 2.3 PC, 1.1 APD, 1.3 APD, and 1.4 APD on the operating system layer were deemed relevant based on the following considerations:

- Oracle ERP system source code is maintained by the entity and the entity has access to make changes to the source code.
- Changes to code are implemented on the operating system and the entity restricts developer access to the operating system. Developer access to the operating system layer could impact how Oracle ERP prevents journal entries from being prepared and approved by the same user and the ongoing effectiveness of the automated process control activity.

		<p>RAFIT 1.2 APD at the operating system was not deemed relevant because the risk of unauthorized users and accounts (including shared or generic accounts) is not deemed a relevant risk since business users are not granted access to the operating system.</p> <p>RAFITS 2.1 PC - 2.2 PC were not deemed relevant at the operating system layer because changes to the application layer affect the way the automated process control activity operates and not the operating system layer. There is not a reasonable possibility that changes to the operating system itself would affect the automated process control activity.</p>	
Oracle database	Database	<p>1.1APD - Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data.</p>	<p>GITC-1.1APD-1</p> <ul style="list-style-type: none"> - Access is authenticated through unique user IDs and passwords as a mechanism for validating that users are authorized to gain access to the system. Password parameters meet company or industry standards (e.g., password minimum length and complexity, expiration, account lockout).
		<p>1.3 APD - Logical access permissions are not revoked in a timely manner.</p>	<p>GITC-1.3APD-1</p> <ul style="list-style-type: none"> - Access for terminated or transferred users is removed or modified in a timely manner.
		<p>1.4 APD - Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e., unauthorized or not</p>	<p>GITC-1.4APD-2</p> <ul style="list-style-type: none"> - Privileged-level access (e.g., configuration, data and security administrators) in the Oracle database is authorized and appropriately restricted for use

		commensurate with job responsibilities).	by designated IT system administrators.
GITC-1.3APD-2 - On a quarterly basis, management reviews access permissions assigned to users. Any access modifications identified are evaluated and corrective action is taken.			
<p>Layer/RAFIT analysis: RAFITs 1.1 APD, 1.3 APD, and 1.4 APD on the database layer were deemed relevant based on the following considerations:</p> <ul style="list-style-type: none"> The entity configures the journal entries to require a separate approver from the preparer within the application and the settings are stored within the Oracle database. Users with access to the database settings can also change the configuration setting. Since the settings are stored within the Oracle database, there is a risk that unauthorized access to the journal entry settings could affect the effective operation of the automated process control activity. <p>RAFIT 1.2 APD at the database was not deemed relevant because business users are not granted access to the database.</p> <p>RAFITs 2.1 PC - 2.2 PC were not deemed relevant at the database layer because there is not a reasonable possibility that changes to the database would affect the way that the automated process control activity operated.</p>			

1.2 Identify and evaluate the design and implementation of relevant GITCs [ISA | 1353]

What do we do?

Identify and evaluate the design and implementation of relevant general IT controls.

Why do we do this?

Identifying and evaluating the design and implementation of GITCs that address relevant RAFITs gives us evidence to support the:

- continued effective operation of automated controls; and/or
- integrity of data and information within the IT systems that we plan to rely on as part of our audit.

Execute the Audit

What are general IT controls? [ISA | 1353.1300]

General IT controls (GITCs) are control activities over the entity's IT processes that support the continued effective operation of the IT environment, including:

- the continued effective operation of automated controls, and
- the integrity of data and information within the entity's IT system.

The IT processes are the entity's processes to manage access to programs and data, manage program changes, manage program acquisition and development, and manage computer operations (see activity '[Understand the entity's IT processes](#)' for more information).

The IT environment encompasses the IT systems the entity uses as part of its financial reporting and business processes, including its layers of technology (application, database, operating system and network), the IT processes and the IT organization (see activity '[Understand how the entity uses IT as part of financial reporting](#)' for more information).

GITCs are not expected to directly prevent, or detect and correct, material misstatements on a timely basis, but ineffective GITCs may lead to automated controls that don't operate consistently and effectively, and therefore might not prevent, or detect and correct, a material misstatement on a timely basis.

How are GITCs different from automated process control activities? [ISA | 1353.10549]

	Automated process control activities	GITCs
Purpose	Address process risk points (PRPs).	<p>Address risks arising from IT (RAFITs).</p> <p>Support the continued effective operation of the IT environment, including:</p> <ul style="list-style-type: none"> • the continued effective operation of automated controls, and <p>the integrity of data and information within the entity's IT system.</p>
Identified	When obtaining an understanding of the business processes and we intend to evaluate the design and implementation.	<p>After identifying automated controls and relevant layers of technology and RAFITs.</p> <p>When, as part of testing management's controls over the completeness and accuracy of</p>

	internal information data integrity risks are addressed by GITCs.
--	---

When we determine whether a control activity is an automated process control activity or a GITC, it is helpful to think about whether the control activity directly mitigates a PRP and an identified risk of material misstatement (RMM).

For example, consider a process control activity related to the individuals who have access to create journal entries in an entity's IT system. This directly addresses a PRP related to the creation of fraudulent journal entries.

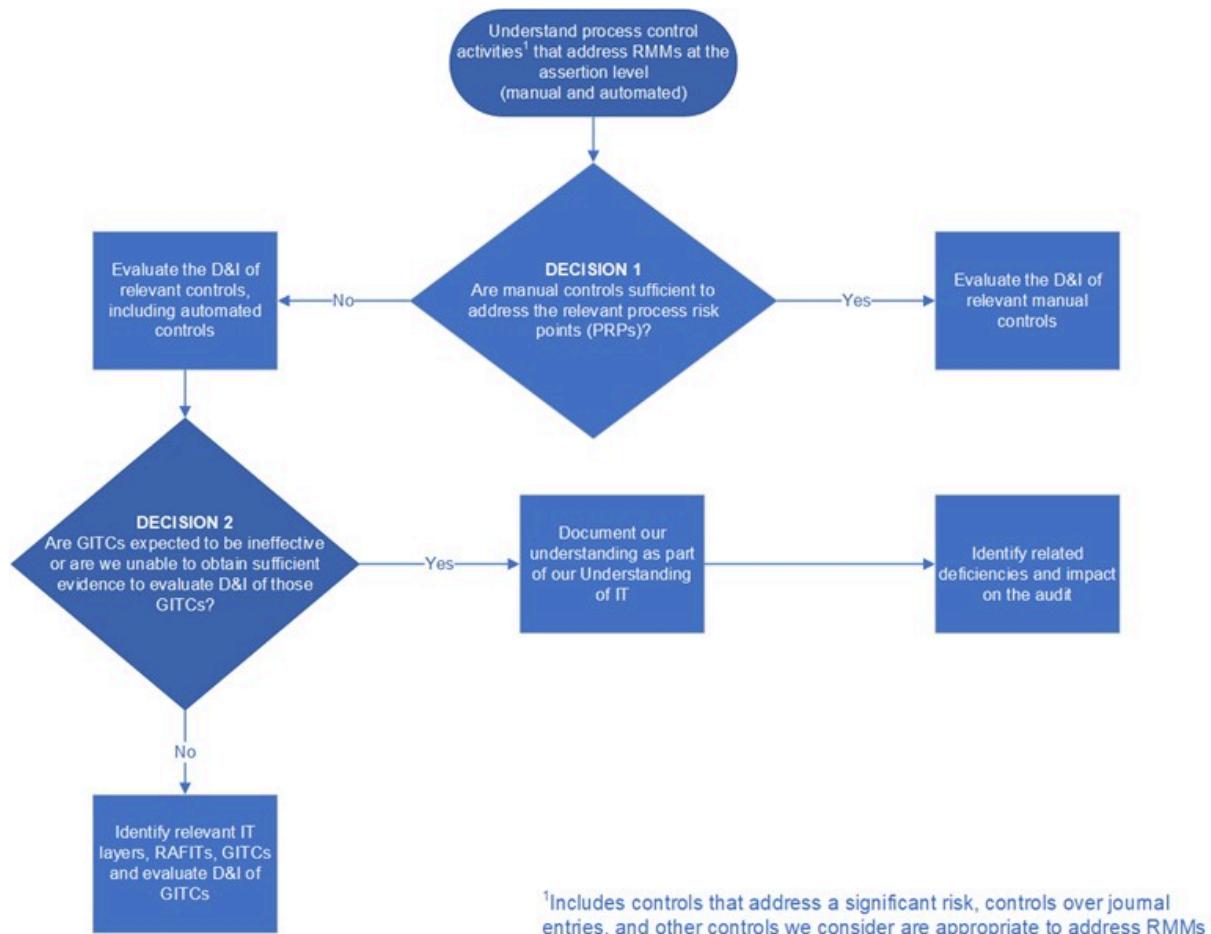
Alternatively, consider a GITC related to the creation of new users and modifications to user permissions within the IT application layer. This supports the effective operation of an automated process control activity that addresses a PRP related to the creation of fraudulent journal entries.

[Under what circumstances do we evaluate the design and implementation of GITCs?](#) [ISA | 1353.1500]

We identify and evaluate the design and implementation of GITCs where we have identified relevant layers of technology and RAFITs (see question '[Under what circumstances do we identify relevant layers of technology and RAFITs?](#)'). In our methodology we name these GITCs as 'relevant GITCs'. In practice, this means that we identify and evaluate the design and implementation of GITCs that:

- support the effective operation of automated control activities, when we:
 - plan to rely on and test the operating effectiveness of those automated control activities, or
 - evaluate the design and implementation of automated control activities, even though we do not plan to test their operating effectiveness (e.g., when we evaluate the design and implementation of an automated process control activity that addresses a significant risk or over journal entries). However, when GITCs are a) informal and, therefore, unable to be evaluated for design and implementation or b) expected to be ineffective (i.e. resulting in a control deficiency), we may document our understanding of relevant layers of technology, RAFITs and GITCs in summary as part of our understanding of the IT environment rather than identifying the individual layers of technology, RAFITS and GITCs for each automated control activity; or
- address the RAFIT(s) identified for the applicable IT system layer (e.g., database) related to data integrity risk, when we are testing management's controls over the accuracy and completeness of internal information to evaluate the reliability of such information (see question '[Are there specific risks that we consider when testing management's controls over internal information?](#)' for more information on audit considerations regarding data integrity risks).

The following decision tree provides an illustration of the decisions to be made and the implications with regards to evaluating the design and implementation of GITCs in the scenario where we evaluate the design and implementation of control activities but we do not plan to test their operating effectiveness:



How may we document our understanding of relevant layers of technology, RAFITs and GITCs in summary as part of our understanding of the IT environment? [ISA | 1353.8899]

When we evaluate the design and implementation of automated control activities but we do not plan to test their operating effectiveness, and GITCs are a) informal and, therefore, unable to be evaluated for design and implementation or b) expected to be ineffective (i.e. resulting in a control deficiency), we may document our understanding of relevant layers of technology, RAFITs and GITCs in summary as part of our understanding of the entity's IT processes within our understanding of the IT environment.

For example, consider an entity with the following circumstances:

- Has a less complex IT environment
- Uses System A, a single commercial accounting software application
- GITCs are not always formalized and documented
- We identified GITC deficiencies in the previous audit
- We have evaluated the design and implementation of an automated control that addresses a significant risk, but we do not plan to rely on the operating effectiveness of that control

Our understanding of the entity's IT processes may include the following:

IT process	Description

Access to programs and data	<p>The IT Manager and the Accounting Manager (as a backup) have security administrative responsibility to administer access to the system. The prior year deficiency related to the privileged access GITC was not remediated in the current year¹. RAFITs related to access to programs and data in system A are considered relevant to automated controls and they are addressed by the following steps in the process.</p> <p>The process to provision access is initiated when the Accounting department identifies a new user that needs access. Generally, the Accounting Manager sends a request either verbally or via email to the IT Manager requesting a new user account. The emails are not always retained².</p> <p>The user is required to change the password upon initial logon. The entity has password rules in place for minimum password length, password expiration, and complexity requirements.</p> <p>The process to de-provision access occurs when the IT Manager is notified of an employee resignation or termination. Upon notification of termination, the IT Manager will revoke the terminated employees' access. The IT Manager indicated that he does not always retain documentation to evidence the timely removal of access².</p> <p>There is no data processing center, as the system is maintained on the cloud.</p>
<p>Footnotes</p> <p>¹ KPMG identifies this as a deficiency</p> <p>² Since the entity has a less complex IT environment and uses a single commercial accounting software application, GITCs may not always be formalized and documented, which in this case is considered appropriate for the size and complexity of the entity and its IT environment.</p>	

Remember: When documenting our understanding of IT processes, we obtain an understanding for all four IT processes even if we identify a deficiency in one process. In this example, only one row was completed to illustrate example documentation when a deficiency is identified.

How do we evaluate the design and implementation of GITCs? [ISA | 1353.1505]

We evaluate the design and implementation of GITCs through inquiry in combination with observation and/or inspection.

Determining whether a GITC has been designed effectively means determining if the GITC satisfies the company's control objectives by addressing the RAFIT(s) it is intended to address.

Determining whether a GITC has been implemented means determining whether the GITC exists and whether the entity is using it.

What do we consider when we evaluate the design and implementation of a GITC? [ISA | 1353.8662]

We evaluate the design and implementation of a GITC considering the same items as when we evaluate the design and implementation of a process control activity, except for:

- anti-fraud control, and
- level of precision.

Given the different characteristics of GITCs and how they function, those characteristics aren't relevant to our evaluation. Remember that a GITC's objective is different from a process control activity's objective, specifically:

- The objective of GITCs is to address RAFITs, whereas
- The objective of process control activities is to mitigate PRPs to prevent, or detect and correct, material misstatements in the entity's financial statements.

[How do we determine whether the design of a GITC achieves its objectives?](#) [ISA | 1353.1600]

A GITC achieves its control objective when it adequately addresses each RAFIT it is designed to address.

To evaluate whether a GITC addresses each RAFIT it is intended to address, we understand how the GITC is performed, which means identifying control attributes. Control attributes are the specific procedures performed by the control operator (an individual or person for manual controls or IT systems for automated controls) that make-up the GITC and that are relevant to the design of the control.

Another way of thinking about control attributes is that they are the specific elements that are necessary for the GITC to be designed, implemented, and operating effectively. For example, if determining whether access to IT systems has been approved by an appropriate individual based on a pre-determined list is a necessary part of how a RAFIT is addressed, then that's a control attribute. If providing access within a certain number of days has no bearing on whether a RAFIT is addressed, then that is not a control attribute. The table below shows example control attributes for an example GITC.

RAFIT	GITC Description	Example Control Attributes - How the GITC is performed
1.2 APD - Logical access permissions (new or modified) are granted to users and accounts (including shared or generic accounts) that are inappropriate (i.e., unauthorized or not commensurate with job responsibilities).	Management approves the nature and extent of user access permissions for new and modified user access in ABC system.	Control operator determines requests for new ABC system access or modification to existing ABC system access, are approved by an authorized user commensurate with the entity's IT delegation of authority.
		Control operator compares the permissions requested in the form/ticket to the entity's approved security profiles or roles by job function.
		Control operator determines that the access provisioned is consistent with access requested and approved.

Can there be common GITCs across multiple layers of technology? [ISA | 1353.8663]

Yes, an entity may use common IT processes across its IT environment or across certain layers of technology, in which case common RAFITs and common GITCs may be identified.

Are there additional considerations when GITCs exist across multiple layers of technology? [ISA | 1353.8664]

Yes, when manual GITCs exist across multiple layers of technology, we consider the shared characteristics to determine whether the GITCs are designed and implemented to operate consistently.

When manual GITCs are designed and implemented to operate consistently across multiple layers of technology, we may test the operating effectiveness of those GITCs to address the relevant RAFITs by using the common approach.

What shared characteristics indicate a GITC operates consistently across multiple layers of technology? [ISA | 1353.8665]

When manual GITCs exist across multiple IT systems and/or layers of technology, we consider the following characteristics to determine that the GITCs are designed and implemented to operate consistently:

Characteristics	Description
Same policies, practices, and procedures	Standard policies, practices, and procedures are followed by the control operators when performing the GITCs and any tools used in the performance of the control are the same
Same type of information used in the performance of the control	Information used by the control operators in the performance of the control is same type of information (e.g., the relevant data elements are the same and the information is generated in the same manner).
Subject to same monitoring activities	Monitoring activities are performed consistently across to monitor internal controls. Refer to activity ' Understand and evaluate monitoring activities ' for guidance.

What is the common approach to testing the operating effectiveness of manual GITCs? [ISA | 1353.8666]

The common approach is summarized below.

Guidance	Common approach
Applicability	Applies to manual GITCs that are designed to operate consistently across multiple layers of technology. Refer to the question 'What shared characteristics indicate a GITC operates consistently across multiple layers of technology?' for guidance.

Population	Single population across all relevant layers of technology. The completeness of the population is important in supporting GITC conclusions; therefore we do not exclude relevant IT systems and/or layers of technology nor do we include non-relevant layers of technology.
Sample size	Follow the guidance in activity ' Determine the control sample size ' .
Deficiencies	Any deviations in GITCs are considered control deficiencies. The deficiencies apply to all layers of technology in the population. It is not appropriate to isolate deficiencies to a single layer of technology when reaching a conclusion.
Conclusions	GITC conclusions apply to all relevant layers of technology included in the population.

Automated GITCs may also be designed to operate consistently across multiple layers of technology; however the testing approach is the same for all automated GITCs whether they operate over one or more layers.

How does an ineffective GITC affect our audit? [ISA | 1353.1700]

If we determine that a GITC is ineffective in its design and/or implementation (see activity '[Determine whether a deficiency in ICFR exists and describe it](#)' for more information), we:

- conclude that there is a deficiency;
- do not plan to rely on or test the operating effectiveness of that GITC.; and
- consider the effect of that deficiency on the automated controls it supports or the integrity of data used in the audit (for example, if the deficient GITC supports a process control activity, it may affect our planned audit response to an identified RMM and our assessment of CAR related to an identified RMM).

See activity '[In response to GITC deficiencies, test other GITCs, perform procedures or conclude on related automated control\(s\) and/or reliability of data within the IT system](#)' for more information on how to respond to GITC deficiencies.

Although GITC deficiencies, on their own, do not directly cause financial statement misstatements, deficient GITCs may render an automated control ineffective or the data within an IT system not reliable, and this may lead to financial statement misstatements that could be material. The significance of a GITC deficiency relates to its impact on the effectiveness of automated controls and/or integrity of data within an IT system.

Examples

How do we support our conclusion that a GITC operates consistently across multiple layers of technology? [ISA | 1353.8674]

Fact pattern

The entity has 3 relevant IT systems. Based on the engagement team's understanding of the relevant business processes, automated process control activities were identified as relevant in each of the three relevant IT systems. The following GITC was identified to address relevant RAFTs in each of the IT systems:

PC2-1: Changes to IT system programs are tested and approved prior to implementation into the production environment.

Additional information:

- The layers of technology relevant to the automated process control activities include the application and database layers.
- Following are the relevant IT systems:
 - System 1: SAP application; SQL server database
 - System 2: Oracle application; Oracle database
 - System 3: Hyperion Financial Management (HFM); SQL server database
- Based on the engagement team's understanding of IT:
 - The IT department is comprised of application development groups that support each of the IT systems - one group supports SAP; one group supports Oracle and one group supports HFM. There is one group that supports all databases.
 - The IT department follows the same program change policies, practices and procedures for all applications
 - The IT department uses the same change management ticketing tool, ServiceNow, to initiate change requests, evidence testing, track changes, and obtain approvals.
 - The control owners indicate the GITC is designed and implemented to operate consistently across all three IT systems and layers of technology.

Analysis

To evaluate the design of the GITC, the engagement team:

- Inquired of the control owners for SAP, Oracle, HFM, and databases to confirm they all follow the same change management process.
- Inspected the change management policies and procedures to determine the requirements for testing system program changes and the required approvals to indicate that testing was successful and applies to ALL relevant layers of technology
- Inspected the change management ticketing tool, ServiceNow configuration (e.g., drop-down list) that shows that all relevant layers of technology are listed.

[How do we determine the population using the common approach?](#) [ISA | 1353.8675]

Fact pattern

An entity has 10 IT systems but only 3 IT systems (systems A, B, and C) are relevant to the audit. Based on the engagement team's understanding of the relevant business processes, 3 automated process control activities were identified as relevant:

- One implemented in system A with the following RAFT: PC1 in SAP and PC 1 in SQL (SAP)
- One implemented in system B with the following RAFT: PC1 in Oracle financials and PC1 in Oracle DB

- One implemented in system C with the following RAFIT: PC1 in Hyperion and PC1 in SQL(Hyperion)

These six layers are therefore all relevant.

The engagement team identifies one GITC to address all six relevant program changes RAFITs.

Based on inquiry and inspection, it was noted that the GITC is designed and implemented to operate consistently across all the entity's relevant layers.

Management provides a listing of 3,750 changes; however, 750 changes are for layers that do not relate to any of the six layers.

The RAWTC for all three automated process control activities was assessed as base and the RAWTC for the GITC was assessed as base.

Analysis

The relevant population of program changes is 3,000. The 750 changes for systems that are not relevant to the audit are excluded from the population from which samples are selected to test the program change control.

The engagement team selects a sample of 25 operations from the population haphazardly. Provided the selection is random or haphazard, the selection does not have to include controls operations for each of the six layers although in this example it is likely to.

Understanding the Components of the Entity's System of Internal Control

International Standards on Auditing: ISA 315.KPMG

ISA Application and Other Explanatory Material: ISA 315.A48-A49 | ISA 315.A90-A95

Obtaining an Understanding of the Entity and Its Environment, the Applicable Financial Reporting Framework and the Entity's System of Internal Control (Ref: Para. 19-27)

Appendices 1 through 6 set out further considerations relating to obtaining an understanding of the entity and its environment, the applicable financial reporting framework and the entity's system of internal control.

Obtaining the Required Understanding (Ref: Para. 19-27)

A48. Obtaining an understanding of the entity and its environment, the applicable financial reporting framework and the entity's system of internal control is a dynamic and iterative process of gathering, updating and analyzing information and continues throughout the audit. Therefore, the auditor's expectations may change as new information is obtained.

A49. The auditor's understanding of the entity and its environment and the applicable financial reporting framework may also assist the auditor in developing initial expectations about the classes of transactions, account balances and disclosures that may be significant classes of transactions, account balances and disclosures. These expected significant classes of transactions, account balances and disclosures form the basis for the scope of the auditor's understanding of the entity's information system.

Obtaining an Understanding of the Entity's System of Internal Control (Ref: Para. 21.27)

Appendix 3 further describes the nature of the entity's system of internal control and inherent limitations of internal control, respectively. Appendix 3 also provides further explanation of the components of a system of internal control for the purposes of the ISAs.

A90. The auditor's understanding of the entity's system of internal control is obtained through risk assessment procedures performed to understand and evaluate each of the components of the system of internal control as set out in paragraphs 21 to 27.

A91. The components of the entity's system of internal control for the purpose of this ISA may not necessarily reflect how an entity designs, implements and maintains its system of internal control, or how it may classify any particular component. Entities may use different terminology or frameworks to describe the various aspects of the system of internal control. For the purpose of an audit, auditors may also use different terminology or frameworks provided all the components described in this ISA are addressed.

Scalability

A92. The way in which the entity's system of internal control is designed, implemented and maintained varies with an entity's size and complexity. For example, less complex entities may use less structured or simpler controls (i.e., policies and procedures) to achieve their objectives.

Considerations Specific to Public Sector Entities

A93. Auditors of public sector entities often have additional responsibilities with respect to internal control, for example, to report on compliance with an established code of practice or reporting on spending against budget. Auditors of public sector entities may also have responsibilities to report on compliance with law, regulation or other authority. As a result, their considerations about the system of internal control may be broader and more detailed.

Information Technology in the Components of the Entity's System of Internal Control

Appendix 5 provides further guidance on understanding the entity's use of IT in the components of the system of internal control.

A94. The overall objective and scope of an audit does not differ whether an entity operates in a mainly manual environment, a completely automated environment, or an environment involving some combination of manual and automated elements (i.e., manual and automated controls and other resources used in the entity's system of internal control).

Understanding the Nature of the Components of the Entity's System of Internal Control

A95. In evaluating the effectiveness of the design of controls and whether they have been implemented (see paragraphs A175 to A181) the auditor's understanding of each of the components of the entity's system of internal control provides a preliminary understanding of how the entity identifies business risks and how it responds to them. It may also influence the auditor's identification and assessment of the risks of material misstatement in different ways (see paragraph A86). This assists the auditor in designing and performing further audit procedures, including any plans to test the operating effectiveness of controls.

For example:

- The auditor's understanding of the entity's control environment, the entity's risk assessment process, and the entity's process to monitor controls components are more likely to affect the identification and assessment of risks of material misstatement at the financial statement level.
- The auditor's understanding of the entity's information system and communication, and the entity's control activities component, are more likely to affect the identification and assessment of risks of material misstatement at the assertion level.

What additional activities do we perform?

[ISA | KAEGWAAP]

1 Obtain an understanding of ICFR [ISA | 1307]

What do we do?

Obtain a sufficient understanding of each component of ICFR to (a) identify the types of potential misstatements, (b) assess the factors that affect the risks of material misstatement, and (c) design further audit procedures.

Why do we do this?

Obtaining an understanding of the entity's internal control over financial reporting (ICFR) is our most complex risk assessment procedure. It combines with our other risk assessment procedures to help us:

- identify and assess risks of material misstatement (RMMs); and
- design audit procedures to respond to RMMs.

Execute the Audit

[How do we obtain an understanding of ICFR?](#) [ISA | 1307.1300]

We obtain an understanding of ICFR by:

- [obtaining an understanding of the CERAMIC components of ICFR \(control environment, risk assessment, information and communication, and monitoring\)](#)
- obtaining an understanding of control activities that are relevant to the audit, which includes obtaining an understanding of business or financial reporting processes, identifying process risk points (PRPs), and evaluating the design and implementation of control activities that are relevant to the audit.

[What is internal control over financial reporting?](#) [ISA | 1307.1400]

Internal control is the process designed, implemented, and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations.

Internal control over financial reporting includes all controls that may have an impact on financial reporting. Although most controls relevant to the audit are likely to relate to reliability of financial reporting objective, controls relating to operations and compliance objectives may also be relevant to an audit if they relate to data the auditor evaluates or uses in applying audit procedures.

The components of ICFR are:

- Control Environment;
- Risk Assessment;
- Information and Communication;
- Control Activities; and
- Monitoring.

[What is effective internal control?](#) [ISA | 1307.11189]

Effective internal control exists when:

- each of the five components of ICFR are 'present' and 'functioning'; and
- the five components of ICFR operate together in an integrated manner.

'Present' means that the components exist in the design and implementation of ICFR.

'Functioning' means that the components continue to exist as the ICFR operates.

The five components of ICFR are interrelated; they work together and support each other to achieve the overall objective of the internal control system, which is to provide an entity with reasonable assurance about achieving its financial reporting objectives.

[What are controls?](#) [ISA | 1307.8465]

Controls are policies or procedures that are a part of internal control over financial reporting. In this context:

- Policies are statements of what should, or should not, be done within the entity to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions.
- Procedures are actions to implement policies.

There are three types of controls: CERAMIC controls, process control activities or GITCs. Process control activities and general IT controls are collectively referred to as control activities.

Overarching term	Control		
Types of controls	CERAMIC controls	Control activities	
		Process control activities	General IT controls
Address	Principles/Elements	PRPs	RAFITS
Nature	Manual or Automated		

[What are the five components of ICFR?](#) [ISA | 1307.1900]

A 'component' is one of the five elements of internal control set out in the auditing standards. The table below describes each of these components.

Component	Description
<u>Control Environment</u>	The control environment includes the governance and management functions and the attitudes, awareness, and actions of those charged with governance and management concerning the entity's system of internal control and its importance in the entity. It sets the tone of the entity, influencing the control consciousness of its people, and provides the overall foundation for the operation of other components of the entity's system of internal control.
<u>Risk Assessment</u>	Risk assessment is a dynamic, iterative process for: <ul style="list-style-type: none"> identifying and analyzing risks to achieving the entity's objectives; and determining the risks to manage and how to manage them. Management consider possible changes in the external environment and within their own business model that may impede the entity's ability to achieve its objectives.
<u>Information and Communication</u>	The entity needs information to carry out internal control responsibilities that support achieving its objectives. Information systems, including the related business processes, relevant to the entity's financial reporting, support informed decision making and the functioning of the internal control.

	Communication — both internal and external — delivers the information needed to carry out day-to-day controls. Communication also helps staff understand their internal control responsibilities and how they help achieve the entity's objectives.
<u>Control Activities</u>	<p>Control activities are actions set by policies and procedures. They help ensure that management directives to mitigate risks to achieving objectives are followed.</p> <p>Control activities are performed:</p> <ul style="list-style-type: none"> (1) at all levels of the entity; (2) at various stages within business processes; and (3) over the technology environment.
<u>Monitoring Activities</u>	<p>Monitoring activities help ascertain whether each of the five components of internal control, including controls within each component, is present and functioning, and to take necessary remedial actions on a timely basis.</p> <p>These evaluations may be ongoing, separate, or a combination of both. Findings are evaluated. Deficiencies are communicated in a timely manner, with serious matters reported to senior management and those charged with governance.</p>

CERAMIC is the acronym used to describe the Control Environment, Risk Assessment, Monitoring, and Information and Communication components of ICFR. Under the auditing standards, the procedures we perform to obtain an understanding of CERAMIC components differ from those we perform for the Control Activities component. We therefore distinguish the CERAMIC components from the Control Activities component.

How are the five components of ICFR interrelated? [ISA | 1307.2000]

The five components interrelate in many ways. Their order in the auditing standards is logical:

- management establishes a control environment to provide a basis for carrying out internal control across the entity and to set an appropriate tone at the top regarding the importance of internal control and expected standards of conduct. Establishment of an appropriate control environment helps ensure that the entity has the right personnel with the right attitudes to identify, analyse and respond to risks to achieving the entity's objectives.;
- management's ability to understand the risks facing the entity helps them understand the entity's information and communication needs;
- management understanding of *how* information flows and is communicated allows them to identify control activities; and
- monitoring activities interact with all other components so management can determine whether the components' controls continue to work as planned.

Another way to look at the components is think of them like the parts of a house. Each component plays a different but important role in an entity's ICFR. If one component is ineffective, the implications to an entity's ICFR can be significant - like a house without walls or a foundation.



We will use this analogy as we walkthrough the components of ICFR individually and consider:

- (1) how they are integrated; and
- (2) how deficiencies in each component may affect our audit.

[What are the elements of the CERAMIC components?](#) [ISA | 1307.2101]

An element of a CERAMIC component helps us obtain an understanding of the component of ICFR.

CERAMIC Component	CERAMIC Elements
Control Environment	<ul style="list-style-type: none"> • Element 1: The organization demonstrates a commitment to integrity and ethical values. • Element 2: When those charged with governance are separate from management, those charged with governance demonstrates independence from management and exercises oversight of the development and performance of internal control. • Element 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. • Element 4: The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. • Element 5: The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
Risk Assessment	<ul style="list-style-type: none"> • Element 6: The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

	<ul style="list-style-type: none"> • <u>Element 7</u>: The organization identifies risks to the achievement of its objectives and analyzes risks as a basis for determining how the risks should be managed. • <u>Element 8</u>: The organization considers the potential for fraud in assessing risks to the achievement of objectives. • <u>Element 9</u>: The organization identifies and assesses changes that could significantly impact the system of internal control.
<u>Information and Communication</u>	<ul style="list-style-type: none"> • <u>Element 10</u>: The organization communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control between people within the entity, including how financial reporting roles and responsibilities are communicated. • <u>Element 11</u>: The organization communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control between management and those charged with governance. • <u>Element 12</u>: The organization communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control to external parties, such as regulatory bodies.
<u>Monitoring of Controls</u>	<ul style="list-style-type: none"> • <u>Element 13</u>: The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. • <u>Element 14</u>: The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

What are points of focus? [ISA | 1307.2201]

'Points of focus' are examples of characteristics of an element of a CERAMIC component that can help us evaluate whether the entity has addressed the objectives of the related element of a CERAMIC component.

How do the size and complexity of the entity affect how it achieves its control objectives? [ISA | 1307.2400]

The entity's size and complexity affects how it designs, implements, and maintains ICFR and within each entity, ICFR varies by process and by specific business risk. The size and complexity of an entity is typically correlated - i.e., the larger the entity, the more complex its operations and/or financial reporting. A smaller entity may use less structured means and simpler activities, policies,

procedures and processes (which may include management's actions and behaviors) to achieve similar objectives.

But that's not always the case. While the size of the entity may be an indicator of its complexity, some smaller entities may be complex and some larger entities may be less complex. A smaller entity may have highly complex financial reporting and related business processes due to complexities in delivering its services to its customers and recording those activities. By comparison, a large entity could have relatively simple processes.

The underlying objectives of the five components of ICFR are important to the achievement of an entity's objectives with regard to reliability of financial reporting; however, these components may not be so clearly distinguished in a less complex entity as compared to a more complex entity.

For example, smaller, less complex entities that have fewer employees which may limit the extent to which segregation of duties is practicable. However, an owner-manager may be more directly involved in the oversight of financial reporting and this oversight may compensate for the more limited opportunities for segregation of duties.

The nature, timing and extent of our risk assessment procedures to obtain an understanding of ICFR depend on:

- the nature, size and complexity of the entity and its business processes;
- our existing knowledge of the entity's ICFR;
- the nature of the entity's controls, including use of IT;
- the nature and extent of changes in its systems and operations; and
- the entity's documentation of ICFR.

[What are the inherent limitations of ICFR?](#) [ISA | 1307.2500]

No matter how effective ICFR is, it can provide an entity with only reasonable assurance about achieving its financial reporting objectives. The likelihood of achieving those objectives is affected by the inherent limitations of internal control.

Examples of inherent limitations of internal control include the following.

- Human judgment in making decisions can be faulty, and human error can cause breakdowns in ICFR.
- Colluding employees or management override of ICFR can circumvent controls.
- Conditions may change, and ICFR may not have been changed in response.

1.1 Obtain an understanding of the CERAMIC components

[ISA | 1309]

What do we do?

Obtain an understanding of the CERAMIC components.

Why do we do this?

Because the CERAMIC components are foundational to the entity's system of internal control, any deficiencies in their operation could have pervasive effects on the preparation of the financial statements. Our understanding and evaluation of the CERAMIC components affect our identification and assessment of risks of material misstatement at the financial statement level and may also affect the identification and assessment of risks of material misstatement at the assertion level.

Execute the Audit

What are CERAMIC components? [ISA | 1309.1300]

CERAMIC is the acronym used to describe the Control Environment, Risk Assessment, Monitoring, and Information and Communication components of ICFR.

Component	Description
<u>Control Environment</u>	The control environment includes the governance and management functions and the attitudes, awareness, and actions of those charged with governance and management concerning the entity's system of internal control and its importance in the entity. It sets the tone of the entity, influencing the control consciousness of its people, and provides the overall foundation for the operation of other components of the entity's system of internal control.
<u>Risk Assessment</u>	<p>Risk Assessment is a dynamic, iterative process for:</p> <ul style="list-style-type: none"> identifying and analyzing risks to achieving the entity's objectives; and forming the basis for how management or those charged with governance determine the risks to be managed. <p>Management or those charged with governance consider possible changes in the external environment and within their own business model that may impede the entity's ability to achieve its objectives.</p>
<u>Information and Communication</u>	<p>The entity needs Information to carry out internal control responsibilities that support achieving its objectives. Information systems, including the related business processes, relevant to the entity's financial reporting, support informed decision making and the functioning of the internal control.</p> <p>Communication — both internal and external — delivers the information needed to carry out day-to-day controls. Communication also helps staff understand their internal control responsibilities and how they help achieve the entity's objectives.</p>
<u>Monitoring Activities</u>	Monitoring Activities help ascertain whether each of the five components of internal control, including controls within each

	<p>component, is present and functioning, and to take necessary remedial actions on a timely basis.</p> <p>These evaluations may be ongoing, separate or a combination of both. Findings are evaluated. Deficiencies are communicated in a timely manner, with serious matters reported to senior management and those charged with governance.</p>
--	---

How are the five components of ICFR interrelated? [ISA | 1309.2000]

The five components interrelate in many ways. Their order in the auditing standards is logical:

- management establishes a control environment to provide a basis for carrying out internal control across the entity and to set an appropriate tone at the top regarding the importance of internal control and expected standards of conduct. Establishment of an appropriate control environment helps ensure that the entity has the right personnel with the right attitudes to identify, analyse and respond to risks to achieving the entity's objectives.;
- management's ability to understand the risks facing the entity helps them understand the entity's information and communication needs;
- management understanding of *how* information flows and is communicated allows them to identify control activities; and
- monitoring activities interact with all other components so management can determine whether the components' controls continue to work as planned.

Another way to look at the components is think of them like the parts of a house. Each component plays a different but important role in an entity's ICFR. If one component is ineffective, the implications to an entity's ICFR can be significant - like a house without walls or a foundation.



We will use this analogy as we walkthrough the components of ICFR individually and consider:

- (1) how they are integrated; and
- (2) how deficiencies in each component may affect our audit.

Do we obtain an understanding of CERAMIC components in all audits? [ISA | 1309.1800]

Yes. We obtain an understanding of CERAMIC components in all audits, regardless of whether we are relying on control activities in our audit.

Not Integrated Audit | How do we obtain an understanding of CERAMIC components? [ISA | 1309.1900]

We obtain an understanding of each CERAMIC component by:

- understanding, through inquiry, each of the elements/principles within that component ([control environment](#), [risk assessment process](#), [information and communications](#), [monitoring activities](#));
- [performing procedures to obtain an understanding of the CERAMIC components](#);
- begin by performing inquiries to obtain an understanding of each element/principle within the component.
- consider whether certain factors apply to determine whether to perform more than inquiry
- If at least one of the factors apply, design additional procedures to obtain an understanding (i.e. observation and/or inspection)

Based upon our understanding obtained, we perform an evaluation of each component ([control environment](#), [risk assessment process](#), [information and communications](#), [monitoring activities](#)) by:

- Determining whether any of the element/principles are not appropriate considering the nature and complexity of the entity
- Identifying a control deficiency when they are not appropriate and [evaluating the severity of the control deficiency and assess the impact on our audit](#)
- evaluate whether the component is appropriate to the entity's circumstances, considering the nature and complexity of the entity based upon any deficiencies identified.

When we conclude that a component is not appropriate considering the nature and complexity of the entity, we identify a financial statement level risk (see activity '[Evaluate RMs at the financial statement level](#)' for additional information) and respond to the risk in line with activity '[Design and implement overall responses](#)'.

When do we obtain an understanding of CERAMIC components? [ISA | 1309.11846]

We conduct risk assessment procedures to obtain an understanding of CERAMIC components early in the audit during the risk assessment phase.

Does the way an entity addresses the CERAMIC components differ based on its size and complexity? [ISA | 1309.11844]

Yes, the entity's size and complexity may affect how it addresses the CERAMIC components.

The size and complexity of an entity is typically correlated - i.e., the larger the entity, the more complex its operations and/or financial reporting. A smaller entity may use less structured means and simpler activities, policies, procedures and processes (which may include management's actions and behaviors) to address the CERAMIC components. In contrast, we may expect a larger entity to have more structured and robust activities, policies, procedures, and processes.

While the size of the entity may be an indicator of its complexity, some smaller entities may be complex and some larger entities may be less complex. We think about both the size and complexity when evaluating whether the CERAMIC component is appropriate for the nature and complexity of the entity.

The following are examples of factors that may impact how the CERAMIC components are addressed for a smaller entity.

Factor	Smaller Entity
Ownership and governance structure	<p>In a less complex entity, an owner-manager may be responsible for the governance and direct oversight of the operations and accounting / financial reporting for the entity.</p> <p>Consequently, the attitudes, awareness, and actions of the owner-manager are key considerations when obtaining an understanding of the CERAMIC components for less complex entities (particularly the Control Environment).</p>
Size of the Organization	<p>Less complex entities often have fewer employees.</p> <p>As a result, the organizational structure, reporting lines, and responsibilities may be clear and evident but not formally documented. In addition, communication between management and the employees may be informal, yet effective considering the circumstances.</p>
Nature of assets, liabilities and transactions	<p>Less complex entities may process more routine transactions and the accounts may not require complex accounting or significant judgments. As such, less complex processes may be necessary to support internal controls.</p>
Nature of the accounting processes and controls and IT systems	<p>Less complex entities may have less sophisticated IT systems and simple record-keeping with few accounting processes with primarily manual control activities performed by a few people. As such, extensive documentation of these processes may not be necessary.</p>
Operating characteristics	<p>A less complex entity may be a single legal entity with operations in only a few geographic locations. As such, monitoring of controls may be accomplished by management's close</p>

involvement in the business and accounting / financial reporting.

For further considerations on how smaller entities may address the CERAMIC components, refer to the following: [Control Environment](#), [Risk Assessment](#), [Information and Communication](#), and [Monitoring of Controls](#).

Copyright

This document includes extracts from materials owned and published by the International Federation of Accountants (IFAC) in 2023, and is used with permission of IFAC.

International Standards on Auditing and their respective logos are trademarks or registered trademarks of the International Federation of Accountants (IFAC).

