Internal control over financial reporting

Handbook

November 2025

kpmg.com/us/en/frv

Contents

ICFR: always in the spotlight, always work to be done

When designed appropriately and operated effectively, internal control over financial reporting (ICFR) provides many benefits: promoting accountability, safeguarding an entity's assets from fraud or significant loss, maintaining integrity of financial data and transactions, facilitating compliance with the applicable financial reporting and statutory compliance frameworks, and enabling information flows across the entity. Simply put, ICFR forms the bedrock of public and investor confidence in the capital markets. Without effective ICFR, entities risk significant financial and reputational harm.

Although the Sarbanes-Oxley Act of 2002 (SOX) is more than 20 years old, ICFR remains in the spotlight as an essential part of an entity's financial reporting agenda. One reason for this is that continuous change is now the normal state for many entities.

Change creates risks and an effective system of ICFR is needed to manage those risks. Entities continue to implement increasingly complex systems to support financial reporting and operating performance. Flaws in these systems – in design or operation – can create significant financial risks. So, too, can the march towards increased automation, use of artificial intelligence (AI), and involvement of specialized service providers in business and financial reporting processes.

External factors also contribute to entities facing new and evolving risks – the recent pandemic, international conflicts and uncertain economic environment, all fuel the need for entities to regularly adapt their business and financial reporting processes to manage the related risks.

So, there is always work to be done, even if you have been certifying ICFR for years. If you are a first-time assessor of ICFR under SOX, the work is just beginning.

In this Handbook, we discuss and illustrate the key elements of a risk-based approach to the design, implementation and evaluation of ICFR using the predominant framework employed in practice – the 2013 Internal Control – Integrated Framework published by the Committee of Sponsoring Organizations of the Treadway Commission (the COSO Framework).

We hope you find our analysis and insights useful as you start or continue your ICFR journey and rise to the challenges of an environment where change is constant.

KPMG LLP
Department of Professional Practice

Acknowledgments

This Handbook has been produced by the Department of Professional Practice (DPP) of KPMG LLP in the United States.

We would like to acknowledge the efforts of the main contributors to this edition:

Michal Dusza

Melissa Perez

Adrienne Seapker

We would also like to acknowledge the current and former members of DPP and other KPMG professionals who contributed significantly to this Handbook: David Barnes II, Jennifer Klebold, Kevin Macfee, Bob Nardone, Regine Ross, Chris Schwartz, Christy Toole and Wendy Wang.

About this publication

Management cannot satisfy its financial reporting responsibilities without strong and effective ICFR. The purpose of this Handbook is to assist management in understanding a risk-based approach to ICFR using the predominant framework employed in practice – the COSO Framework.

Organization of the text

This Handbook is organized around the risk-based approach to ICFR in the COSO Framework. Given their pervasive nature, the Handbook starts with **entity-level controls**. It then moves on to **risk assessment** and **process understanding**, both of which are integral to identifying, designing and implementing the necessary **process control activities**. From there, the Handbook moves on to **information used in controls**, **general IT controls (GITCs)** and **service organizations**, all of which touch on various aspects of an entity's ICFR. The Handbook wraps up with **identifying and evaluating deficiencies**, which may come to light at any point in the process. It also introduces considerations related to an entity's use of AI and automation in the financial reporting process.

While this Handbook discusses and illustrates the various aspects of a risk-based approach to ICFR in a sequential manner, designing, implementing, and maintaining an effective system of ICFR really is an iterative process. As management moves through the process, it will inevitably need to revisit earlier aspects of the process and reassess previous conclusions.

November 2025 edition

See Appendix F for a discussion of 'What's new' in the Handbook as compared with its previous version released in July 2023.

COSO Framework

This Handbook makes regular references to the COSO Framework. As discussed further in section 2.2, there are five components of ICFR under the COSO Framework and 17 principles underlying those components. Important characteristics of each principle are highlighted in points of focus. While the points of focus are included in a compendium that accompanies COSO's Internal Control – Integrated Framework, references to the COSO Framework in this Handbook are inclusive of that compendium as well as the separate COSO publication with illustrative tools.

Practical tips

Seeing the COSO Framework applied in practice brings an incredible amount of insight to bear on what the concepts really mean. In addition, as your external auditor also may be required to opine on the effectiveness of your entity's ICFR, insights into working effectively with your auditor in applying this risk-based approach are critically important. These insights are highlighted throughout this Handbook as 'practical tips'.

Terminology

The following terminology is used in this Handbook:

- **controls** include entity-level controls and control activities;
- **entity-level controls** are policies, procedures and structures that operate at the entity level with an indirect relationship to financial reporting;
- **control activities** include process control activities and GITCs;
- **process control activities** mitigate a specific risk point within a business process that could lead to a material misstatement of the entity's financial statements; and
- **GITCs** support the continued effective operation of automated process control activities and the integrity of data and information within the entity's IT systems by addressing risks arising from IT.

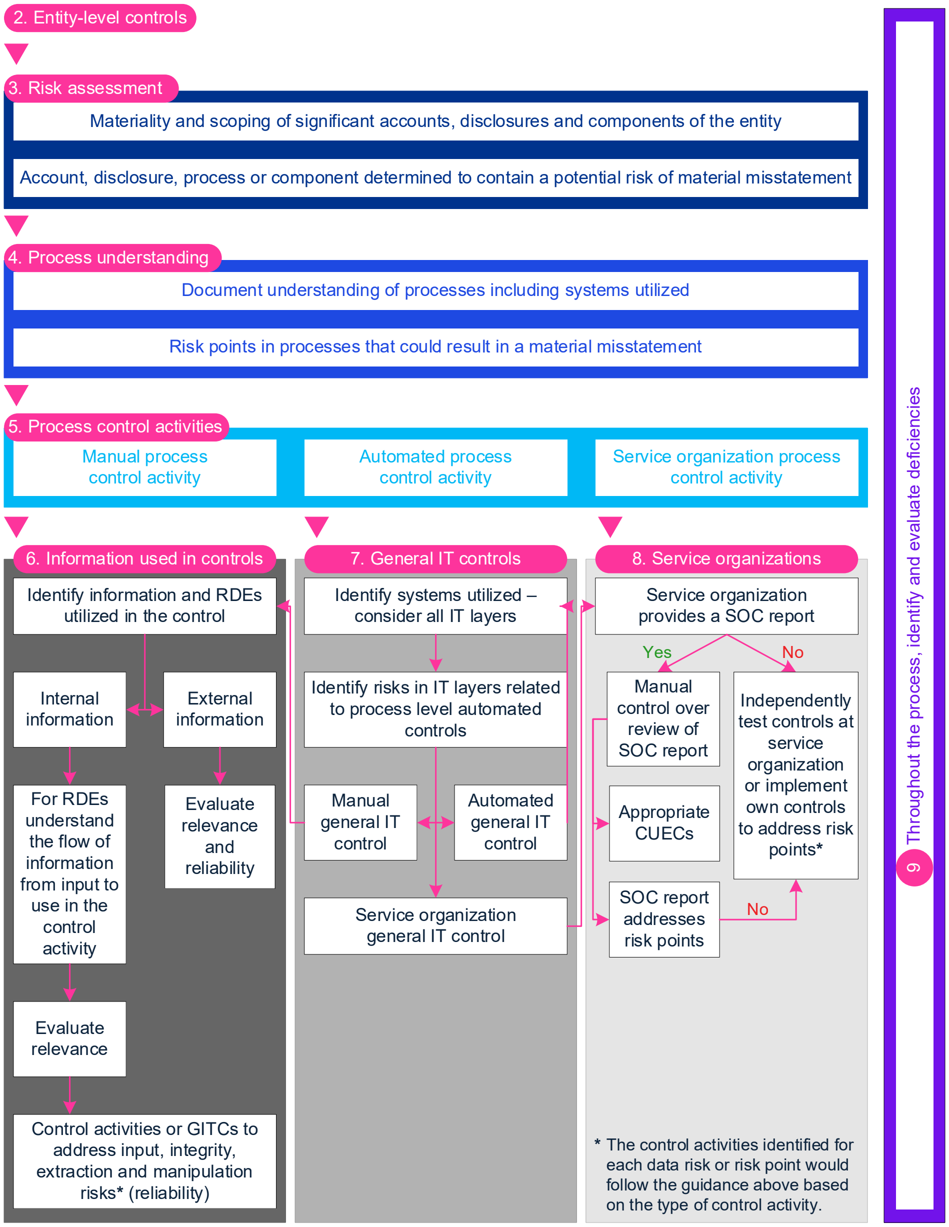
Abbreviations

We use the following abbreviations in this Handbook:

AI	Artificial intelligence
AICPA	American Institute of Certified Public Accountants
ACL	Allowance for Credit Losses
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CUEC	Complementary user entity control
FASB	Financial Accounting Standards Board
GAAP	Generally Accepted Accounting Principles
GITC	General IT control
ICFR	Internal control over financial reporting
ISD	IT System Diagram
PCAOB	Public Company Accounting Oversight Board
PRP	Process risk point
RAFIT	Risk arising from IT
RDE	Relevant data element
RM	Risk of misstatement
RMM	Risk of material misstatement
SEC	Securities and Exchange Commission
SOC	System and Organization Controls

1. Executive summary

This Handbook is focused on management's ICFR journey and describes a risk-based approach to designing, implementing and maintaining an effective system of internal control and its evaluation. Following a risk-based approach allows management to identify and address the areas of highest risk. Management's ICFR journey has many steps along the way. Each step is captured in a separate chapter of this Handbook, and the following diagram summarizes those steps and the related chapter numbers and titles.


2. Entity-level controls
3. Risk assessment
Materiality and scoping of significant accounts, disclosures and components of the entity
Account, disclosure, process or component determined to contain a potential risk of material misstatement
4. Process understanding
Document understanding of processes including systems utilized
Risk points in processes that could result in a material misstatement
5. Process control activities
Manual process control activity
Automated process control activity
Service organization process control activity
6. Information used in controls
Identify information and RDEs utilized in the control
Internal information
External information
For RDEs understand the flow of information from input to use in the control activity
Evaluate relevance and reliability
Evaluate relevance
Control activities or GITCs to address input, integrity, extraction and manipulation risks* (reliability)
7. General IT controls
Identify systems utilized – consider all IT layers
Identify risks in IT layers related to process level automated controls
Manual general IT control
Automated general IT control
Service organization general IT control
8. Service organizations
Service organization provides a SOC report
Yes
No
Manual control over review of SOC report
Independently test controls at service organization or implement own controls to address risk points*
Appropriate CUECs
SOC report addresses risk points
No
9 Throughout the process, identify and evaluate deficiencies

* The control activities identified for each data risk or risk point would follow the guidance above based on the type of control activity.

While a risk-based approach to designing, implementing, maintaining and evaluating ICFR can be described in a sequential manner, if properly performed, it is really an iterative process. Each successive step of the process is a building block on a journey to effective ICFR and, in the case of an assessment of ICFR, it adds to the total body of evidence considered. This cumulative body of evidence may cause management and auditors to reassess initial conclusions as new evidence is obtained throughout the assessment.

COSO Framework

Management and, if applicable, external auditors may be required to determine whether the entity maintained, in all material respects, effective ICFR as of a specified date, based on the criteria established by a suitable framework, which is typically the Internal Control – Integrated Framework published by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.

There are five interrelated components of internal control established in the COSO Framework that must be present and functioning, and the five components must operate together in an integrated manner, for an effective system of internal controls.

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

The COSO Framework includes 17 principles that underpin each of the five components of ICFR as fundamental concepts. The 17 principles form the basis for designing an effective integrated system of ICFR.

Each of the five components and 17 principles is covered in more detail throughout this Handbook.

Read more: Section 2.2 and Appendix A.

Entity-level controls

In this Handbook, management's ICFR journey starts with entity-level controls, which represent a broad range of policies, procedures and controls that operate at the entity level instead of the process level. They often have an indirect relationship to financial reporting because they are designed to operate through a top-down approach.

Entity-level controls are prevalent in the following components of ICFR.

Control environment	Risk assessment
The control environment includes: • the set of standards, processes and structures that provide the basis for carrying out ICFR; and	Risk assessment is a dynamic, iterative process for: • identifying and analyzing risks to achieving the entity's objectives;

Control environment

- the attitudes, awareness and actions of those charged with governance and management concerning the entity's ICFR and its importance.

The control environment also:

- sets the tone at the top of the entity;
- influences the control consciousness of its people; and
- provides the overall foundation for the operation of other components of the entity's ICFR.

Risk assessment

- identifying the risks to manage; and
- determining how to manage the risks identified.

As part of risk assessment, management considers possible changes that may impede the entity's ability to achieve its objectives. These changes can be present in the external environment and/or within the entity's own business.

Information and communication

The information and communication component addresses:

- the importance of information management and continuous communication between and among those responsible for ICFR, both internal and external; and
- how reliable information from both internal and external sources is needed to support the functioning of the other four components of internal control.

Monitoring activities

Monitoring activities are required to:

- determine whether controls are designed and operating to evidence that the five components of internal control, and each related principle, are present and functioning;
- determine that the established controls functioned in a manner to effectively address the current risks to the entity's financial reporting process; and
- identify deficiencies in internal control and communicate those deficiencies to the parties responsible for taking corrective action, including those charged with governance, as relevant.

Read more: Chapter 2 and Appendix A

Risk assessment

Management's ICFR journey for each financial reporting cycle requires the performance of risk assessment – a dynamic process for identifying and assessing risks to the achievement of objectives.

While an entity's risk assessment process starts early in the financial reporting cycle, it is an iterative, cumulative process that requires a reassessment of initial conclusions based on evidence obtained throughout the financial reporting cycle.

Identifying the relevant risks to financial reporting is an essential component of ICFR because failure to understand the likely sources of misstatements may lead to ineffectively designed control activities, which, in turn, increases the possibility of a material misstatement in the financial statements.

Management performs the entity's risk assessment at various levels within the entity by following a top-down approach that starts at the entity level and moves down to the process level.

The following are specific activities involved in executing an effective risk assessment.

- **Consideration of materiality.** Materiality involves both quantitative and qualitative considerations, and separate materiality analyses could be needed at the consolidated level and component level.
- **Scoping of accounts and disclosures.** Management identifies significant accounts and disclosures and links them to the appropriate financial statement assertions (e.g. completeness, existence, accuracy). This is necessary given management's overall objective to produce reliable financial reporting in accordance with the relevant financial reporting framework. Risks of misstatement to significant accounts and disclosures require an ICFR response.
- **Scoping of components.** Management determines which of the entity's components (e.g. subsidiaries, divisions, operating units) present a risk that the financial statements contain a material misstatement. A necessary part of this exercise is determining component materiality.
- **Identifying and assessing fraud risks.** Management must assess the potential for fraud in evaluating risks to the achievement of its objectives. This assessment should be comprehensive, cover various levels within the entity and involve appropriate members of management and employees.
- **Consideration of changes that could impact ICFR.** Management's risk assessment must identify changes that could significantly impact the entity's financial reporting and the system of internal control, assess the risks resulting from those changes and respond to those risks.

Documentation of risk assessment often involves the creation and maintenance of a risk and control matrix, which includes the account or disclosure, account balance, the risk factors considered, and the significance of the risk to the accounts, disclosures and relevant assertions, as well as linking the risks to the controls designed to address them.

Read more: Chapter 3

Process understanding

Obtaining an understanding of business processes and the financial reporting process provides the basis for management to identify and assess risks of material misstatement (RMMs) and process risk points (PRPs). An inadequate understanding of a business process and the related RMMs and PRPs often can lead to inappropriate design and selection of controls (i.e. deficiencies or gaps in the entity's ICFR).

Identifying and documenting RMMs and PRPs

The PRP is the 'where' and the 'how' in the business process a misstatement (including a misstatement due to fraud) could be introduced. The RMM is the 'what' that could be misstated. Those PRPs that could result in a material misstatement, individually or in combination with other misstatements, require an ICFR response.

PRPs that could result in RMMs should be documented in sufficient detail to identify the specific condition that would allow for a material misstatement to occur within the financial statements.

Obtaining and documenting process understanding

There are many ways management may obtain an understanding of its business processes, but, generally, performing a walkthrough is the most comprehensive method of doing so. In a walkthrough, a single transaction is followed from initiation through the entity's processes, including its information systems, until the transaction is reflected in the entity's financial records.

The documentation of process understanding should be of sufficient detail to provide understanding of the flow of information through the entity's processes and relevant IT systems and identify the relevant RMMs and PRPs associated with a particular process.

Additional considerations

Management also considers each of the following in its process understanding.

- **Financial reporting and disclosures.** Understand the period-end financial reporting process and identify the related PRPs, including those related to the development of financial statement disclosures.
- **Estimates.** Management should identify where there are estimates or changes in estimates in their business processes. Once identified, management determines whether there are RMMs and related PRPs associated with the selection or application of the methods, assumptions or data elements of the estimate.
- **IT.** Understanding the flow of transactions into, through and out of the relevant IT systems and identifying the related PRPs is an integral part of process understanding.
- **Journal entries.** Management obtains an understanding of business processes all the way through the recording of journal entries and uses this understanding to identify the RMMs and PRPs related to journal entries.

Read more: Chapter 4

Process control activities

The crux of management's ICFR journey is control activities. In the context of management's ICFR, control activities are focused on identifying the policies and procedures established to mitigate (either directly or indirectly) RMMs in the entity’s business processes and financial reporting process. Control activities include process control activities and GITCs (which are addressed more in Chapter 7). Each process control activity's objective is to mitigate an identified PRP.

An entity’s ICFR is effective when it provides reasonable assurance that its financial statements are reliable and prepared in accordance with the applicable financial reporting framework. Accordingly, process control activities should be designed and operated at a ‘would’ level of assurance – they ‘would’ (i.e. probably will) mitigate an identified PRP and, therefore, prevent, or detect and correct, on a timely basis, a material misstatement in the financial statements.

The following are considerations in designing a process control activity.

- Control objective
- Nature and type of control
- Frequency
- Judgment involved
- Level of precision
- Investigation and resolution process
- Authority and competence of the control operator
- Information used in the performance of the process control activity

Given their nature, additional considerations may apply to the design and operation of process control activities related to fraud risks, journal entries, going concern, significant unusual transactions and related parties.

Management must monitor its process control activities and obtain evidence necessary to support their assessment of ICFR. Management has several different ways they may obtain this evidence, including through direct testing of controls. Direct testing involves reperformance, inspection and/or observation of the control together with inquiry. If it is determined through management’s direct testing that a process control activity is ineffective in its design and/or operation, a deficiency exists.

Read more: Chapter 5

Information used in controls

Appropriately identifying and assessing the relevance and reliability of information used in controls is critically important to management’s ICFR journey. Management and others with ICFR responsibilities (such as control operators and IT personnel) first identify the population of information associated with a control and whether the information is external or internal, then identify the data elements in the information that are relevant to the design and operation of the control.

Once information used in controls is identified and the source is determined, management assesses the information’s relevance and reliability.

Management's evaluation of the reliability of external information considers the information's nature and source. Management's evaluation of the reliability of internal information or external information stored in the entity's IT systems involves understanding the flow of information and how the data risks associated with the information's completeness and accuracy are addressed.

Throughout the process of identifying information used in controls and assessing its relevance and reliability, management considers whether it has identified **all** such information and clearly documented its assessment of the information's relevance and reliability. If information used in a control is not clearly identified and/or its relevance and reliability are not properly addressed, the control using the information is deficient.

Read more: Chapter 6

General IT controls

GITCs are control activities over the entity's IT processes that support the continued effective operation of the IT environment and the integrity of data and information within the entity's IT system. Designing and implementing effective GITCs is an important part of management's ICFR journey because GITCs are critical to the effective operation of automated process control activities that have been identified to address RMMs.

Before GITCs are designed and implemented, management must first understand the IT layers within the entity's IT system and then identify the relevant risks arising from IT (RAFITs) within each IT layer.

- **IT layers.** The four layers of technology that comprise an IT system are application, database, operating system and network. A layer of technology is relevant to ICFR when there is one or more RAFITs within that layer of technology that is relevant to the effective operation of automated control activities and/or the integrity of data and information within the IT system.

- **RAFITs.** RAFITs represent the susceptibility of automated control activities to ineffective design or operation, or risks to the integrity of information in the entity's IT systems, due to ineffective design or operation of GITCs. A relevant RAFIT is an IT risk where there is a 'reasonable possibility' that the risk could prevent the effective operation of the related automated control activity and/or affect the integrity of data within the IT system.

- **GITCs.** GITCs are not expected to directly prevent, or detect and correct, material misstatements. However, ineffective GITCs may lead to automated control activities that don't operate consistently and effectively, which may lead to the automated control activities not preventing, or detecting and correcting, a material misstatement on a timely basis. Preparing and retaining sufficient documentation to evidence the design, implementation and operation of the entity's GITCs is important to demonstrating the effectiveness of the entity's ICFR.

Management monitors the effectiveness of GITCs designed to address relevant RAFITs, which may result in the identification of GITC deficiencies.

- **Monitoring procedures over GITCs.** GITCs are included in management's monitoring, which may involve testing the operating effectiveness of the control activities. If monitoring involves direct testing of GITCs, it should be performed throughout the period.
- **GITC deficiencies.** If GITCs are ineffective, management may not be able to rely on the automated control activities and/or the integrity of the information the GITCs support, which may impact management's conclusions on ICFR effectiveness.

Consideration must be given to cybersecurity risks when identifying, designing and implementing GITCs.

Read more: Chapter 7

Service organizations

An entity (user entity) may engage another entity (service organization) to provide services that become part of the user entity's information systems. Common services provided by service organizations are payroll processing and hosting services for applications or IT infrastructure components.

Depending on the nature of the services provided, a service organization is often considered part of the user entity's control environment. When that is the case, the service organization becomes part of management's ICFR journey, which results in management needing to:

- understand the service organization's processes;
- evaluate the nature, timing and extent of the service organization's controls and related testing; and
- assess deficiencies at a service organization in its evaluation of ICFR deficiencies.

Key to performing these activities is whether the service organization provides a SOC report to management, and if so, the nature and contents of that report.

Specific management responsibilities related to a SOC report include:

- reviewing the SOC report to determine whether it provides the entity's management with sufficient evidence to address risk points in the service organization's processes;
- implementing appropriate complimentary user entity controls as indicated in the SOC report;
- evaluating deficiencies identified in the SOC report;
- identifying relevant information the SOC report covers or affects;

- evaluating whether the period(s) the SOC report covers is appropriate for the entity, including performing appropriate procedures over the period subsequent to the period addressed in the SOC report; and
- responding when a SOC report is not available or identifying 'control gaps' when a SOC report does not achieve the desired objectives of the entity's management.

Read more: Chapter 8

Identifying and evaluating deficiencies

Control deficiencies may be discovered at any point in management's ICFR journey. 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. The existence of a control deficiency means that there is an opportunity for a misstatement to occur, even though a misstatement may not have occurred.

Identifying and evaluating control deficiencies may seem straightforward, but challenges may, and often do, arise. The following six-step process may help management to properly identify and evaluate the severity of control deficiencies, while avoiding or properly navigating common challenges.

Identifying the internal control deficiency	
Step 1	Determine whether a deficiency exists and identify the deficient or missing control
Step 2	Understand the cause of the deficiency
Step 3	Determine whether the deficiency is indicative of other deficiencies
Evaluating the internal control deficiency	
Step 4	Evaluate the severity of the deficiency individually
Step 5	Evaluate the effect of compensating controls and conclude on the severity of the individual control deficiency
Step 6	Evaluate the severity of similar deficiencies in the aggregate

Read more: Chapter 9

Artificial intelligence and automation

The use of AI and automation is being increasingly embraced across industries to transform all areas of business, including financial reporting.

While driving both productivity and efficiency and having the potential to increase the quality of financial reporting, AI and automation also introduce additional operational, financial reporting, and regulatory risks. Management and those tasked with corporate governance over the financial reporting process are expected to identify AI and automation tools currently in use, evaluate the ones being considered, identify the accompanying risks and respond to those risks by establishing strong governance and control policies and procedures over the tools' development, acquisition, deployment and operation.

Read more: Chapter 10

2. Entity-level controls

Detailed contents

Examples

2.5 Risk assessment

Questions

Examples

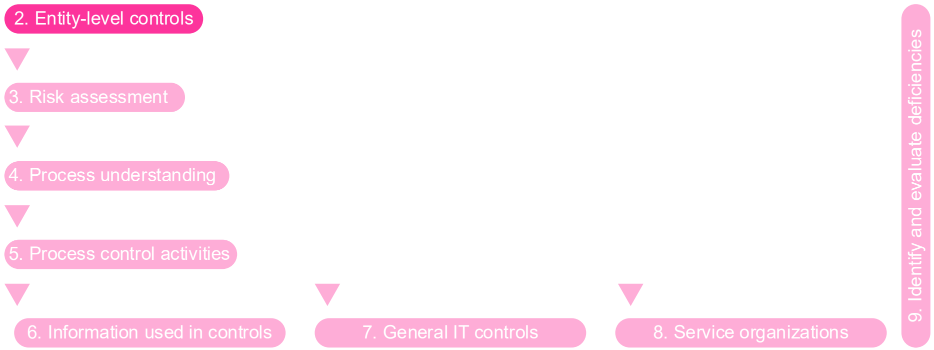
Questions

Examples

Questions

Examples

2.1 Management's ICFR journey



Entity-level controls represent a broad range of controls that operate at the entity level instead of the process level. They often have an indirect relationship to financial reporting because they are designed to operate through a top-down approach.

The board of directors and others charged with governance play an important role in identifying, implementing, executing and monitoring the effectiveness of entity-level controls. Within this chapter, 'those charged with governance' is used to capture the board of directors, audit committee and any others that are charged with governance of the entity.

After discussing the basics of entity-level controls, this chapter concentrates on those controls in the context of each internal control component (except for process control activities, which are discussed in chapter 5) by:

- providing additional information about each component;
- highlighting the specific principles related to each component; and
- identifying and providing examples of entity-level controls related to the principles.

Appendix A includes the COSO Framework's points of focus, which are important characteristics of each principle and help management to:

- design, implement and conduct an integrated system of ICFR; and
- assess whether controls responsive to each principle are designed and operating, and therefore, the principles are present and functioning.

Abbreviations

We use the following abbreviations in this chapter.

COSO	Committee of Sponsoring Organizations of the Treadway Commission
GAAP	Generally accepted accounting principles
GITC	General IT control
ICFR	Internal control over financial reporting
PCAOB	Public Company Accounting Oversight Board

RMM	Risk of material misstatement
SEC	Securities and Exchange Commission
SOC	System and Organization Controls

2.2 The COSO Framework

Question 2.2.10

What are the five components of ICFR?

Interpretive response: The five components of ICFR are the interrelated elements of internal control established by the COSO Framework that must be present and functioning for an effective integrated system of internal controls.

The table below describes each of these components further.

**Control environment
(section 2.4)**

The control environment includes:

- the set of standards, processes and structures that provide the basis for carrying out ICFR; and
- the attitudes, awareness and actions of those charged with governance and management concerning the entity's ICFR and its importance.

The control environment also:

- sets the tone at the top of the entity;
- influences the control consciousness of its people; and
- provides the overall foundation for the operation of other components of the entity's ICFR.

**Risk assessment
(section 2.5, chapters 3 and 4)**

Risk assessment is a dynamic, iterative process for:

- identifying and analyzing risks to achieving the entity's objectives;
- identifying the risks to manage; and
- determining how to manage the risks identified.

As part of risk assessment, management considers possible changes that may impede the entity's ability to achieve its objectives. These changes can be present in the external environment and/or within their own business.

**Information and communication
(section 2.6 and chapter 6)**

The information and communication component addresses:

- the importance of information management and continuous communication between and among those responsible for ICFR, both internal and external; and
- how reliable information from both internal and external sources is needed to support the functioning of the other four components of internal control.

**Control activities
(chapters 5 and 7)**

Control activities are actions, governed by established policies and procedures, that directly address financial reporting risks.

Control activities are performed:

- at all levels of the entity;
- at various stages within business processes relevant to ICFR; and
- over the consistent and effective operation of technology relied on in ICFR.

Monitoring activities (section 2.7)

Monitoring activities are required to:

- determine whether controls are designed and operating to evidence the five components of internal control, and each principle associated with those components, are present and functioning;
- determine that the established controls function in a manner to effectively address the current risks to the entity's financial reporting process; and
- identify deficiencies in internal control and communicate those deficiencies to the parties responsible for taking corrective action, including those charged with governance, as relevant.

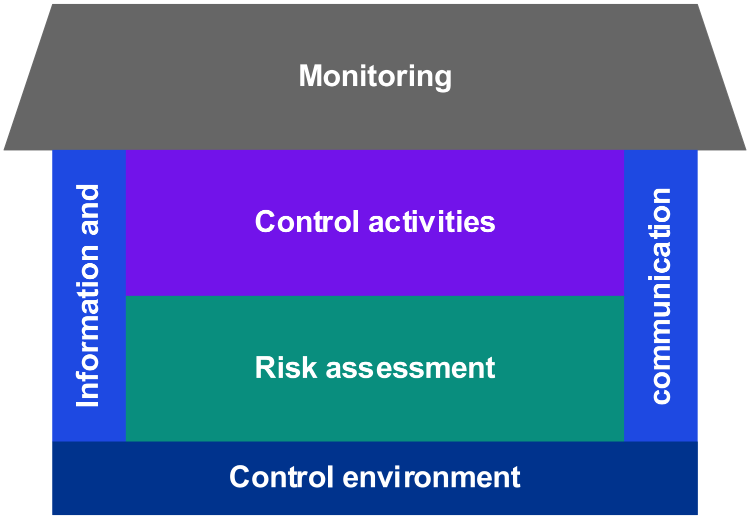
Monitoring activities may include ongoing evaluations, separate evaluations that are performed periodically, or a combination of both.

Question 2.2.20

Are the five components of ICFR interrelated?

Interpretive response: For a system of internal controls to be effective, each of the five components of internal control and the related principles must be present and functioning, and the five components must operate together in an integrated manner.

To understand the importance of the five components operating together in an integrated manner, think of the five components of internal control as different parts of a house (e.g. roof, foundation, walls). Each component plays a unique but important role contributing to an entity's overall system of ICFR. If one component is missing or not functioning properly, the implications to an entity's overall system of ICFR can be significant – like a house without walls or a foundation.



Question 2.2.30

What are COSO principles as they relate to the five components of ICFR?

Interpretive response: The COSO Framework includes 17 principles that underpin each of the five components of ICFR as fundamental concepts. The 17 principles form the basis for designing an effective integrated system of ICFR.

For an ICFR system to be 'effective,' each of the five components, including the principles *within* each component, must be present and functioning.

'Present' refers to the determination that components and relevant principles exist in the design and implementation of the entity's system of ICFR.

'Functioning' refers to the determination that components and relevant principles continue to exist in the operation of the entity's system of ICFR.

Appendix A includes the COSO Framework's points of focus, which are important characteristics of each principle and help management to:

- design, implement and conduct an integrated system of ICFR; and
- assess whether controls responsive to each principle are designed and operating, and therefore, the principles are present and functioning.

Question 2.2.40

Does management need to have controls that address each of the 17 COSO principles?

Interpretive response: Yes. The COSO Framework views all five components and all 17 principles as relevant to an integrated system of internal controls, irrespective of the entity or its objectives. Controls must be designed and operating under each of the 17 principles to demonstrate that the principle has been achieved.

Often, entities will start by taking a bottoms-up approach to map existing controls within the entity's process to each of the 17 principles to determine whether there are controls under each principle. Caution should be exercised because missing from this approach might be an overall assessment, or a top-down evaluation, of whether the controls that have been mapped are sufficient to demonstrate that the principle has been achieved. Typically, the number of controls and nature of controls under each principle will vary from entity to entity based on the nature of the business and results of the entity's own risk assessment.

A control deficiency exists in the entity's system of ICFR if:

- insufficient controls exist to demonstrate that the principle has been achieved; and/or
- controls are not designed appropriately to address the principle.

Practical tip

Due to their nature, some controls address multiple principles, even across different components. For example, having a code of conduct and effective communication about it via the entity's intranet and annual compliance training can address both:

- Principle 1 (see Question 2.4.60) because it demonstrates a commitment to integrity and ethical values; and
- Principle 14 (see Question 2.6.90) because it shows how the commitment to integrity and ethical values is communicated.

2.3 Entity-level controls: The basics

Question 2.3.10
What are entity-level controls?

Interpretive response: Entity-level controls describe a broad range of controls that operate at the entity level rather than at the process level. Entity-level controls include established policies, procedures and structures that have an important but indirect relationship to financial reporting. This is because they are designed to operate through a top-down approach to address the principles under control environment, risk assessment, information and communication, and monitoring within an entity's overall integrated system of ICFR.

Question 2.3.20
How do entity-level controls differ from process control activities?

Interpretive response: Process control activities (addressed in detail in chapter 5) are designed to operate at a level of precision that 'would' adequately prevent, or detect and correct, misstatements on a timely basis. In contrast, entity-level controls usually have an indirect, but still important, effect on the likelihood that a misstatement will be prevented or detected on a timely basis – a 'could' level of precision. Rather than directly mitigating a risk, entity-level controls are typically policies, procedures, processes and structures that support the effective operation and oversight of the entity's system of ICFR, including process control activities.

Entity-level controls *support* control activities, which include process control activities, by facilitating the existence of:

- an environment in which control activities can operate effectively;
- a process to identify risks to financial reporting that need to be addressed by control activities; and
- activities to monitor the effectiveness of the control activities.

Question 2.3.30

What is a ‘would’ level of assurance for a control?

Interpretive response: Process control activities operate at a ‘would’ level of assurance. 'Would' means 'probable' in the context of designing process control activities to prevent or detect and correct material misstatements in the entity’s financial statements.

Process control activities, unlike entity-level controls, must be selected and developed by an entity to directly mitigate the identified risks to the achievement of financial reporting objectives to acceptable levels. The COSO Framework’s objective is for the entity’s ICFR to achieve reasonable assurance – meaning process control activities must be designed and functioning to make it ‘probable’ the entity will achieve its financial reporting objectives. Absolute assurance is not possible due to limitations inherent in in all systems of internal control, such as human error, judgment uncertainty and events outside management’s control.

For a control to function properly as a process control activity, it needs to be designed and operated in a manner to confidently support that it ‘would’ (i.e. probably will) prevent, or detect and correct, a material misstatement in response to the risk being addressed. Question 2.3.20 discusses how process control activities differ from entity-level controls.

Question 2.3.40

What is a ‘could’ level of assurance for a control?

Interpretive response: Entity-level controls require at least a ‘could’ level of assurance. ‘Could’ means ‘may’ or ‘might’ in the context of a control’s ability to prevent or detect a material misstatement to the entity's financial statements. It does not mean ‘probable.’

Entity-level controls typically function at the ‘could' level as they could alert an entity to the existence of a potential error or misstatement in financial reporting; however, they do not operate at a precise enough level of detail to provide reasonable assurance (e.g. probable) that the financial statements will be free from material misstatement.

For example, a monitoring control that reviews the fluctuation in consolidated financial statement account balances year-over-year may identify an unusual fluctuation that management investigates further. However, the act of performing the fluctuation analysis itself does not directly address the risk as to whether the transactions in the account were processed completely and accurately (e.g. at the assertion level within the process).

Due to their lack of precision, entity-level controls are not likely to mitigate the risk that the financial statements will be free from material misstatement to an acceptable level.

Question 2.3.50

How does an entity evidence that entity-level controls are designed and operating?

Interpretive response: Management is required to prepare and retain sufficient documentation to:

- evidence the entity-level controls designed and implemented to achieve the principles of each component of internal control addressed individually and/or in combination with other controls; and
- evidence the entity-level controls are operating as intended in an integrated manner.

Management assumes a greater responsibility for detailed documentation when it asserts to regulators, shareholders or other third parties that the entity's ICFR is effective. In cases where an external auditor attests to the effectiveness of an entity's system of internal control, management will likely be expected to provide the auditor with support for its assertion on the effectiveness of its ICFR.

The extent of evidence will vary based on the nature of the control. By nature, entity-level controls often require less extensive documentation in comparison to control activities. This is because entity-level controls operate at a higher level of precision and are related to control components and principles generally achieved through the establishment of policies, procedures and structures operating at the top levels. As a result, the operation of entity-level controls can often be evidenced through inspection and observation of published documentation already made available to those responsible for ICFR.

However, in general, management is expected to retain documentation that would enable someone with reasonable knowledge of the entity and financial reporting to understand the design and operation of the control. The documentation is also expected to show the results of operating the control, including any further investigation required to conclude the control is designed and operating.

For example, consider an entity-level control related to the control environment whereby the entity's ethics and compliance committee has established policies and procedures to identify and address improprieties and noncompliance by employees, third-party service providers, and other business partners. When determining the documentation necessary to support the operation of this control, the documentation must include evidence that there is a process for identifying, assessing and evaluating the financial reporting implications of noncompliance matters. In addition, documentation must exist to evidence that:

- instances of noncompliance requiring investigation were appropriately captured;
- the severity of noncompliance matters was appropriately assessed on a timely basis;
- the investigation into noncompliance matters was conducted in accordance with the entity's policies based on the severity assessed; and
- the financial reporting implications of noncompliance matters were properly evaluated by an appropriate member of the accounting and financial reporting department on a timely basis.

Practical tip

It is important that documentation of entity-level controls is available and sufficiently detailed to demonstrate that the entity-level controls are designed and operating effectively. Often entity-level controls may be carried out through meetings, either between key members of management or those charged with governance, or both. Due to the timing and nature of these meetings, those performing monitoring or testing may not be able to directly observe (i.e. attend) the meetings where the entity-level controls operate. Therefore, the minutes, agendas and materials related to the meeting are the primary evidence of the discussions held and conclusions reached (i.e. the operation of the entity-level control). For those materials to sufficiently evidence the operation of the control, they should be detailed, finalized, and approved timely.

Question 2.3.60

What is considered when designing and documenting an entity-level control?

The following table sets out the items considered when designing an entity-level control. The considerations in the table should also be present in the documentation (see Question 2.3.50) for each entity-level control. Some considerations only apply to manual controls, where indicated.

Considerations	Description	Section/ Question
Control objective	The principle the control is intended to address. This is achieved using control attributes.	5.5
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.	5.6
Frequency	The frequency with which a manual control is performed, which could be:	5.7

Considerations	Description	Section/ Question
	• annually; • quarterly; • monthly; • weekly; • daily; • recurring; or • ad hoc.	
Authority and competence of the control operator (see Question 5.4.40)	The level of competence and authority necessary to operate a manual control (i.e. is the right person performing the control?).	5.8
Information used in the performance of the control	Information is usually used when performing a manual control (e.g. system reports, manually prepared spreadsheets, queries), including the relevant data elements (see Question 6.2.40).	2.3.70

Practical tip

Clear and concise documentation of the design of entity-level controls (addressing the considerations in the preceding table) provides evidence to support the achievement of the ICFR principles. Clear documentation of the design of the entity-level control also enables management to perform separate evaluations necessary to monitor that the ICFR principles are present and functioning.

For example, if the design of a control is not clear in its documentation, the control may fail to function properly if the control operator leaves the entity and the control needs to be reassigned to a new person.

Question 2.3.70

How does the control operator consider the relevance and reliability of information used in entity-level controls?

Interpretive response: Prevalent throughout an entity's system of ICFR, information must be sufficiently relevant and reliable for use in controls. To establish the relevance and reliability of information used in entity-level controls, the control operator should understand the source and the nature of the information used (see Appendix D for practical guidance on evaluating the relevance and reliability of information used in controls).

If the control operator assumes that information used in a control is relevant and reliable without having a basis for that assumption, the information may contain errors that could lead to incorrect conclusions about the entity-level control.

The assessment of relevance and reliability for information used should be included in the control operator's documentation as part of the design and operation of the entity-level control.

Example 2.3.10
Evaluating the reliability of information used in whistleblower hotline entity-level control

Background: On a quarterly basis, those charged with governance monitor the calls received through the entity's whistleblower hotline, which is operated by a third-party operator. The individual responsible for assessing the content of calls received through the hotline prepares a presentation to summarize calls received for those charged with governance. The summary is supported by reporting received from the third-party operator provided along with the presentation.

On behalf of those charged with governance, a separate evaluation is performed by Internal Audit at least annually to assess whether the whistleblower hotline is operating effectively by conducting a test call and ensuring the details of the test call are completely and accurately captured in the third-party operator's reporting back to those charged with governance.

Assessment*:* The control operator concludes within the entity-level control documentation that the information used in the entity-level control (listing of calls received through the whistleblower hotline presented to those charged with governance) is:

- relevant, because the information details reports received through the hotline during the quarter; and
- reliable, because the information is sourced from the third-party operator's reporting, which is monitored for completeness and accuracy.

Question 2.3.80
Is management required to test entity-level controls?

Interpretative response: Yes. Entity-level controls are tested as part of monitoring if management determines it appropriate to perform separate evaluations as part of their monitoring activities (see Question 2.7.200).

2.4 Control environment

Question 2.4.10
What is the control environment component of ICFR?

Interpretive response: The control environment component of ICFR is the set of standards, processes and structures that provide the basis for carrying out internal controls across an entity.

The control environment includes:

- the integrity and ethical values of the organization;
- the structure and oversight of those charged with governance;
- the governance, roles and responsibilities of management functions;
- the process for attracting, hiring and retaining competent individuals; and
- the rigor around performance measures and rewards to drive accountability for performance of internal control responsibilities

Those charged with governance and management set the tone at the top regarding the importance of internal control including the expected standards of conduct. Management also reinforces expectations at all levels of the organization relevant to financial reporting.

Question 2.4.20
Does the control environment encompass all levels of an entity?

Interpretive response: Yes. The control environment underpins how ICFR is carried out across all levels of the entity. An entity likely will need to assess the effectiveness of the control environment at levels below the parent or corporate level (e.g. regions, divisions, operating units, functional areas).

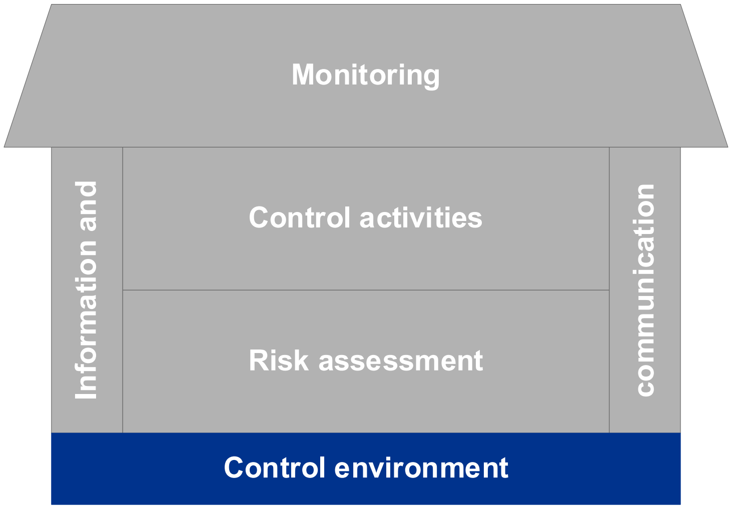
Question 2.4.30
Does the control environment encompass third-party service providers?

Interpretive response: Yes. The control environment includes third-party service providers (e.g. a third-party that provides payroll processing) and business partners. Although the entity may rely on an outsourced service provider to conduct business processes, policies and procedures on behalf of the entity, management retains ultimate responsibility for ICFR effectiveness, including the controls around risks associated with outsourced activities. Therefore, third-party service providers must be considered in designing effective entity-level controls to enable principles within the control environment to be present and functioning.

Question 2.6.70 discusses further considerations for third-party service providers in entity-level controls.

Question 2.4.40
What is the relevance of the control environment to ICFR?

Interpretive response: Entity-level controls addressing the principles of the control environment provide the foundation on which the other components of ICFR are able to function properly.



If an entity lacks the overall governance, structure or tone at the top to promote and manage the entity's system of ICFR, it is more likely that deficiencies exist in other areas of the entity's system of ICFR.

Question 2.4.50
What are the principles in the COSO Framework related to the control environment component of ICFR?

Interpretive response: There are five principles necessary for an effective control environment within a system of ICFR. Designing and putting in place controls that collectively achieve all five principles demonstrates that the control environment is established appropriately to support the rest of the entity's system of ICFR.

Control environment	
Principle 1	The organization demonstrates a commitment to integrity and ethical values.

Control environment	
Principle 2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
Principle 3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
Principle 4	The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
Principle 5	The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Source: COSO Internal Control – Integrated Framework (2013).

Question 2.4.60
What is the importance of an entity demonstrating a commitment to integrity and ethical values (Principle 1)?

Interpretive response: The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer and monitor them (i.e. tone at the top).

Integrity and ethical behavior are the product of the entity's ethical and behavioral standards or codes of conduct and how they are communicated and reinforced in practice.

The communication of entity policies on integrity and ethical values may include the communication of behavioral standards to personnel through policy statements, codes of conduct and by example.

The reinforcement of entity policies on integrity and ethical values may occur through management's actions to eliminate or mitigate incentives or temptations that might promote personnel to engage in dishonest, illegal or unethical acts.

Question 2.4.70
What is the tone at the top?

Interpretive response: The tone at the top of an entity comes from management and those charged with governance leading by example in creating and maintaining the entity's culture by developing values, a philosophy and an operating style for the entity. An appropriate tone at the top and throughout the organization is fundamental to the effective functioning of an internal control system.

Question 2.4.80

Why is a consistent tone at the top important to the control environment?

Interpretive response: A consistent tone from those charged with governance and management (including at operating units) helps establish a common understanding of the values, business drivers and expected behavior of employees and partners of the entity.

Not having a consistent tone at the top to support a strong culture of internal control undermines the awareness of risk and can lead to:

- inappropriate responses to risks;
- lack of focus and discipline around control activities that may result in deficiencies in their design and operating effectiveness;
- lack of information and miscommunication; and
- lack of action on feedback from monitoring activities.

The consistency of the tone at the top can therefore either drive or impede internal control; for example:

Drivers	Impediments
• History of consistent ethical and responsible behavior by management and those charged with governance • Demonstrated commitment to addressing misconduct	• Personal indiscretions • Lack of receptiveness to bad news • Unfairly balanced compensation practices

These behaviors could positively or negatively affect an entity's culture and its employees' conduct and integrity. Employees are likely to develop the same attitudes about right and wrong – and about risks and controls – as those shown by management.

Question 2.4.90

What drives the tone at the top?

Interpretive response: The tone at the top is driven by the following characteristics of management and those charged with governance:

- operating style;
- personal conduct;
- attitudes toward risk;
- approach to making judgments (e.g. conservative versus aggressive positions on estimates and policy choices); and
- degree of formality (e.g. potential for more informal controls in a small family business).

Question 2.4.100
How does an entity document and demonstrate the tone at the top?

Interpretive response: An entity often documents and demonstrates the expectations of management and those charged with governance in the form of:

- missions and value statements;
- standards or codes of conduct;
- policies and practices; and
- operating principles, directives, guidelines and other supporting communications.

Management and those charged with governance also demonstrate the tone at the top through their:

- actions and decisions;
- attitudes and responses to violations and deviations; and
- informal and routine communications.

Practical tip

Tone at the top and other control environment entity-level controls are sometimes evidenced through meetings of the Board of Directors and other subcommittees. The minutes of these meetings should be at a detailed enough level to provide evidence of the nature of the discussions and how the entity has met the related principle. In addition, these minutes should be approved in a timely manner (e.g. at the following meeting, or if meetings are sparse/annual, via other methods).

Example 2.4.10
Controls that may be in place to address Principle 1

Principle 1: The organization demonstrates a commitment to integrity and ethical values.

Example controls that may be in place to address Principle 1 include:

- The code of conduct defines and communicates expectations on integrity, ethical values and compliance with laws and regulations at all levels of the entity and key external parties.

- The ethics and compliance committee verifies that all employees and key external parties acknowledge receipt of the code of conduct and confirm compliance status annually.

- All employees complete training on the code of conduct.

- The ethics and compliance committee establishes policies and procedures to identify and address improprieties and noncompliance with the code of conduct and other matters by employees, third-party service providers and other business partners.

- The CEO's quarterly newsletter emphasizes the importance of ethics and compliance with the code of conduct.

Question 2.4.110

What is the importance of those charged with governance demonstrating independence and exercising oversight of ICFR (Principle 2)?

Interpretive response: The 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 importance of ICFR oversight responsibilities being held by those charged with governance is recognized in codes of practice and other laws and regulations, as well as guidance produced for their benefit.

The independence of those charged with governance is important due to their responsibility to question and evaluate the activities of management.

Question 2.4.120

How is the control environment influenced by the independence of those charged with governance?

Interpretive response: When independent of management, those charged with governance provide value to the oversight of ICFR through their impartiality, healthy skepticism and unbiased evaluation. This independence allows them to question and scrutinize management's activities, present alternative views, and have the courage to act in the face of obvious or suspected wrongdoing.

Example 2.4.20

Controls that may be in place to address Principle 2

Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Example controls that may be in place to address Principle 2 include:

- the board of directors establishes its roles and responsibilities for the oversight of internal control;

- the board of directors' risk and governance committee oversees the content and communication of the code of conduct, as well as investigation and resolution of noncompliance;
- based on its charter, the audit committee is primarily responsible for overseeing external financial reporting and ICFR;
- the board of directors oversees the design and effective operation of whistle blower procedures; and
- the board of directors completes a directors and officers (D&O) questionnaire each year, which is reviewed by the entity's general counsel to identify potential independence matters.

Practical tip

When an entity uses D&O questionnaires to evidence Principle 2 (independence from management), management should consider:

- the timeliness of the questionnaire;
- the completeness of the population of individuals that fill out the questionnaire;
- whether the questionnaire is sufficiently robust in nature to prompt considerations of potentially uncommon relationships or other independence matters;
- the sufficiency of the control in place to review the questionnaires; and
- the process in place to include any related-party relationships identified in the questionnaires on the related-party listing.

Question 2.4.130

What is the importance of management establishing structure, authorities and responsibilities (Principle 3)?

Interpretive response: Management and those charged with governance establish the organizational structure and reporting lines to carry out their oversight responsibilities. Along with delegating authority and responsibility, the structure provides accountability to management and other personnel. Competency should be considered as part of proper application of how authority and responsibility are delegated.

Example 2.4.30

Controls that may be in place to address Principle 3

Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Example controls that may be in place to address Principle 3 include:

- The entity uses organization charts and documented authorization policies to establish reporting lines, and to define, assign and limit authorities and responsibilities. This documentation is revised to respond to change as needed and is communicated throughout the organization.
- The entity's Operating Policies and Procedures Manual details the monetary commitment and transaction approval authorities of management and employees for each occurrence. Exceeding the individual transaction's authority requires approval from the appropriate member of higher-level management, up to and including the CEO.

Question 2.4.140

What is the importance of an entity's ability to attract, develop and retain talent (Principle 4)?

Interpretive response: Effective ICFR is designed, implemented and carried out by employees of the entity. If an entity does not have appropriate programs and processes in place to attract, develop and retain competent individuals, there may not be enough employees with the right level of competence and authority (see section 5.8 for further discussion) to perform the controls as designed. In turn, this may result in deficiencies in other components of ICFR.

Example 2.4.40

Controls that may be in place to address Principle 4

Principle 4: The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Example controls that may be in place to address Principle 4 include:

- the entity identifies the competencies needed to support effective financial reporting and ICFR, evaluates competencies across the entity and at external service providers, and acts to address gaps;
- the entity establishes policies to attract employees, third-party service providers and other professionals with sufficient competencies, and provides training to maintain and develop sufficiently competent personnel; and
- the entity establishes contingency, and succession plans to prepare for re-assignment of financial reporting and ICFR responsibilities in the event of changes in leadership.

Question 2.4.150
What is the importance of holding individuals accountable for ICFR (Principle 5)?

Interpretive response: Along with the other principles, holding individuals accountable for their internal control responsibilities helps to enforce the entity's commitment to ICFR, as well as values of integrity and ethics. By connecting internal control responsibilities to established performance measures, management and those charged with governance reinforce the tone at the top that ICFR is important to the entity at all levels.

Example 2.4.50
Controls that may be in place to address Principle 5

Principle 5: The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

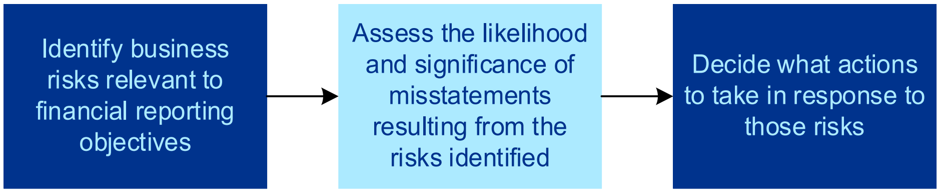
Example controls that may be in place to address Principle 5 include:

- Quarterly, the director responsible for compliance with the Sarbanes-Oxley Act asks employees with internal control responsibilities (control operators) to:
  - confirm their accountability; and
  - represent they have fulfilled their internal control responsibilities during the quarter, highlighting any exceptions.
- The entity's performance incentive plans establish performance measures that:
  - incorporate ICFR and ethical responsibilities;
  - consider excessive pressures; and
  - provide rewards or penalties, as appropriate.
- The entity's annual employee performance reviews and employee incentive rewards reinforce expected standards of behavior, consistent with the entity's code of conduct, including:
  - adherence to their ICFR responsibilities;
  - evaluation of their competencies; and
  - achievement of business goals.

2.5 Risk assessment

Question 2.5.10
What is the risk assessment component of ICFR?

Interpretive response: An entity's risk assessment process relevant to the preparation of the financial statements includes the entity's processes to:



Identify business risks relevant to financial reporting objectives

Assess the likelihood and significance of misstatements resulting from the risks identified

Decide what actions to take in response to those risks

Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Rarely in practice do entities formally identify and assess risks on a daily basis. Risk assessment is often an annual process or may be quarterly, depending on the entity's financial reporting requirements. In addition, changes in the external environment or within an entity's own business model result in the need for identification and assessment of new risks by management and/or the reconsideration of prior risk assessments.

Question 2.5.20
What is the relevance of risk assessment to ICFR?

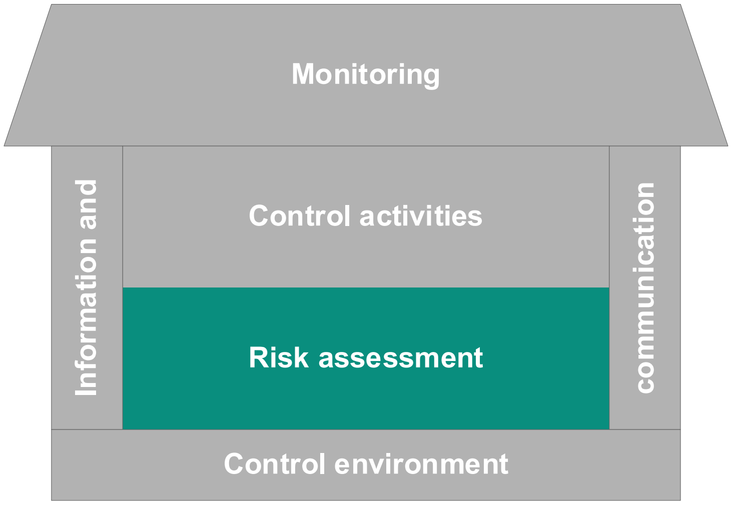
Interpretive response: Risk assessment is an important component of ICFR because it forms the basis for how management:

- identifies and analyzes risks relevant to its financial reporting objectives; and
- determines the risks to be managed.

Failure to perform an appropriate risk assessment process may lead to:

- unidentified/unaddressed risks relevant to an entity’s financial reporting objectives;
- ineffectively designed control activities; and
- increased possibility of a misstatement in the financial statements.

Using the house example, the risk assessment process is the blueprint or map of the house, which is needed for the house to be appropriately designed and built.



Question 2.5.30
What is an entity-level risk assessment?

Interpretive response: The entity-level risk assessment is the top level of an entity's risk assessment process. It refers to the risk assessment performed at the level of the consolidated entity and its components, which may be subsidiaries, divisions or entities or business units.

The identification and assessment of ICFR-related risks at the entity level helps the entity identify a comprehensive population of risks to the achievement of its financial reporting objectives. Chapter 3 provides more information on considerations in performing an effective risk assessment, and chapter 4 dives into process-level risk assessment, which accompanies the entity-level risk assessment.

Question 2.5.40
At what level within the entity is risk assessment performed?

Interpretive response: The COSO Framework makes it clear that, for purposes of ICFR, management should perform its risk assessment at various levels within the entity. This is a top-down approach that starts at the entity level and moves down to the business process level to identify risks to preparing financial statements free from material misstatement.

Question 2.5.50

How is an entity-level risk assessment typically documented?

Interpretive response: Entities can evidence their entity-level risk assessment in multiple ways, including through:

- a formal Business Risk Assessment that had been provided to the Risk and Governance Committee for input and approval, which includes identifying, assessing and making plans to mitigate the related operational and compliance risks;
- analyzing business plans and associated business risks from Business Risk Assessment meetings to identify and assess associated financial reporting risks related to significant accounts;
- analyzing business plans and associated business risks from the Business Risk Assessment meetings to identify and assess associated financial reporting risks related to significant accounts;
- the ICFR Risk and Control Matrix, which is accessible to employees with ICFR roles; and
- the annual plan and financial forecast, that had been provided to the Board for input and approval.

Proper documentation of the process-level risk assessment discussed in chapter 4, in conjunction with documentation of the entity-level risk assessment discussed in this chapter and chapter 3, is necessary to evidence the risk assessment component of COSO is present and functioning.

Question 2.5.60

When should an entity's risk assessment process be documented?

Interpretive response: Because much of the risk assessment process takes place in meetings and discussions – including senior levels of management and those charged with governance – timely documentation of the risk assessment activities undertaken by the entity and their results helps demonstrate an effective assessment of the entity's ICFR.

Question 2.5.70

When does an entity perform its entity-level risk assessment process?

Interpretive response: Risk assessment at the entity level should be formally performed, or updated, and documented at least annually.

However, an effective risk assessment process is iterative in nature. The COSO principles within the risk assessment component of ICFR are not always considered sequentially given the significant overlap among the principles. Further, as an entity performs and monitors controls, management may identify factors that require previous risk determinations to be re-evaluated. Changes in internal or external factors may indicate a need for re-evaluation.

Question 2.5.80

What are the principles in the COSO Framework related to the risk assessment component?

Interpretive response: The COSO Framework sets out four principles for the risk assessment process component of ICFR. Meeting all four principles demonstrates that controls have been designed and implemented effectively to meet the risk assessment objectives.

Risk assessment	
Principle 6	The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
Principle 7	The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
Principle 8	The organization considers the potential for fraud in assessing risks to the achievement of objectives.
Principle 9	The organization identifies and assesses changes that could significantly impact the system of internal control.

Source: COSO Internal Control – Integrated Framework (2013).

Question 2.5.90

What is the importance of specifying objectives to identify and assess risks (Principle 6)?

Interpretive response: An entity must set its objectives first because it is the basis on which risk assessment is performed. Once the objectives have been set, the risks to achieve those objectives can be ascertained.

In the context of financial reporting objectives, typically the objective of ICFR is to provide reasonable assurance regarding the reliability of an entity's financial reporting for external purposes in accordance with US GAAP (or other relevant accounting framework).

Without clear objectives, risk assessment activities will likely be inefficient and are likely to result in deficiencies in other components of internal control.

Example 2.5.10
Controls that may be in place to address Principle 6

Principle 6: The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Example controls that may be in place to address Principle 6 include:

- The entity specifies financial reporting and ICFR objectives that are consistent with US GAAP and SEC regulations, reflect the entity's activities and consider materiality.
- The entity's accounting policies for all financial statement accounts, underlying transactions and disclosures are:
  - maintained by the Financial Reporting Manager responsible for SEC reporting; and
  - reviewed and approved by the Corporate Controller and CFO.
- Management assesses materiality at the consolidated financial statement level at the beginning of the fiscal year, and again as necessary if the entity's business changes (e.g. the results of operations and financial position change significantly).
- The entity monitors compliance with laws and regulations that could potentially have a significant effect on financial reporting in the event of noncompliance.

Question 2.5.100
What is the importance of identifying risks to the achievement of objectives across the entity and performing an analysis on how to manage them (Principle 7)?

Interpretive response: Once the objective is clearly defined, an entity may proceed with its risk assessment process at all levels to identify a complete population of risks that could jeopardize the achievement of the objective.

Once a complete population of risks is identified, the next step is to analyze the population to design and put in place appropriate control activities responsive to the risks.

If the risk assessment process is not detailed enough or performed at all relevant levels of the organization, management may fail to identify control activities to address *all* risks that could jeopardize the achievement of the stated objective.

Additionally, if risks are not properly analyzed and understood by management, the control activities designed and put in place may fail to mitigate the identified risks, or alternatively could result in inefficiencies in the performance of control activities.

Chapter 3 provides detailed guidance on completing a risk assessment at the entity level, while chapter 4 dives into performing an effective and efficient process-level risk assessment.

Question 2.5.110

What factors does an entity consider as part of their risk assessment to demonstrate that Principle 7 is 'present' and 'functioning'?

Principle 7: The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

Interpretive response: To demonstrate that Principle 7 is 'present' and 'functioning,' an entity considers both internal and external risk factors, as well as sources of risk. For example, an entity considers those risk factors that affect the entity's ability to initiate, authorize, process and record transactions and other adjustments that are reflected in the financial statements.

Chapters 3 and 4 provide more examples of internal and external risk factors that an entity may consider as part of the risk assessment process.

Example 2.5.20

Controls that may be in place to address Principle 7

Principle 7: The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

Examples of controls that may be in place to address Principle 7 include:

- The Finance Group identifies, analyzes and assesses the significance of financial reporting risks across the entity, and how it will manage those risks. This assessment is documented in an ICFR Risk and Control Matrix available to employees with ICFR roles.
- Internal Audit performs an annual risk assessment to develop the internal audit plan. The risk assessment is updated periodically to address any emerging risks.
- The Director of Financial Reporting reviews scoping material, risk assessments, and other supporting ICFR material completed by the entity's operating units to obtain a full population of risks at the entity and determine how the entity will respond to those risks.

Question 2.5.120

What is the importance of an entity considering the potential for fraud in assessing risks to the achievement of objectives (Principle 8)?

Interpretive response: Considering fraud in the risk assessment process is important because every entity faces some risk of fraud from within.

Specific to ICFR, management's financial statements could be materially misstated due to error or fraud. 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.

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. These difficulties elevate the significance of fraud risk to a level deserving of its own COSO principle, making it clear that an appropriate risk assessment process should specifically consider the vulnerability of the entity to fraudulent activity. The SEC also requires the assessment of fraud risks.

To achieve this principle, management makes an informed assessment of specific areas where fraud might exist (see Question 2.5.140) and then further analyzes the likelihood of occurrence and potential effect.

Question 2.5.130

What types of misstatements are relevant to consideration of fraud risks?

Interpretive response: Two basic types of misstatements are relevant when considering fraud risks.

Fraudulent financial reporting	
Description	**How it's accomplished**
Intentional misstatements or omissions of amounts or disclosures designed to deceive financial statement users	• Manipulating, falsifying or altering accounting records or supporting documentation • Misrepresenting or intentionally omitting events, transactions or other significant information from the financial statements • Intentionally misapplying accounting policies or principles

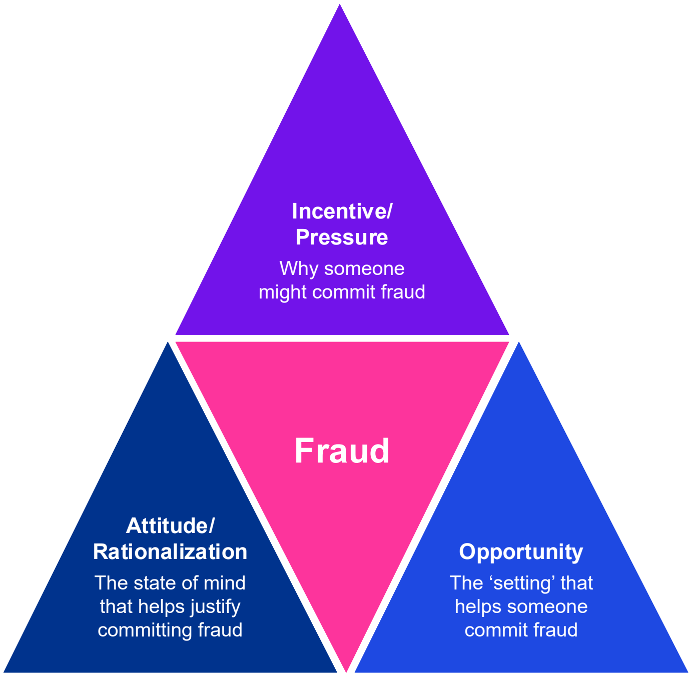
Misappropriation of assets	
Description	**How it's accomplished**
Theft of an entity's assets, causing the financial statements to be misstated	• Embezzling receipts • Stealing assets • Causing an entity to pay for goods or services that have not been received and may be accompanied by false or

Misappropriation of assets	
Description	**How it's accomplished**
	misleading records or documents, possibly created by circumventing controls

Question 2.5.140
What are fraud risk factors?

Interpretive response: Fraud risk factors include a broad range of specific events and conditions observed or identified that promote or foster an environment where fraud could occur. Understanding these factors helps identify where fraud risks may exist.

Identifying fraud risk factors does not necessarily mean that fraud exists or will eventually occur. But there are three categories of fraud risk factors often present in circumstances in which fraud exists, which make up the fraud triangle.



An example of each category of fraud risk factor is included in the following table.

Category of fraud risk factor	Example
Incentive or pressure	An employee may be in financial distress (internal incentive), or management may be under extreme pressure to meet financial targets (external incentive). These

Category of fraud risk factor	Example
	situations can be a catalyst for committing fraud and could be internal or external to the entity or the person committing the fraud.
Opportunity	Deficiencies in entity-level controls or poorly designed control activities can make it easier (or present the opportunity) for an individual to carry out fraud.
Attitude or rationalization	Management's attitude that the entity will meet its targets at all costs, or an employee justifying the fraud by claiming it doesn't really harm anybody.

See Appendix B for example fraud risk factors.

Question 2.5.150

What is the step an entity takes after identifying fraud risk factors?

Interpretive response: Once an entity identifies fraud risk factors, it evaluates whether the identified fraud risk factors, individually or in combination, indicate that a fraud risk is present. These identified fraud risks then require an appropriate control activities response, which is discussed in chapter 5.

Question 2.5.160

How is materiality considered in an entity's fraud risk assessment?

Interpretive response: When identifying and evaluating risks of fraud in the entity's financial reporting process, and designing and evaluating relevant anti-fraud controls, the entity considers the quantitative materiality of any potential misstatements and the qualitative effects of the fraud.

Risks of fraud generally demand careful consideration and response, even if the misstatements that could arise because of those fraud risks are lower than the quantitative measure of materiality. Section 3.3 discusses materiality.

Qualitative considerations that an entity may consider as part of its fraud risk assessment include:

- intent to achieve a particular outcome;
- involvement in the fraud by members of senior management; and
- questions about the pervasiveness of the fraud and its effect on the reliability of the entire set of financial statements.

Question 2.5.170

How are those charged with governance involved in an entity's fraud risk assessment?

Interpretive response: The COSO Framework emphasizes the importance of those charged with governance overseeing the fraud risk assessment process. This is particularly important when it comes to the risk of management override of controls. In line with the COSO Framework, those charged with governance challenge management, depending on the circumstances, when performing this oversight.

For example, based on the results of the entity's risk assessment process, those charged with governances might exercise its oversight role by, on a periodic basis:

- selecting a sample of significant accounting estimates in the financial statements; and
- reviewing and challenging management's key judgments in these estimates.

Those charged with governance might perform similar oversight for the accounting and financial reporting of significant unusual transactions and other matters that may be prone to bias and override of controls.

Example 2.5.30

Controls that may be in place to address Principle 8

Principle 8: The organization considers the potential for fraud in assessing risks to the achievement of objectives.

Examples of controls that may be in place to address Principle 8 include:

- Internal Audit performs an annual risk assessment that includes consideration of fraud risks;
- the legal department reviews all proposed related-party transactions over a threshold, which are then presented to and approved by the board of directors; and
- General counsel reports all matters to the board of directors, including any issues reported to the whistleblower hotline and the actions taken.

Question 2.5.180

What is the importance of an entity identifying and assessing changes that could impact ICFR (Principle 9)?

Interpretive response: When changes occur at an entity (or to the environment the entity operates in), it can have an impact on ICFR. Unidentified changes can result in risks not being properly identified and addressed by internal controls. Many material weaknesses in ICFR are rooted in circumstances where changes occurred, but the ICFR implications were not identified or thoroughly considered.

Question 2.5.190

What types of changes to ICFR should be identified and assessed as part of Principle 9?

Principle 9: The organization identifies and assesses changes that could significantly impact the system of internal control.

Interpretive response: An entity must identify and assess changes that could significantly impact its system of internal control. The COSO Framework provides examples of such changes, including:

- changes in the external environment (e.g. regulatory, economic or physical environment);
- changes in the business model (e.g. new accounts/transactions, change in delivery of services, significant acquisitions/dispositions);
- changes in leadership (e.g. significant personnel changes); and
- changes in other internal factors (e.g. implementation of new technology).

Section 3.7 discusses changes to ICFR in more detail.

Example 2.5.40

Controls that may be in place to address Principle 9

Principle 9: The organization identifies and assesses changes that could significantly impact the system of internal control.

Examples of controls that may be in place to address Principle 9 include:

- Internal Audit performs an annual risk assessment, which includes identifying and assessing changes to risks;
- on a quarterly basis, control certifications are sent to all process owners to confirm controls are in place and operating effectively;
- management performs a risk assessment on newly acquired businesses and updates the overall entity's risk assessment; and
- a disclosure committee meeting is held quarterly to discuss any significant developments or changes during the period.

2.6 Information and communication

Question 2.6.10
What is the information and communication component of ICFR?

Interpretive response: 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.

An information system may be located at the entity, its service organization or both. It is used to generate relevant and quality information used in executing the entity's business and financial reporting objectives. For example, an information system can be used to produce and sell an entity’s products and services and/or measure and record the entity’s performance.

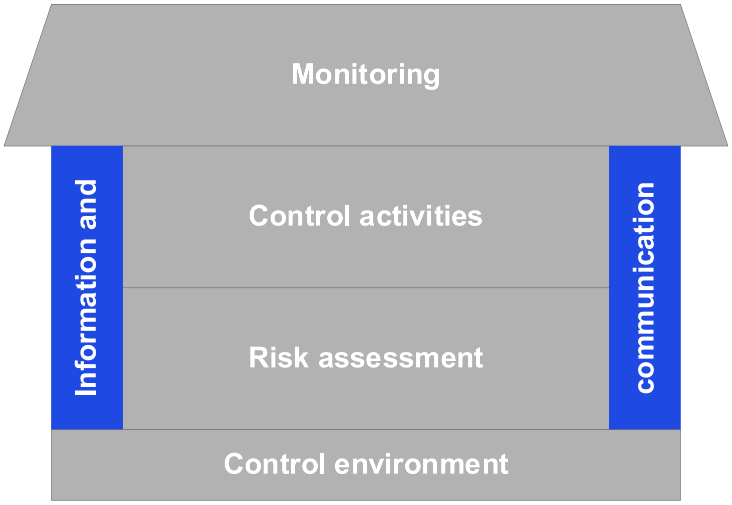
Communication, both internal and external, delivers the information the entity needs to carry out day-to-day controls. Communication also helps staff understand their internal control responsibilities and how they help achieve the entity's objectives.

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 both:

- how information flows from:
  - the initiation and authorization of individual transactions; and
  - the occurrence of other events and conditions relevant to financial reporting.
- how those transactions and other events and conditions are reported in the financial statements and related disclosures.

Question 2.6.20
What is the relevance of information and communication to ICFR?

Interpretive response: An entity's ICFR uses information and communication to achieve its ICFR objectives across all ICFR components. Continuing with the house example, information and communication are the walls and pipes of the house.



Information and communication touch all 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.

Communication is pervasive to the effective operation of an entity's overall ICFR. Consider the following two examples.

- **Communication of accounting policies –** If an entity has written accounting policies, but does not communicate them consistently across affected employees, those responsible for financial reporting may not appropriately account for transactions in accordance with the applicable financial reporting framework.
- **Communication about a legal contingency –** 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.

These examples capture the critical importance of having processes and controls in place to support effective communication about financial reporting matters.

Question 2.6.30

What are the principles in the COSO Framework related to the information and communication component?

Interpretive response: The COSO Framework sets out three principles for the information and communication component of ICFR. Meeting all three principles demonstrates that controls have been designed and implemented effectively to satisfy the information and communication objectives.

Information and communication	
Principle 13	The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.
Principle 14	The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
Principle 15	The organization communicates with external parties regarding matters affecting the functioning of internal control.

Source: COSO Internal Control – Integrated Framework (2013).

Question 2.6.40

What is the importance of an entity obtaining or generating and using relevant, quality information to support the functioning of internal control (Principle 13)?

Interpretive response: It is important for an entity to obtain or generate and use relevant, quality information to support the functioning of internal control because doing so affects management's ability to:

- make appropriate decisions in managing and controlling the entity's activities; and
- prepare reliable financial reports.

Obtaining or generating and using inaccurate or incomplete data, and information derived from such data, could result in potentially erroneous judgments, estimates, or other management decisions.

Question 2.6.50

What is the role of IT systems in the entity's information systems relevant to financial reporting?

Interpretive response: In today's technology-focused economy, using IT systems, including enterprise resource planning systems, has become commonplace. Entities often use IT systems extensively to create, share and transfer information (i.e. 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.

To enhance efficiency and effectiveness, entities may choose to automate certain functions within business processes using IT systems, including process control activities to address risks.

Automation may be particularly common when processing and reporting larger volumes of transactions. In some cases, it may not be feasible to process and aggregate information or data elements without using IT systems.

Question 2.6.60

Are general IT controls part of the information and communication or control activities component of ICFR?

Interpretive response: No. General IT controls are part of the control activities component of ICFR, which are discussed further in chapter 7.

Question 2.6.70

Are third-party service providers and business partners part of the information and communication component of ICFR?

Interpretive response: It depends. Because an entity's information system is not limited by legal boundaries, third-party service providers (e.g. a third party that provides payroll processing) and business partners contracted by that entity may be part of its information systems. Whether that is the case depends on the nature of the processes and activities the third-party service provider (or service organization) or business partner performs.

A service organization is part of the entity's information system when the processes and activities they perform:

- are part of the entity's accounting and reporting processes; or
- have an indirect effect on those processes (e.g. when a service organization performs IT processes and activities that mitigate risks arising from IT).

Chapter 8 provides detailed discussion of service organizations.

Question 2.6.80

What is the difference between Principle 13 and the control activities component of ICFR related to IT?

Principle 13: The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

Interpretive response: Principle 13 is a broadly written concept. In the context of a financial statement audit or an audit of ICFR (an integrated audit), controls over the quality of *information reported in the financial statements* are part of the control activities component of ICFR. Chapter 6 provides detailed discussion on control activities over information used in financial reporting.

In contrast, controls addressing the quality of *information used throughout the entity* – including other COSO components – *that does not appear in the financial statements* but supports the effective design and implementation of ICFR are part of the information and communication component of ICFR.

Example 2.6.10
Controls that may be in place to address Principle 13

Principle 13: The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

Examples of controls that may be in place to address Principle 13 include:

- Management prepares an inventory of information required to support financial reporting and ICFR, which is maintained on the entity's information repository, and updates the inventory of information as changes occur.
- Management retains external specialists to consult with on legal, financial and tax matters where the entity does not maintain in-house expertise.
- Management subscribes to multiple sources of information, including industry and regulatory publications, and finance personnel evaluate the information monthly.
- Senior finance personnel meet monthly with management and personnel in other areas of the business to gather information on business events and trends.

Question 2.6.90
What is the importance of an organization internally communicating information necessary to support the functioning of internal control (Principle 14)?

Interpretive response: Communication is important to an entity's overall ICFR because it is how an entity internally shares the information necessary to support the functioning of ICFR. A lack of effective internal communication may result in a misunderstanding of individual roles and responsibilities for ICFR and how those roles and responsibilities impact the achievement of the entity's objectives. In addition, a lack of communication between management and those charged with governance may result in those charged with governance not receiving information needed to exercise its oversight responsibility.

Question 2.6.100
What are management's communication responsibilities?

Interpretive response: Management's communication responsibilities include:

- establishing a process to make sure that complete, accurate and appropriate information is made available on a timely basis to control operators;
- enabling inbound communication from external parties to support its system of internal control; and
- establishing expectations of control operators to:
  - be aware of significant internal control matters that may impact other functions, operating units or divisions; and
  - communicate their observations up, down and across the entity.

Significant matters management expects control operators to communicate around the entity include:

- instances of weak or deteriorating internal controls;
- absence of key controls; and
- non-adherence to established controls.

Management's communication about ICFR should result in personnel understanding how their roles, responsibilities and actions relate to the work of others in the entity and how they may affect the achievement of effective ICFR.

Question 2.6.110
What channels are used to internally communicate information related to financial reporting and ICFR?

Interpretive response: An entity may use a variety of different channels to communicate information internally about its objectives, policies and procedures, and control requirements related to financial reporting, as well as information necessary for the effective operation of ICFR. Examples of these channels include:

- departmental vision and mission objective signs posted in high-traffic areas or on the entity's website;
- accounting and finance internal meetings or conferences to discuss internal control matters and accounting policy changes;
- public display of the code of conduct;
- an anonymous hotline where employees can report fraud or ethical matters;
- regular entity-wide emails, newsletters, conference calls, webcasts, focused trainings or meetings about updates on internal control matters;
- senior finance and executive management visits to plants, sales offices, major customers and other locations;

- periodic internal reporting packages that contain key financial and non-financial information; and
- departmental and executive meetings that exchange information about activities and decisions in parts of the business that could affect others.

Practical tip

Ensuring there is communication to the field/employees is important and can include whistleblower hotlines. However, there should also be evidence of employees being made aware of the hotline and a distinct policy in place on how to handle any integrity claims, including how they are communicated to those charged with governance.

Example 2.6.20

Controls that may be in place to address Principle 14

Principle 14: The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

Examples of controls that may be in place to address Principle 14 include:

- Monthly management meetings are held to provide a forum for communication of information affecting financial reporting and related ICFR.
- The annual internal audit plan is reviewed by management and the Audit Committee. Quarterly, progress against the plan and/or changes to the plan are provided to both management and the Audit Committee.
- The Board of Directors establishes a board charter that defines the guidelines for information to be shared with the board of directors, responsibilities for communication, and the method of communication.

Question 2.6.120

What is the importance of an entity communicating with external parties regarding ICFR (Principle 15)?

Interpretive response: With open external communication channels, important information concerning the entity's objectives may be provided to shareholders or other owners, business partners, customers, regulators, financial analysts, government entities and other external parties. Management's communication to external parties sends a message about the importance of internal control in the organization by demonstrating open lines of communication. Communication to external suppliers and customers supports the entity's ability to maintain an appropriate control environment.

Question 2.6.130
How does an entity communicate with external parties?

Interpretive response: An entity can communicate with external parties about matters affecting the functioning of internal control in a variety of different ways. Examples include:

- code of conduct or business relationship agreements with external suppliers;
- promoting to external suppliers and service providers the anonymous hotline to report fraud or ethical matters;
- service agreements with external service providers;
- policies surrounding regulatory compliance and assignment of oversight for such compliance to qualified individuals within the organization; and
- establishment of a Disclosure Committee to review documents to be filed with the SEC or other external parties to enable appropriate disclosure of relevant information.

Example 2.6.30
Controls that may be in place to address Principle 15

Principle 15: The organization communicates with external parties regarding matters affecting the functioning of internal control.

Examples of controls that may be in place to address Principle 15 include:

- the entity has a process to enable communication of information regarding regulatory compliance that affects external reporting objectives;
- earnings and press releases are prepared by management and are reviewed by the CEO before release; and
- the disclosure committee reviews and approves all documents to be filed with the SEC or other external parties.

2.7 Monitoring activities

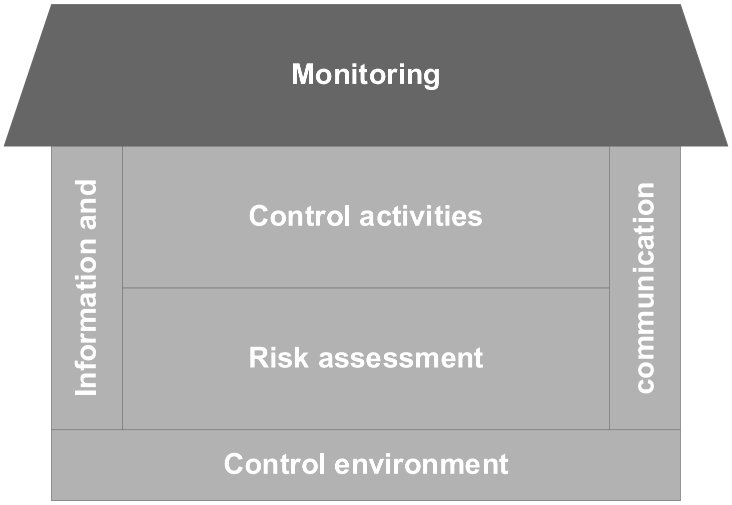
Question 2.7.10
What is the monitoring activities component of ICFR?

Interpretive response: Monitoring activities help ascertain whether each of the ICFR components, including the principles within each component, is present and functioning as intended.

Management's monitoring activities over ICFR involve assessing the effectiveness of internal control performance over time and taking necessary remedial actions. Assessing the effectiveness of internal controls may be performed through ongoing activities, separate evaluations or a combination of the two.

Question 2.7.20
What is the relevance of monitoring activities to ICFR?

Interpretive response: Continuing with the house example, monitoring activities are like the roof of the house. They oversee and protect the other ICFR components. Without effective monitoring, management does not have a basis to rely on their own ICFR.



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 changes to ICFR needed to prevent or detect, on a timely basis, future errors in the financial statements.

The goal of monitoring activities is to determine both that ICFR operated and operated effectively. Monitoring also includes evaluating the severity of identified deficiencies and communicating deficiencies to the appropriate parties.

Question 2.7.30

What are the principles in the COSO Framework related to the monitoring activities component of ICFR?

Interpretive response: The COSO Framework sets out two principles for the monitoring activities component of ICFR. Meeting both principles demonstrates that controls have been designed and are operating effectively to meet the objectives of the monitoring activities component.

Monitoring activities	
Principle 16	The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
Principle 17	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.

Source: COSO Internal Control – Integrated Framework (2013).

Question 2.7.40

What is the importance of an entity performing ongoing and/or separate evaluations of their ICFR (Principle 16)?

Interpretive response: Monitoring activities are selected, developed and performed to ascertain whether each component continues to be present and functioning, or if change is needed. Monitoring activities provide valuable input for management to use when determining whether the system of internal control continues to be relevant and can address new risks.

Question 2.7.50

How does an entity demonstrate that it has met Principle 16?

Principle 16: The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

Interpretive response: Demonstrating that the entity has met Principle 16 requires implementing procedures to determine that:

- a control has been performed; and
- the control has been performed effectively.

Effective performance of a control is relevant when determining which monitoring method to use, and who should perform the monitoring.

An entity's evidence of the operating effectiveness of controls comes from monitoring activities, which include:

- ongoing monitoring (what the COSO Framework calls 'ongoing evaluation');
- direct tests of controls (what the COSO Framework calls 'separate evaluations'); or
- a combination of both.

Question 2.7.60

What are ongoing evaluations?

Interpretive response: Ongoing evaluations are built into the routine operations of the entity and performed in real time. They are often built into management's normal recurring activities (including regular management and supervisory activities) and provide information about the operation of controls.

Ongoing evaluations either monitor business performance or the effective operation of other controls to identify unusual trends that may indicate control deficiencies.

Example 2.7.10

Ongoing evaluations: KPIs

Within the sales process, management monitors several key performance indicators (KPIs) on a daily, weekly and monthly basis. The KPIs include:

- the quantity of products shipped by day and by warehouse location;
- days sales outstanding at the end of each week; and
- analysis of accounts receivable agreed over 120 days.

The KPIs are designed to provide a timely indication of unexpected or anomalous changes or events within the entity's sales process and are added as a process-level monitoring activity to the entity's annual monitoring plan.

In addition, quarterly business reviews are completed and obtained from component locations. These reviews analyze KPIs and certain other financial statement captions compared to budget.

Example 2.7.20
Ongoing evaluations: Control testing status

Management maintains a status listing of the monitoring activities over all controls. This status listing includes:

- the control description;
- the control operator;
- status of testing;
- identified deficiencies; and
- remediation plan and status.

The status listing is reviewed by management on a weekly basis for them to assist in actioning any testing or remediation necessary. It is then presented to those charged with governance on a quarterly basis.

Question 2.7.70
Are monitoring business performance and ongoing monitoring activities the same?

Interpretive response: No. Monitoring business performance and ongoing monitoring activities are not the same, although their purposes may overlap.

Monitoring business performance establishes whether the entity's business performance (or that of its components) is meeting the objectives or expectations set by management or third parties. Such objectives or expectations can be expressed in the form of forecasts, budgets or prior-period normal results that serve as a benchmark for evaluating the current-period actual results.

An example of monitoring trends in business performance is observing KPIs – such as the analysis of accounts receivable aged over 120 days – and following up on unexpected trends. While an unexpected trend in the aging of accounts receivable may not be a result of a breakdown in internal controls, it represents a trigger for management to look more closely at their processes for:

- credit sales, and
- accounts receivable collection.

Although their investigation may identify breakdowns in relevant control activities in one or more of these processes, that is not the intended purpose. Monitoring activities are performed to 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.

Question 2.7.80
What are the benefits of ongoing evaluations?

Interpretive response: There are several benefits associated with ongoing evaluations, particularly:

- routine execution and continuous operation as part of the entity's everyday business processes;
- focus on relationships and inconsistencies that are most important to management and other stakeholders; and
- real-time identification of issues allowing for a timelier response by management.

Question 2.7.90
What are separate evaluations?

Interpretive response: Separate evaluations involve objective management personnel, internal audit and/or external parties (and others) periodically conducting testing to monitor the effectiveness of internal controls.

Question 2.7.100
What parties can perform separate evaluations?

Interpretive response: Various parties can perform separate evaluations as set out in the following table, each with differing degrees of objectivity and independence.

Evaluator	Description
Internal audit	Performed by internal auditors, whether in-house or outsourced, that perform separate evaluations either as part of their regular duties or at the specific request of senior management or those charged with governance.
Objective parties other than internal audit	Performed by other internal or external objective reviewers, such as a compliance team, IT security specialists or consultants. Generally consistent objectivity and competence of internal audit.
Cross-functional personnel	Performed by personnel from different functions or departments that are independent of the process and controls being evaluated.

Evaluator	Description
Self-assessments	Performed by the personnel responsible for operation of the control. Least objective as performed by the control operator themselves.

Question 2.7.110

When might an ongoing evaluation be more appropriate than a separate evaluation and vice versa?

Interpretive response: One type of evaluation may be more appropriate in certain circumstances. The following table lists circumstances that may indicate whether an ongoing or separate evaluation is more appropriate.

Ongoing evaluation	Separate evaluation
Lower risk in the execution of the control or in the related account or disclosure	Higher risk in the execution of the control or in the related account
Less judgment in executing the control	More judgment in executing the control
No history of errors in the related account or disclosure	History of errors in the related account or disclosure
No changes to the process or design of the control	Changes that may affect the way information is processed or the design of the control (e.g. an acquisition, changes in economic conditions)
No expectation from management for external auditors to rely on the work of others relative to the control	An expectation from management for external auditors to rely on the work of others relative to this control

Question 2.7.120

When might an entity increase the extent of its monitoring activities?

Interpretive response: An increase in the extent of monitoring activities may be warranted when:

- management assesses the risk associated with a control as higher;
- there is an increase in the risk of material misstatement of the entity's financial statements related to a particular significant account or disclosure, or the related process; or
- the particular area of the entity's financial reporting process:
  - has been historically prone to errors;
  - is complex;

- is exposed to higher RMMs due to error or fraud; and
- involves a significant degree of judgment.

Question 2.7.130

How might an entity increase the extent of its monitoring activities?

Interpretive response: An entity can increase the extent of its monitoring activities through the following actions, among others:

- using more objective monitoring personnel, which might include:
  - moving away from self-assessments and towards monitoring activities performed by personnel from other functions or departments who are independent of the process and controls being monitored;
  - instituting evaluations performed by internal audit or other objective evaluators;
- changing or extending the period of time covered by the monitoring activities; or
- supplementing or replacing ongoing evaluations with periodic direct testing of the underlying controls to:
  - corroborate evidence from ongoing monitoring activities; and
  - evaluate how effectively the underlying controls operate and whether they continue to adequately address financial reporting risks.

Question 2.7.140

Can an entity's monitoring activities be accomplished entirely through separate evaluations?

Interpretive response: Yes. An entity can accomplish its monitoring activities entirely through separate evaluations. However, an entity can identify internal control issues more quickly through ongoing evaluations.

Management should consider the rate of change in the business and the significance of risks so that it determines the appropriate mix of both ongoing and/or separate evaluations.

Question 2.7.150

Should an entity have monitoring activities over processes and controls performed by third-party service providers?

Interpretive response: Yes. As a general rule, although management may outsource a process to a third-party service provider, they may not outsource their responsibility for the results of the service provider's work.

When the entity uses third-party service providers, management still monitors whether controls performed by those service providers have been appropriately designed and implemented and are operating effectively.

Such monitoring may be accomplished by performing one or both of the following:

- Separate evaluations, such as:
  - reviewing a SOC 1® – Type II report (if such a report is available for the service provider); or
  - directly testing controls in place at the service organization.
- Ongoing evaluations, such as reviewing output provided by the service organization for outliers that may indicate its controls have not been appropriately designed or are not operating effectively.

Chapter 8 provides detailed discussion about the involvement of service organizations in ICFR.

Question 2.7.160

How are monitoring activities different from process control activities?

Interpretive response: As it relates to ICFR, monitoring controls, consistent with most entity-level controls, provide a 'could' level of assurance (see Question 2.3.40), whereas process control activities provide a 'would' level of assurance (see Question 2.3.30). Additionally, monitoring activities have a different purpose from that of process control activities, as detailed in the table below:

Purpose of monitoring activities	Purpose of process control activities
• Evaluate the effectiveness of control activities and other components of ICFR and identify deficiencies timely. • Monitor operations to identify unusual trends or anomalies that may warrant further investigation.	• Respond directly to mitigate a specific risk within a process relevant to financial reporting.

Purpose of monitoring activities	Purpose of process control activities
• Analyze root cause of deficiencies. • Design and implement effective remediation plan.	
• 'Could' identify errors themselves, but that is not the primary purpose of their design and operation.	• Designed with sufficient precision such that the control, if designed and operating effectively, 'would' prevent, or detect and correct, errors in financial reporting.

Example 2.7.30
Financial statement review

A review of the financial statements performed as a monitoring control may identify an unusual change in the entity's balance of fixed assets between periods that, on further investigation, is attributable to a deficiency in the design of the entity's process control activity to address the accuracy of the accounting for fixed asset additions. Although the entity-level control in this instance detected a misstatement, it alone is not operating at an appropriate level of precision to replace the need for a process control activity directly responsive to the risk that additions are accounted for inaccurately. Said another way, the financial statement review 'could' detect an error but does not operate at a level of precision ('would' level of assurance) to mitigate the risk identified to an appropriately low level.

Question 2.7.170
What is a flux analysis?

Interpretive response: A flux analysis is a monitoring activity whereby management understands and investigates changes in account balances within the balance sheet and income statement across two periods.

A flux analysis may compare:

- actual account balances for the current period to actual account balances from the prior period (e.g. actual results from the current month to the previous month); or
- account balances for the current period to a budget or forecast for the current period (e.g. actual results from the current month to the budget for the month).

Question 2.7.180
Can a flux analysis be a process control activity?

Interpretive response: Typically, no. A flux analysis is best classified as a monitoring activity as it usually has a different purpose than a process control activity and is not designed at the level of precision necessary to mitigate risks identified at the process level.

If the flux analysis directly addresses a specific risk at the process level and is designed at a level of precision that would prevent or detect a material misstatement, it could function as a process control activity. However, this is rare as it is difficult to design a flux analysis to achieve the precision required in a process control activity. Flux analyses are typically performed over amounts at a higher level of aggregation, which may be at an appropriate level of precision for a monitoring control (e.g. require investigation of all changes over a low dollar threshold). But it is often impractical to *perform and document* the control at the level of detail required to effectively evidence all the activity driving the fluctuation due to the existence of offsetting activity between and among accounts underlying the amount at the aggregate level. There are also other items to consider including, but not limited to:

- the reliability of the information used, specifically when budgets or forecasts are used;
- the risk that there should be fluctuation and there isn't; and
- the risk that outliers identified are 'explained away' and errors are not properly identified and resolved.

As such, care should be exercised when asserting that a flux analysis is a process control activity.

Question 2.7.190
When separate evaluations are used as part of monitoring procedures, is testing of controls performed?

Interpretive response: Yes. Management, usually with the assistance of internal audit, performs testing of their internal controls, including entity-level controls, process control activities and GITCs.

Question 2.7.200
How are entity-level controls evaluated and tested and how does that differ from evaluating and testing control activities?

Background: Entity-level controls include standards, processes, structures, communications and other activities the entity undertakes to help management carry out ICFR across the organization. By contrast, a process control activity directly addresses process risk points arising from business processes that account for the entity's transactions. Given their nature, entity-level controls are evaluated and tested differently from control activities.

Interpretive response: Testing entity-level controls means testing the 'set of standards, processes and structures' rather than specific control activities. Also, because of the indirect nature of entity-level controls, an assessment of the effectiveness of the controls often requires qualitative considerations.

When entity-level controls are policies, procedures, processes and structures, and there are no discrete instances of procedures being performed (similar to control activities), the procedures performed to test the effectiveness might include:

- inquiring of management and those charged with governance regarding the policies, procedures, processes and structures in place at the entity;
- inspecting documentation evidencing that the policies, procedures, processes and structures exist; and
- observing the policies, procedures and processes being performed by management or those charged with governance.

Inquiry alone is not sufficient to provide evidence that the controls are present and functioning.

Certain entity-level controls may incorporate discrete instances of procedures being performed, similar to control activities, such as when employees are required to re-affirm compliance with the code of conduct on an annual basis.

For entity-level controls with discrete instances of procedures being performed, the effectiveness of these procedures is tested in a manner similar to testing control activities. This includes ensuring there is a complete population from which to select a sample to test and testing discrete instances of the operation of the control. The number of items to test would be based on the population and the risk associated with the control.

Practical tip

For entity-level controls, maintaining proper and complete evidence is important, especially for testing purposes. For an entity-level control that operates on a recurring basis, the ability to establish a complete population is important, as is maintaining evidence of the control's operation. For example, for an entity-level control where all employees are required to sign a code of conduct each year, a complete listing of all employees throughout the year needs to be available, as well as a documented understanding of how that listing is determined to be complete. In addition, the signed copies of the code of conduct for all employees needs to be maintained and available.

Example 2.7.40
Management meeting to assess risks

Consider entity-level controls related to risk assessment whereby key members of the finance and accounting department meet to identify, analyze and assess the significance of financial reporting risks across the entity and how the entity will manage those risks. When testing this control, evidence is obtained to conclude whether the entity has a process for identifying, assessing and making plans to address financial reporting risks. This could be accomplished through inquiries of those who attended the meeting combined with review of:

- the meeting invites to establish the appropriate parties were included in the meeting;
- the materials provided to the meeting participants to establish the purpose and content of the meeting; and
- the minutes of the meeting to establish the discussions held and the conclusions reached during the meeting.

The combination of these testing methods would support that the entity-level control was in place and operating effectively.

Question 2.7.210
How are process control activities evaluated and tested as part of monitoring activities?

Interpretive response: See section 5.18.

Question 2.7.220
How are general IT controls evaluated and tested as part of monitoring activities?

Interpretive response: See section 7.4.

Question 2.7.230
What are examples of entity- (or group-) level monitoring activities implemented in a multi-component or multi-location setting?

Interpretive response: Most entities with multiple components or locations perform various types of reviews or other evaluations at the consolidated entity-level, which are targeted at the financial, operating, or control performance of the individual components or locations. Examples of such consolidated entity-level reviews may include:

- regular meetings between group and location or component management to discuss business developments and to review performance;
- monitoring the locations' or components' operations and their financial results, including regular reporting routines, against budgets or forecasts, and taking appropriate action;
- monitoring the timeliness and assessment of the accuracy and completeness of financial information received from locations or components; and
- monitoring controls, including activities of the internal audit function and self-assessment programs.

Question 2.7.240

Can entity-level monitoring activities be relied on to eliminate the need to rely on or evaluate controls at the entity's individual locations or components?

Interpretive response: Typically, no. These consolidated entity-level reviews often do not represent control activities, but rather are designed as monitoring activities. Their objective is to identify unusual trends or anomalies in business or operating performance that may indicate possible breakdowns in process control activities at the location or component level. The reviews are not designed to operate at a level of precision that would, by themselves, sufficiently address the risk of material misstatements of the group financial statements. As monitoring activities, these consolidated entity-level reviews alone will not be sufficient to address the risk of material misstatement at the location or component level.

To eliminate the need for reliance on and evaluation of controls at a specific location or component of the entity, the reviews performed at the consolidated entity level need to represent control activities. For this to be the case, the reviews at the consolidated entity level need to be designed and operated with an appropriate 'would' level of precision. The level of precision needed provides confidence to both management and external auditors that the reviews would prevent or detect, on a timely basis, a misstatement that could arise at the location or component and be material to the entity's consolidated financial statements. The materiality of the individual misstatement and the aggregate of misstatements are both considered for purposes of assessing materiality. It can be difficult to perform the control at a precise enough level due to the aggregation level used, as well as the ability to identify and resolve outliers and not just 'explain them away.'

When the consolidated entity-level reviews are not or cannot be converted from monitoring activities to process control activities, management should design and implement relevant process control activities at the individual locations or components of the entity. For this purpose, management includes the locations or components that either individually, or when aggregated with others, include a more-than-remote risk of material misstatement of the group financial statements (see chapter 3 for discussion of scoping the ICFR risk assessment in a multi-location or group entity situation). Management and external auditors should then evaluate the design and operating effectiveness of the controls in place.

While the consolidated entity-level reviews that are designed as monitoring activities typically are not sufficient to eliminate the need for reliance on and testing of controls at individual components or locations of the entity, such monitoring activities would address Principle 16. In addition, such monitoring controls, if appropriately designed and operating effectively, may allow management and external auditors to reduce (but not eliminate) the testing of other controls, including those controls that operate at individual components or locations. In the case of entities with multiple homogenous locations, effective monitoring controls may also allow management and auditors to reduce the number of locations at which testing of process control activities needs to be performed.

Question 2.7.250

To what extent can external auditors rely on the entity's monitoring activities?

Interpretive response: It depends. The degree of reliance on monitoring activities by external auditors in their audit of an entity's ICFR is governed by the applicable auditing standards. Paragraph 39 of PCAOB Auditing Standard (AS) 2201 states that in an audit of ICFR, "the auditor should test those controls that are important to the auditor's conclusion about whether the company's controls sufficiently address the assessed risk of misstatement to each relevant assertion."

There is a direct focus in the ICFR audit on control activities that mitigate the risk of misstatement to specific assertions over significant accounts and disclosures. Because of this, it will be rare that an external auditor will be able to obtain sufficient evidence of the design and operating effectiveness of these control activities by testing only the monitoring activities operating over the control activities. However, as stated in paragraph 40 of PCAOB AS 2201, "there might be more than one control that addresses the assessed risk of misstatement to a particular relevant assertion." In some situations, a monitoring control may represent an important element of a larger suite of controls designed to address an assertion-level risk and, in such situations, the monitoring activity would need to be evaluated and documented together with the related control activities.

External auditors' ability to rely on management's monitoring activities is particularly limited when it comes to ongoing evaluations (see Question 2.7.60). This is because ongoing evaluations are rarely performed by independent objective evaluators and do not directly test the underlying controls, but rather look for indicators of their deficiency.

Considering the characteristics of some of these monitoring activities and the requirements of the auditing standards, external auditors' reliance on the work of others is usually limited to the direct testing performed by internal auditors over low risk, routine controls. When an external auditor relies on the work of others, they will have to sufficiently reperform the work to determine that it can, in fact, be relied upon.

Generally, whenever management does not monitor the controls by direct testing, auditors will not be able to rely on management's work.

Question 2.7.260

What documentation standard is management held to with respect to its monitoring activities?

Interpretive response: Management must keep documented evidence of the effectiveness of controls, including the monitoring activities performed.

Regardless of whether the entity has chosen to monitor through ongoing or separate evaluations, the documentation of monitoring activities should be sufficient to:

- enable a prudent official to understand the nature, timing and extent of the monitoring activities performed; and
- provide sufficient information to be able to conclude on the appropriateness of design and operating effectiveness of the monitoring activities.

Documentation of monitoring control activities will likely be more robust than documentation of monitoring the other ICFR components. A reasonable level of documentation is always necessary to meet the 'prudent official' principle of documentation and for management to assert that each of the ICFR components and related principles are present and functioning.

Appropriate documentation of management's monitoring activities is also critical to the external auditors' ability to test these activities and obtain evidence of the entity's compliance with the requirements of Principle 8 (see Question 2.5.120).

Question 2.7.270

What is the importance of an entity maintaining, tracking and communicating deficiencies in ICFR to those parties responsible for taking corrective action and those charged with governance (Principle 17)?

Interpretive response: Communication of deficiencies in ICFR to the appropriate parties allows for the appropriate levels to oversee the effectiveness and timeliness of remediation.

In monitoring that the components of ICFR are present and functioning, it is not uncommon for an entity to identify shortcomings in the design and operation of internal controls for a variety of reasons. When deficiencies are identified, it is important that each deficiency is tracked and communicated to the appropriate parties so that remedial actions may be performed and overseen to support the effective design and operation of ICFR on a go-forward basis.

Question 2.7.280

How does an entity maintain, track and communicate deficiencies in ICFR to executive management and the Audit Committee (Principle 17)?

Interpretive response: An entity typically has a process in place to maintain, track, and communicate deficiencies in ICFR to executive management and the Audit Committee that is part of assessing the results of its monitoring activities. This process will vary depending on the entity's circumstances; however, it will probably contain a variation of the following steps.

Step 1	Determine whether a deficiency in ICFR exists
Step 2	Perform a root cause analysis of the deficiency
Step 3	Determine whether the deficiency indicates other deficiencies
Step 4	Evaluate the severity of the deficiency individually
Step 5	Evaluate the effect of compensating controls, if applicable
Step 6	Evaluate the severity of similar deficiencies in the aggregate

The results of the entity's process of identifying and evaluating a control deficiency assists in the development and initiation of remedial actions.

Chapter 9 includes further discussion on identifying and evaluating control deficiencies.

Question 2.7.290

What is communicated when a control deficiency is identified and who is it communicated to?

Interpretive response: Deficiencies are communicated to parties responsible for taking corrective action. All control deficiencies are also communicated to the external auditor and to at least one level of management above the control operator. Deficiencies may be reported to senior management and those charged with governance, depending on the reporting criteria as established by regulators, standard-setting bodies, or the entity, as appropriate.

Management of an SEC registrant also discloses material changes to ICFR in Item 4 of their SEC filings.

Practical tip

External auditors are required to report all significant deficiencies and material weaknesses to those charged with governance; therefore, management generally will, at a minimum, report these matters as well.

Question 2.7.300

How does an entity monitor whether corrective actions to remediate control deficiencies take place?

Interpretive response: Once an entity has identified and assessed a control deficiency, it puts in place processes to:

- determine what corrective actions are necessary to remediate the control deficiency; and
- monitor whether the corrective actions have taken place in a timely manner.

Typically, the individuals responsible for monitoring whether corrective actions have taken place in a timely manner are different from the individuals responsible for determining and implementing the corrective actions.

Question 2.7.310

How does an entity monitor if corrective actions to remediate a control deficiency take place in a timely manner?

Interpretive response: The status of corrective actions – i.e. remediation status – is often discussed with senior management. This may occur as part of a periodic ICFR-focused steering committee meeting. Management also discusses the remediation status of significant deficiencies and material weaknesses with the audit committee as part of periodic audit committee meetings.

When corrective actions have not taken place in a timely manner, the entity may put additional monitoring activities in place until the corrective actions have been implemented.

Further, Principle 5 requires the entity to hold individuals accountable for their internal control responsibilities, which includes responsibilities related to corrective actions necessary to remediate control deficiencies (see Question 2.4.150).

Example 2.7.50
Communication of deficiencies and corrective actions

Internal Audit maintains a control deficiency report that is updated with any new deficiencies identified or when remediation activities are tested and completed.

Internal Audit has biweekly meetings with management where control deficiencies are communicated to management and remediation plans are discussed. The process or control owner develops a remediation plan including a timeline for remediation and subsequently remits to the Internal Audit department for review and approval.

Internal Audit performs a follow up process to verify remediation has occurred in accordance with the approved timeline. Testing is performed to evaluate whether the control is operating effectively after remediation.

Internal Audit presents the control deficiency status report to the Audit Committee on a quarterly basis.

Key takeaways

- Assessment of the control environment component of ICFR should be performed across the entity and at all levels, as well as third-party service providers and other external business partners.
- Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives and is performed at least annually by management.
- Both the SEC and the COSO Framework require the assessment of fraud risk.
- Risk assessment considers changes that could have an impact on ICFR. Many material weaknesses in ICFR are rooted in circumstances where changes occurred but the ICFR implications were not identified or thoroughly considered.
- Management's risk assessment should be documented on a timely basis and be comprehensive in nature.
- Entities should establish processes for identifying information needs across the entity and communicating the necessary information appropriately and on a timely basis. Failure to communicate the relevant information to the appropriate person(s) may result in a material weakness if it effects the financial statements.
- Effective monitoring allows management to determine whether controls within each of the five components of ICFR are operating as intended and to determine what needs to be changed to prevent future errors. In obtaining objective evidence to support their monitoring, management should determine the appropriate mix of both ongoing and/or separate evaluations.

3. Risk assessment

Detailed contents

3.4 Scoping of accounts and disclosures

Questions

3.4.10 Is risk assessment performed at the assertion level?

3.4.20 What is a significant account or disclosure?

3.4.30 How are significant accounts and disclosures aggregated or disaggregated?

3.4.40 What is risk tolerance and how is it considered when defining significant accounts?

3.4.50 What actions should management consider taking to fulfill their ICFR-related responsibilities related to non-GAAP financial measures?

Examples

3.4.10 Considering qualitative factors when identifying significant accounts

3.4.20 Disaggregation and aggregation in defining significant accounts

3.5 Scoping of components

Questions

3.5.10 Which of the components of the group are deemed in scope for purposes of management's ICFR assessment?

3.5.20 Can an entity-level analytical review control be sufficient to mitigate risks in an individual component or aggregated components of an entity?

3.5.30 Are newly acquired businesses subject to management's assessment of ICFR?

3.5.40 Are disposal groups included in management's scoping of components?

3.5.50 What should the entity consider for components that are financially insignificant?

3.5.60 Is aggregation risk considered when determining whether a component is in scope (or out of scope)?

3.5.70 What are factors to be considered in determining component materiality?

3.5.80 Should management document the scoping of its accounts, processes and components performed as part of risk assessment?

3.6 Identifying and assessing fraud risks

Questions

3.6.10 Are all entities required to consider fraud risks in their risk assessment?

3.6.20 How is a fraud risk assessment performed?

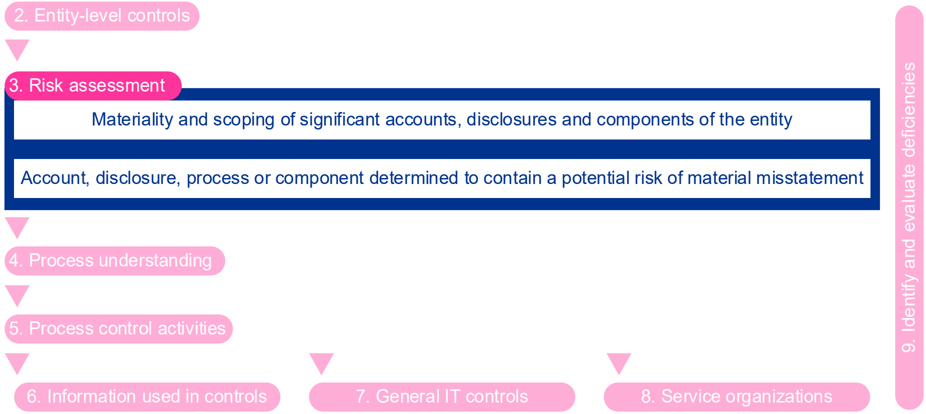
Examples

Questions

Examples

3.1 Management's ICFR journey

Management's ICFR journey for each financial reporting cycle requires the performance of risk assessment – a dynamic and iterative process for identifying and assessing risks to the achievement of objectives.


2. Entity-level controls
3. Risk assessment
Materiality and scoping of significant accounts, disclosures and components of the entity
Account, disclosure, process or component determined to contain a potential risk of material misstatement
4. Process understanding
5. Process control activities
6. Information used in controls
7. General IT controls
8. Service organizations
9. Identify and evaluate deficiencies

While an entity's risk assessment process starts early in the financial reporting cycle, it requires a reassessment of initial conclusions based on evidence obtained throughout the financial reporting cycle. As stated by the Chief Accountant of the Securities and Exchange Commission, when business risks change, a robust, iterative risk assessment process and strong entity- and process-level controls are essential to transparent and high-quality financial reporting[1].

This chapter provides an overall view on the process management uses to identify and assess risks, as well as specific activities involved when executing an effective risk assessment.

Identifying and assessing risks (see section 3.2)

Identifying the relevant risks to financial reporting is an essential component of ICFR because failure to understand the likely sources of misstatements may lead to ineffectively designed control activities, which in turn increases the possibility of a material misstatement in the financial statements.

Management performs the entity's risk assessment at various levels within the entity by following a top-down approach starting at the entity level and moving down to the process level.

Consideration of materiality (see section 3.3)

Materiality involves both quantitative and qualitative considerations. Separate materiality analyses could be needed at the consolidated level and component level.

[1] Paul Munter, SEC Chief Accountant, The Importance of a Comprehensive Risk Assessment by Auditors and Management, August 2023.

Scoping of accounts and disclosures (see section 3.4)

Management identifies significant accounts and disclosures and links them to the appropriate financial statement assertions (e.g. completeness, existence, accuracy). This is necessary given management's overall objective is to produce reliable financial reporting in accordance with the relevant GAAP.

A significant account or disclosure is an account or disclosure where there is a reasonable possibility that it could contain a misstatement that, individually or when aggregated, has a material effect on the financial statements. The determination of significant accounts is important because any accounts determined to be significant require an ICFR response.

Scoping of components (see section 3.5)

Management determines which of the entity's components (e.g. subsidiaries, divisions, operating units) present a risk that the financial statements contain a material misstatement. A necessary part of this exercise is determining component materiality, which will be less than consolidated materiality – how much less depends on the facts and circumstances.

Identifying and assessing fraud risks (see section 3.6)

Management must assess the potential for fraud in evaluating risks to the achievement of its objectives. This assessment should be comprehensive, cover various levels within the entity and involve appropriate members of management and employees. Generally, the identified fraud risks should be linked to a specific financial statement assertion or assertions.

Consideration of changes to ICFR (see section 3.7)

Management's risk assessment must identify changes with a significant effect on financial reporting and assess the risks resulting from those changes. Identified changes are typically analyzed down to the process level.

Documentation of the risk assessment process often involves the creation and maintenance of a risk and control matrix, which includes the account, account balance, the risk factors considered, the significance of the risk to the accounts and assertions, as well as linking risks to the internal controls designed to address them.

Abbreviations

We use the following abbreviations in this chapter.

AICPA	American Institute of Certified Public Accountants
COSO	Committee of Sponsoring Organizations of the Treadway Commission
FASB	Financial Accounting Standards Board
GAAP	Generally accepted accounting principles
ICFR	Internal control over financial reporting
PRP	Process risk point

RM	Risk of misstatement
RMM	Risk of material misstatement
SEC	Securities and Exchange Commission

3.2 Identifying and assessing risks

Question 3.2.10
Why is risk assessment necessary?

Interpretive response: Identifying the relevant risks to financial reporting is an essential component of ICFR because failure to understand the likely sources of misstatements may lead to ineffectively designed control activities, which in turn increases the possibility of a material misstatement in the financial statements.

The importance of risk assessment has also been emphasized by the SEC staff who have stated that[2] to accomplish the objective of effective ICFR, management must identify the risks to reliable financial reporting before identifying controls and monitoring them for effectiveness.

Question 3.2.20
At what level is an entity's risk assessment performed?

Interpretive response: The COSO Framework makes it clear that management should perform the entity's risk assessment at various levels within the entity by following a top-down approach that starts at the entity level and moves down to the process level.

Question 3.2.30
Are there certain activities or matters that should be considered as part of the entity's risk assessment process?

Interpretive response: Activities or matters that should be considered as part of an entity's risk assessment process include:

- safeguarding of assets (see Example 3.2.10);
- authorization of receipts and expenditures (see Example 3.2.10);

[2] 17 CFR Part 241 (Release No. 33-8810), Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934, p. 9.

- an entity's ability to continue as a going concern (see Question 3.2.40); and
- fraud (see section 3.6).

It is important that an entity's risk assessment process is comprehensive and results in a complete population of risks affecting ICFR. Exclusion of the above items from an entity's risk assessment could result in ineffective ICFR, as noted in the examples below, if risks are not properly identified and the related controls to address those risks are not in place and operating effectively.

Example 3.2.10

Risks related to safeguarding of assets and authorization of receipts and expenditures

Scenario A: Unauthorized change to vendor bank account number

Facts: The Accounts Payable (A/P) Manager receives a phone call from an individual who introduces himself as Account Manager at Supplier X. The caller requests that Entity A change the number of the bank account to which the payments due to Supplier X should be remitted on a going-forward basis. The A/P Manager updates the payment information, and Entity A begins processing payments to the bank account on file.

A month later, a representative of Supplier X contacts Entity A to complain about missing payments for several recent deliveries. Entity A fell victim to a fraud scheme perpetrated by an unidentified third party and lost several million dollars.

Analysis: In this scenario, Entity A failed to safeguard its assets in violation of the SEC's definition of effective internal control that requires each issuer to maintain policies and procedures that provide reasonable assurance regarding prevention or timely detection of unauthorized use or disposition of the issuer's assets.

In addition, Entity A also did not comply with Principle 15 (see Question 2.6.120) in the COSO Framework that requires entities to select appropriate methods of communication with external parties. In this case, Entity A either did not have a policy in place that required an 'in writing' submission of updated payment information by an authorized representative of a vendor or failed to effectively operate relevant controls under such policy. Entity A also did not have a process in place to verify the validity of the updated payment information.

These failures in controls fall into the scope of management's ICFR assessment under the rules of the SEC, and the control deficiencies, as described above, would likely represent a material weakness in Entity A's ICFR. However, a material weakness may not exist if Entity A can demonstrate the existence of effective compensating controls that would have prevented, on a timely basis, the stolen amount from becoming material to Entity A's financial statements.

Scenario B: Unauthorized wire transfer

Facts: At the end of a busy day, the head of Entity B's A/P Department (the A/P Manager) receives an urgent e-mail message directing her to make an immediate wire transfer in the amount of $50 million to a bank account identified in the e-mail message as an account belonging to an investment advisor assisting Entity B in a confidential business acquisition. The e-mail address bears the name of Entity B's CFO.

The message also urges the A/P Manager to keep the wire transfer confidential given the nature of the underlying transaction. It also explains that the CFO is not able to execute the wire transfer himself as he is currently boarding a plane heading to a meeting with the investment advisor. The A/P Manager executes the wire transfer as instructed.

The next day, the Manager follows up with the CFO to obtain written approval for the wire transfer and is shocked to learn that the e-mail communication with the party presumed to be the CFO was fictitious. The entity fell victim to a fraud scheme perpetrated by an unknown third party.

Analysis: Entity B failed to exercise appropriate controls over the authorization of its cash disbursements. It also failed to safeguard its cash in violation of the SEC's definition of effective internal control.

In addition, Entity B did not comply with Principle 14 (see Question 2.6.90) in the COSO Framework that requires entities to select appropriate methods for internal communication. In this case, Entity B either did not have a policy in place that required appropriate supporting documentation for a significant cash transaction or failed to effectively operate relevant controls under such a policy.

Further, the wire transfer was likely processed in violation of Principle 3 (see Question 2.4.130) in the COSO Framework that requires entities to segregate incompatible duties and institute requisite checks and balances from the highest to the lowest levels of the organization. The A/P Manager should not have been able to process such a significant wire transfer without appropriate segregated approval and authorization.

These failures in controls fall within the scope of management's ICFR assessment under the rules of the SEC, and the control deficiencies, as described above, would likely represent a material weakness in Entity B's ICFR. However, a material weakness may not exist if Entity B can demonstrate the existence of effective compensating controls that would have prevented, on a timely basis, the stolen cash amount from becoming material to Entity B's financial statements.

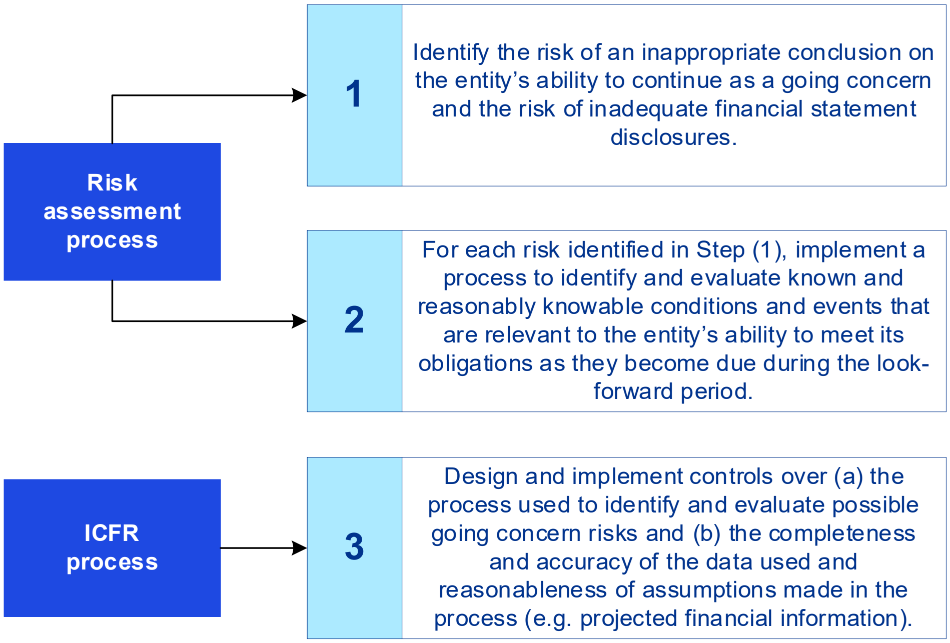
Overall observations

It would be unreasonable to expect management to be able to design, implement and operate controls that would protect an entity from every potential fraud scheme against the entity by internal or external parties. However, an entity should have processes and controls in place that would reduce the risk of a material misstatement in its financial statements due to fraud to a remote level. Such risk should be considered in the specific circumstances of the entity following evaluation of the relevant fraud risk factors.

Question 3.2.40

How does management perform risk assessment relative to an entity’s ability to continue as a going concern?

Interpretive response: Management performing the following steps during risk assessment can adequately address the risk associated with applying Subtopic 205-40 (going concern) of the *FASB Accounting Standards Codification*®.



1 Identify the risk of an inappropriate conclusion on the entity’s ability to continue as a going concern and the risk of inadequate financial statement disclosures.

2 For each risk identified in Step (1), implement a process to identify and evaluate known and reasonably knowable conditions and events that are relevant to the entity’s ability to meet its obligations as they become due during the look-forward period.

3 Design and implement controls over (a) the process used to identify and evaluate possible going concern risks and (b) the completeness and accuracy of the data used and reasonableness of assumptions made in the process (e.g. projected financial information).

Management’s assessment of going concern typically includes an analysis of the entity’s current and forecasted financial condition and liquidity, as well as the forecasted effect of management’s plans to mitigate conditions and events that give rise to a going concern uncertainty, if any. Depending on facts and circumstances, management’s assessment of going concern may lead to the determination of an RMM that would require an appropriate ICFR response.

The going concern assessment in Subtopic 205-40 requires management to assess, as of the date of the issuance of the financial statements, an entity’s ability to continue as a going concern and provide related disclosures. There may be events that occur during the year, or even subsequent to year-end but before the financial statements are issued, that may require further consideration on whether there are conditions and events that raise ‘substantial doubt’ about the entity’s ability to continue as a going concern, These events and circumstances could be specific to the entity, or could be a broader regulatory, economic, or industry matter that requires careful consideration of rapidly changing circumstances. The risk assessment related to going concern should extend through the issuance of the financial statements and the entity’s controls should be designed to identify relevant events and circumstances that could impact the entity’s ability to continue as a going concern.

Question 5.15.10 provides further discussion of controls related to going concern.

Question 3.2.50
What are the key activities involved in entity-level and process-level risk assessments?

This table summarizes the key activities involved in an entity's entity-level and process-level risk assessments.

Entity-level risk assessment	Process-level risk assessment
Performed at the level of the consolidated entity and its components.	Performed at the lowest level of an entity's risk assessment process.
• Determine materiality • Identify components with quantitative or qualitative significance • Identify significant accounts and disclosures • Consider fraud risks • Enable the entity to identify a comprehensive population of risks to the achievement of its financial reporting objectives	• Understand the flow of transactions within a business process from initiation to reporting • Translate the RMs into significant accounts and assertions • Identify the PRPs and determine whether the PRPs result in an RMM • Identify the controls implemented to address the PRPs and related RMMs

Process-level risk assessment is covered in more detail in chapter 4.

Question 3.2.60
Can ERM suffice for entity-level risk assessment?

Interpretive response: No. However, a robust enterprise risk management (ERM) or similar analysis performed by the entity may provide a good starting point to performing a comprehensive risk assessment under the COSO Framework.

Specifically, entity-level risk assessment requires incremental determinations about whether:

- any of the identified risks in the ERM analysis have a potential ICFR implication; or
- there are specific ICFR risks at the entity level that were not contemplated in the broader ERM analysis.

Question 3.2.70

Are IT systems included in management's risk assessment?

Interpretive response: Yes. IT systems support informed decision making and the functioning of ICFR by processing relevant, timely and quality information from internal and external sources. IT systems are pervasive to the entity's overall ICFR. As such, they need to be covered by management's risk assessment.

In addition, changes to IT systems (e.g. new systems, upgrades to an existing system) are examples of entity-wide events that could have a related financial reporting risk.

Chapter 7 provides more information about ICFR considerations related to IT systems.

Question 3.2.80

How does management execute an entity-level risk assessment?

Interpretive response: Management may perform the following steps as part of their entity-level risk assessment.

Step 1	Management uses the concept of materiality to determine what amounts it deems to be material to an end-user of its financial statements. See section 3.3.
Step 2	Management uses materiality and other qualitative factors to determine which accounts and processes contain a potential risk of material misstatement. See section 3.4.
Step 3	Management considers if the entity contains components and if the components contain a potential RMM either for all or some specific accounts and processes identified in Step 2. See section 3.5.

Question 3.2.90

How is the significance of potential risks evaluated?

Interpretive response: The significance of identified risks to reliable financial reporting can be evaluated in many ways. The most frequently used criteria to assess the significance of financial reporting risks are:

- the likelihood of a risk occurring;
- the pace of potential change; and
- the potential magnitude of the identified risk's effect on the entity's financial statements.

Question 3.2.100
When a potential RMM is identified, what is management's response?

Interpretive response: Once identified and assessed as to significance, risks to the achievement of the entity's financial reporting objectives require an appropriate ICFR response. Not all ICFR responses are required to be fashioned with the same level of response – a risk of fraudulent revenue recognition merits a more robust response than a risk of a balance sheet classification error. But the process to respond to each identified risk is similar:

- The risks should be linked to the relevant assertions over significant accounts and disclosures (see section 3.4 for a discussion of significant accounts).

- The accounting literature governing the significant accounts should be understood.

- The process for the transaction or estimate that drives the accounting should be understood from initiation to reporting, and PRPs should be identified (see chapter 4).

- The appropriate controls to mitigate the risks should be designed, implemented, operated and monitored (see chapter 5).

Question 3.2.110
When does an entity perform and document its risk assessment process?

Interpretive response: An effective risk assessment process is iterative in nature. The four principles within the risk assessment component of the COSO Framework (see section 2.5) are not always considered sequentially because there is considerable overlap among the principles. Further, as an entity performs and monitors controls, management may identify items requiring reassessment of earlier risk determinations.

Much of the risk assessment process takes place in meetings and discussions with senior management and those charged with governance. Timely documentation of these and other risk assessment activities undertaken by the entity and their results helps demonstrate an effective ICFR risk assessment process.

Practical tip

Related to documentation of management's risk assessment process, a better practice is the creation and maintenance of a risk and control matrix, which includes the account, account balance, the risk factors considered, the significance of the risk to the accounts and assertions, as well as linking the risks to the controls designed to address them. The matrix also includes evidence of proper review and modification when new risks are identified. Documentation of this review likely includes more than just evidence of a meeting or its minutes.

Question 3.2.120

Who should perform and review the risk assessment?

Interpretive response: The risk assessment should be conducted by appropriate levels of management to properly consider the sources and likelihood of potential misstatements in the entity's financial statements. Management involved should have sufficient knowledge and understanding of the entity's business, its organization, operations, and processes. This may include senior management and representatives from the entity's finance and accounting departments, operations, legal and compliance, human resources, and other functional areas.

Findings and conclusions from the risk assessment process should be presented to and reviewed by the audit committee or those charged with governance. Doing so assists these groups in fulfilling their oversight responsibilities regarding the entity's development and performance of ICFR under Principle 2 of the COSO Framework (see Question 2.4.110).

Example 3.2.20

Management's risk assessment process and audit committee review

Entity A is a global manufacturer of farm equipment. Its Financial Planning and Analysis (FP&A) department is responsible for preparing the entity's annual financial and operating plan. In fulfilling these responsibilities, they carry out an annual planning and risk assessment process, which involves FP&A personnel meeting with senior management and representatives of the various functions of the entity and all its components that are quantitatively or qualitative significant to ICFR. They review business plans and conduct a comprehensive analysis of risks to the achievement of established operating and financial goals.

Throughout the year, FP&A personnel monitor a number of internal and external factors that may indicate a need for revisions to the entity's plans and forecasts.

In conjunction with the annual planning and risk assessment process conducted by FP&A, representatives of Entity A's Internal Audit and Finance Management departments meet with FP&A personnel. The meeting enables the FP&A process to give appropriate consideration to the risks to reliable financial reporting in accordance with US GAAP and SEC rules and regulations. The Internal Audit and Finance Management representatives also join FP&A personnel in various planning and risk assessment activities (meetings, workshops, brainstorming sessions, etc.), as considered necessary. Their participation in these activities enables personnel with sufficient understanding of the entity's financial reporting objectives to be appropriately represented in the FP&A process.

All risks identified in connection with the annual planning and risk assessment process led by FP&A personnel are summarized in a spreadsheet and analyzed for potential effects on the financial reporting process. Risks identified as relevant to financial reporting are then separately analyzed to determine if they rise to the level of an RMM. This analysis is performed by Internal Audit and Finance Management representatives, including the entity's CFO and Controller. In addition, RMMs are linked to the affected significant accounts and disclosures and the related business processes using a risk and control matrix.

Entity A's CFO or Controller presents a summary of the identified RMMs to the audit committee on an annual basis in connection with the committee's review and approval of Internal Audit's annual testing plan. They also provide an overview of the risk assessment process undertaken by management. In assessing the sufficiency of the process, Audit committee members consider:

- the reasonableness of the summarized RMMs based on their understanding of Entity A and its financial reporting process; and
- the appropriateness of management's planned response to those risks, including through Internal Audit's annual testing plan.

3.3 Consideration of materiality

Question 3.3.10
Why is materiality important in management's design of an effective system of ICFR?

Interpretive response: Materiality is important in management's design of an effective system of ICFR because it focuses attention on those financial statement amounts and disclosures that could influence the decisions of the users of the financial statements.

Management's ability to properly identify RMMs and controls that mitigate those risks comes from applying the concept of materiality to the financial reporting process and the resulting financial statements. Establishing an appropriate materiality measure is an integral component of a focused and effective risk assessment process.

Practical tip

Given their common purpose in establishing materiality, the materiality used by management and external auditors generally would be within close proximity to one another. Open and early communication with auditors on management's scoping and what has been deemed to be immaterial and/or not contain a potential RMM is important for alignment on the determination of materiality.

Question 3.3.20
Is a materiality analysis solely quantitative?

Interpretive response: No. Management should consider the guidance in SEC Staff Accounting Bulletin (SAB) Topic 1M related to materiality. Provided below is an excerpt indicating that a materiality analysis involves more than quantitative considerations.

Excerpt from SAB Topic 1M

…quantifying, in percentage terms, the magnitude of a misstatement is only the beginning of an analysis of materiality; it cannot appropriately be used as a substitute for a full analysis of all relevant considerations. Materiality concerns the significance of an item to users of a registrant's financial statements. A matter is "material" if there is a substantial likelihood that a reasonable person would consider it important. In its Concepts Statement 2, Qualitative Characteristics of Accounting Information, the FASB stated the essence of the concept of materiality as follows:

> The omission or misstatement of an item in a financial report is material if, in the light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item.

Question 3.3.30
Is materiality considered only at the consolidated entity level?

Interpretive response: No. Materiality established at the consolidated entity level corresponds with the ultimate objective of effective ICFR, defined in SEC Regulation 13a-15(f) as "reliable financial reporting and financial statements prepared in accordance with GAAP." However, given the complex and multilayered structure of many of today's businesses, it is important for management to 'translate' this consolidated entity-level objective into relevant sub-objectives and measures of materiality at the component (e.g. division, subsidiary, operating unit) and business process levels.

Question 3.5.70 provides further discussion of considering materiality at the component level.

3.4 Scoping of accounts and disclosures

Question 3.4.10
Is risk assessment performed at the assertion level?

Interpretive response: Yes. The Internal Control over External Financial Reporting: A Compendium of Approaches and Examples is a companion document to the COSO Framework. It defines subobjectives of financial reporting in terms of assertions over significant accounts and disclosures in the entity's financial statements – meaning, the overall objective is reliable financial reporting in accordance with US GAAP. However, to achieve that objective, an entity should determine that the relevant assertions of significant accounts and disclosures have been met.

Financial statement assertions include:

- Completeness
- Accuracy
- Obligations and rights
- Existence
- Valuation
- Presentation

Question 3.4.20
What is a significant account or disclosure?

Interpretive response: A significant account or disclosure is an account or disclosure where there is a reasonable possibility that the account or disclosure could contain a misstatement that, individually or when aggregated with others, has a material effect on the financial statements. The determination of whether an account or disclosure is significant is made without regard to the effect of internal controls and may require judgment.

An entity decides which accounts present a risk that the financial statements contain a material misstatement. Based on the definition of a significant account, this analysis considers not only the individual account, but also whether the account in combination with other accounts might give rise to a material misstatement.

The determination of significant accounts is important because those accounts determined to be significant will require an ICFR response. Conversely, if an account is not significant, either individually or in the aggregate, no further ICFR work is required for that account.

While quantitative measures are important, the identification of significant accounts and relevant assertions also should consider qualitative factors and the results of management's entity-level risk assessment, including changes that might have an effect on financial reporting.

Example 3.4.10
Considering qualitative factors when identifying significant accounts

Scenario A: Accounts for a new strategically significant line of business

Facts: The entity is beginning a new line of business and will separately disclose information about that line of business because it is considered a significant part of the entity's strategy and is touted by management to investors and analysts.

Analysis: The revenues, costs and other accounts associated with the new line of business may be considered 'significant accounts' (i.e. a material misstatement could arise in those accounts) even if they are quantitatively less than materiality, due to them being separately disclosed and considered important to users of the financial statements.

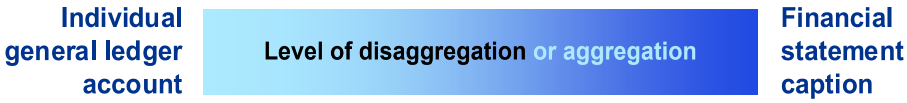
Scenario B: Accounts for which the completeness assertion is relevant

Facts: Some accounts, like the litigation accrual, or assets/liabilities associated with hedging activities, may be significant even if the current balance is less than materiality.

Analysis: A risk exists that these accounts could be misstated by more than materiality because material transactions or events may not be appropriately reflected in the accounts (i.e. the completeness assertion is relevant). For example, management has recorded a litigation accrual of $1m, which is less than materiality ($5m), however the potential effect of the litigation is $10m.

Question 3.4.30
How are significant accounts and disclosures aggregated or disaggregated?

Interpretive response: It depends on the facts and circumstances. As a general principle, significant accounts and disclosures should represent classes of transactions or balances that are subject to similar risks of error or fraud and similar controls. Therefore, determination of significant accounts and disclosures may require, on the one hand, disaggregation of the financial statement captions into components representing distinct classes of transactions or balances with varying risk profiles. On the other hand, entities may be able to aggregate multiple general ledger accounts into one significant account or disclosure based on the same principle.



Individual general ledger account

Level of disaggregation or aggregation

Financial statement caption

Appropriately defined significant accounts and disclosures will typically fall somewhere in between these two limits, depending on the specific facts and circumstances of the entity. Management considers factors such as the level of detail disclosed in the external financial statements and organization of the entity's chart of accounts when defining its significant accounts and disclosures.

Practical tip

It is important for management to precisely associate the identified risks with specific accounts or disclosures and to articulate why the controls designed and implemented by management and included in the annual ICFR assessment are responsive to such risks.

For example, if an entity's significant accounts are defined too broadly (e.g. at the financial statement caption level), the risk associated with a particular significant account may be presumed to exist across the entire account instead of an appropriately disaggregated portion of the account. Defining significant accounts too broadly may require a control response more pervasive than would otherwise be necessary.

Example 3.4.20

Disaggregation and aggregation in defining significant accounts

Scenario A: Industrial manufacturer with two revenue streams

Facts: An industrial manufacturing entity has two material revenue streams combined in the entity's financial statements into one caption called 'revenues' with additional disclosures included in the footnotes to the financial statements. One revenue stream relates to routine product sales while the other represents sales from arrangements with multiple deliverables. Each revenue stream results from a different process subject to different risks and a separate set of controls.

Analysis: Without disaggregating the 'revenues' financial statement caption into the two revenue streams previously described, management is unlikely to identify all the different risk points that could lead to a material misstatement for each revenue stream. Without identifying the proper risk points, management is also unlikely to design and identify the appropriate controls. In this case, it would be appropriate to disaggregate the revenue streams into separate significant accounts.

Scenario B: Retailer with retail store and e-commerce sales

Facts: A national retailer with a chain of physical store locations, as well as a large e-commerce sales platform, maintains a general ledger with separate accounts for sales generated by each store and the e-commerce business.

The merchandise sold at all store locations is similar and all stores use the same IT system to support their sales.

Analysis: Management aggregates all general ledger sales accounts related to the physical store locations into one significant account because all these general ledger accounts have a similar risk profile and are subject to a similar set of controls.

Management identifies another significant account for sales made through the e-commerce sales platform. Those risks include ones related to the delivery of the entity's merchandise to its e-commerce customers and the timing of the related revenue recognition.

Management identified two different significant accounts for the retailer's revenue because each is a result of a separate process and exposed to different risks.

Question 3.4.40

What is risk tolerance and how is it considered when defining significant accounts?

Interpretive response: The COSO Framework introduced a concept called 'risk tolerance', which is formally defined as "the acceptable level of variation in performance relative to the achievement of objectives." Said differently, risk tolerance represents the amount of error or uncorrected misstatement in relevant assertions over significant accounts and disclosures that management is willing to accept without concluding that the financial statements are materially misstated.

Risk tolerance for individual financial statement accounts and disclosures is established quantitatively at a level lower than materiality for the financial statements as a whole. Lower risk tolerance for individual accounts and disclosures reduces the probability that uncorrected misstatements across the various accounts and disclosures will, in the aggregate, become material to the overall financial statements.

Question 3.4.50

What actions should management consider taking to fulfill their ICFR-related responsibilities related to non-GAAP financial measures?

Background: A non-GAAP measure is a financial, operating, regulatory or statutory measure that is not determined under US GAAP. It is important to differentiate between non-GAAP financial measures and other non-GAAP measures. Non-GAAP financial measures reported by registrants are subject to certain SEC rules and oversight while operating, regulatory and statutory measures are not subject to those same rules. A non-GAAP financial measure is a numerical measure of a registrant's historical or future financial performance, financial position or cash flows.

Interpretive response: Management may take the following actions to fulfill their ICFR-related responsibilities for non-GAAP financial measures:

- evaluate and document on a routine basis the registrant’s population of non-GAAP financial measures, including:
  - how the registrant’s non-GAAP financial measures are used;
  - why the non-GAAP financial measures are relevant and important to investors and other users;
- communicate and discuss the registrant’s non-GAAP financial measures with the audit committee and senior management;
- incorporate the development and review of non-GAAP financial measures into management’s disclosure controls and procedures; and
- establish a written policy that requires non-GAAP financial measures to be transparent, consistent and comparable.

Most of these actions originate from recommendations of the SEC staff. The SEC released Compliance & Disclosures Interpretations on Non-GAAP Financial Measures in December 2022 and non-GAAP measures are discussed regularly at the annual AICPA conference.

The SEC staff has also emphasized that audit committee members should seek to understand management’s judgments related to the design, preparation and presentation of non-GAAP financial measures and how those measures might differ from other entities.

3.5 Scoping of components

Question 3.5.10
Which of the components of the group are deemed in scope for purposes of management's ICFR assessment?

Interpretive response: Management determines which of the entity's components (e.g. subsidiaries, divisions, entities, business units) present a risk that the financial statements contain a material misstatement. This evaluation includes quantitative measures (i.e. the volume or dollar amount of account balances) as well as qualitative measures (i.e. the nature of the transactions or activity at the component). Further, this analysis considers not only the individual component, but also whether the component in combination with other components might give rise to a material misstatement.

The only 'out of scope' components (i.e. components that may be excluded from the scope of management's ICFR assessment) are those components for which there is only a remote risk that the component individually, or in combination with other insignificant components, includes a material misstatement. The term 'remote' has the same meaning as in Topic 450 (contingencies) of the FASB's Accounting Standard Codification, which indicates a future event or events is remote when the chance of occurrence is 'slight'. Therefore, 'remote' is a rather low threshold for assessing the risk of a material misstatement of an entity's financial statements.

Question 3.5.20
Can an entity-level analytical review control be sufficient to mitigate risks in an individual component or aggregated components of an entity?

Interpretive response: It depends. Analytical reviews and comparisons of actual results to budget are common entity-level controls exercised by management over components of the entity (see Question 2.7.180). If such analytical reviews are used to address RMMs in the entity's financial statements, they need to be performed at an appropriate level of precision, meaning they would detect and correct a material misstatement in the underlying accounts and balances being reviewed. The level of precision of these controls should be documented along with evidence of their operation, including questions followed-up on and the related answers.

There is no bright line for the size of components (individually or in the aggregate) that an entity can address with these types of entity-level analytical review controls because it depends on each entity's facts and circumstances and the design of the analytical review control.

The burden is on the entity to demonstrate that entity-level analytical review controls operate in a manner that would prevent or detect, on a timely basis, a material misstatement in the entity's financial statements. However, practically speaking, it is difficult to design, operate and evaluate entity-level analytical review controls that are sufficient to mitigate risks in an individual component or aggregated components of an entity.

Question 3.5.30

Are newly acquired businesses subject to management's assessment of ICFR?

Interpretive response: Yes, but the SEC allows for a delay in reporting on ICFR for acquired businesses because it acknowledges management may have insufficient time to assess the controls at the 'as of date' for a recently acquired business. In such instances, management may scope out the acquired businesses from the assessment of ICFR and make appropriate disclosures in their annual filing. The period during which management may omit such assessment may not extend beyond one year from the date of acquisition, nor may such assessment be omitted from more than one annual management report on ICFR.

However, as it relates to the processes and controls over the preliminary acquisition accounting ('Day 1 Accounting') and consolidation of the acquired business, those controls need to be designed and operating effectively by the first public reporting date after the close of the transaction.

When designing controls over the measurement of amounts recognized in accounting for an acquired business, management should take into consideration the measurement uncertainty, which is affected by the degree to which the estimate is considered to be provisional (i.e. preliminary) (see chapter 10 of KPMG Handbook, Business combinations). However, even if provisional, controls still need to exist over the measurement, even if less precise, given the reporting requirements. As the acquisition accounting is finalized, controls should become more precise.

Section 4.5 provides discussion on understanding how estimates are determined and the identification of related risks and chapter 5 provides further guidance on process control activities.

Question 3.5.40

Are disposal groups included in management's scoping of components?

Interpretive response: Yes. Management needs to:

- assess if a reasonable possibility of material misstatement exists within the pre-divestiture activity of the disposal group in its risk assessment; and

- determine if the component includes a risk that the financial statements contain a material misstatement.

Regardless of the timing of disposal, management's ICFR assessment includes the entity's controls over applying accounting principles to the discontinued operations (e.g. determining whether the planned disposal constitutes discontinued operations under the financial reporting framework, preparing the presentation and related disclosures for the discontinued operations).

Question 3.5.50

What should the entity consider for components that are financially insignificant?

Interpretive response: If a component has been classified as being quantitatively insignificant, management should consider whether the component includes any RMMs and address the identified RMMs through ICFR.

For example, a component could be responsible for foreign exchange trading that creates an RMM to the group, even though the component is not otherwise of individual financial significance to the group.

Question 3.5.60

Is aggregation risk considered when determining whether a component is in scope (or out of scope)?

Interpretive response: Yes. There is aggregation risk related to entities comprised of multiple components (e.g. divisions, subsidiaries, operating units) where consolidated (or group) financial statements are prepared by aggregating financial information prepared for each component. For such entities, materiality established at the consolidated entity level is first translated into component materiality, or the amount of error that could be tolerated in the individual component (e.g. division, subsidiary, operating unit) financial statements. Component materiality is always lower than materiality established at the consolidated entity level.

Question 3.5.70

What are factors to be considered in determining component materiality?

Interpretive response: Component materiality for individual components should reflect a sufficient decrease from materiality to adequately address the aggregation risk that exists at the consolidated financial statement level. The size of the decrease from materiality for the overall financial statements may differ for each component and should be commensurate with the assessed aggregation risk.

Factors that should be considered when determining the size of the decrease from materiality include:

- the number and relative size of the components;
- the nature and extent of difference in operations, financial reporting and the control environment at each component in the current period (e.g. different systems, operations, financial reporting guidelines, etc. would lead to a lower component materiality); and
- the nature and extent of accounting judgments made at the component level.

As the number of components increases, the aggregation risk is also likely to increase, thus necessitating an even more careful analysis and consideration of a lower materiality for the component. The aggregation risk of component materiality for groups consisting of a smaller number of similarly sized components is likely lower and therefore components may have a higher materiality. The higher the aggregation risk identified, the lower the materiality should be for individual components.

Question 3.5.80

Should management document the scoping of its accounts, processes and components performed as part of risk assessment?

Interpretive response: Yes. It is important for management to document the consideration of materiality and ICFR objectives at the entity level and the translation of these entity-level concepts into relevant sub-objectives and measures of risk tolerance (see Question 3.4.40) and materiality at the division, subsidiary, operating unit and business process level. Management then uses these materiality considerations and ICFR objectives to scope the entity's accounts, processes and components and document these conclusions. Timely documentation of these considerations is key to an effective assessment of the entity's ICFR.

Practical tip

Scoping documentation may take the form of a memoranda on entity-level considerations, such as materiality, and a scoping matrix presenting the following:

- management's determination of the relevant components of the entity;
- significant accounts and disclosures at the entity and component level;
- relevant assertions over the accounts and disclosures; and
- information on how these items link to the related business processes and internal controls.

3.6 Identifying and assessing fraud risks

Question 3.6.10
Are all entities required to consider fraud risks in their risk assessment?

Interpretive response: Yes. The COSO Framework requires entities to consider the potential for fraud in assessing risks to the achievement of its objectives.

Every business entity faces some risk of fraud from within. However, the very nature of fraud makes it difficult to detect. It can also evolve and change over time, which makes prevention or detection of fraud even more difficult. In addition, 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.

Given the nature of fraud and the difficulties involved in its detection, both the SEC staff and the COSO Framework make it clear that an appropriate risk assessment should specifically consider the entity's vulnerability to fraudulent activity.

Principle 8 of the COSO Framework (see Question 2.5.120) identifies four types of fraud that require consideration in an entity's risk assessment process:

Type of fraud	Impact
Fraudulent financial reporting	May result in a misstatement in the financial statements. See Question 2.5.130.
Misappropriation of assets	May result in a misstatement in the financial statements. See Question 2.5.130.
Corruption and other illegal acts	Corruption is generally considered more of a compliance matter but could influence the control environment that also affects the entity's external financial reporting objectives.
Management override of controls	Management override describes action taken to override an entity's controls for an illegitimate purpose including personal gain or an enhanced presentation of an entity's financial condition or compliance status. See Question 5.14.40.

Question 3.6.20
How is a fraud risk assessment performed?

Interpretive response: As part of the fraud risk assessment process, management and those charged with governance first look at broad programs that detect or deter fraud. This assessment crosses over with many of the processes, controls and programs considered in the control environment component of ICFR (see section 2.4), such as:

- the entity's whistleblower hotlines;
- the tone at the top and how it is communicated throughout the organization; and
- the entity's response when fraud or potential fraud is identified.

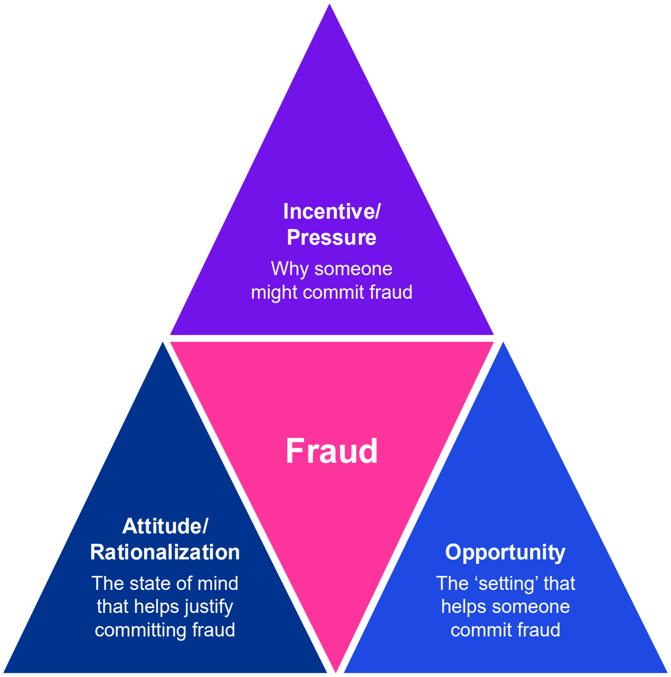
The SEC has highlighted the importance of the whistleblower hotline and noted that a hotline should not just be a check the box requirement and instead should focus on a culture that encourages whistleblowers to come forward.

These broad programs are critical to effective fraud prevention and, therefore, are considered when determining whether fraud risk is effectively mitigated. However, consideration of these broad programs is only the first step in considering the risk of fraud. A robust fraud risk assessment also includes:

- identifying fraud risk factors present at various levels within the entity (see Question 3.6.30); and
- identifying specific fraud risks at the financial statement and assertion level (see Question 3.6.50).

Question 3.6.30
How are fraud risk factors identified?

Interpretive response: Identifying fraud risk factors involves assessing the three categories of fraud risk factors represented in the 'fraud risk triangle' – incentives and pressures, opportunity, and attitudes and rationalizations – as illustrated in the following diagram.



- **Incentives and pressures** are typically assessed by considering:
  - what those incentives or pressures are (e.g. pressure to meet or exceed analysts' earnings expectations or to meet financial covenants required in debt agreements; incentive to meet financial targets to earn bonuses or increase stock value); and
  - who is exposed to those incentives and pressures (e.g. management, sales representatives, finance personnel).

  An analysis of compensation plans for key individuals is likely necessary to fully understand whether an incentive to commit fraud exists and, just as important, where the factor might manifest itself into an assertion-level fraud risk.

- **Opportunity** refers to conditions that exist that might allow employees to commit fraud. Examples where an opportunity to commit fraud may exist include:
  - the entity's inventory is not properly secured and therefore is subject to theft and resale by employees; and
  - the entity's sensitive financial statement estimates can be manipulated, resulting in a material effect on an entity's earnings.

- **Attitudes and rationalizations** is a subjective analysis that often coincides with an evaluation of the tone at the top. However, it is not just an analysis of whether someone has an attitude of committing fraud – such an attitude may be difficult to detect. An analysis of attitudes and rationalizations extends to whether key management understand the importance of accurate financial reporting. For example, a CEO who is unduly interested in improving financial results may either have an attitude or create a rationalization in others that fosters an environment where fraud might be tolerated.

In general, at least one of these fraud risk factors is present when fraud exists. All three factors are not required to be observed or evident to conclude that a fraud risk exists. An entity may conclude that a fraud risk exists even when only one of the three factors is present.

The COSO Framework identifies factors that may influence the various ways that fraud in financial reporting could occur and that should be considered in management's fraud risk assessment.

Factors that may influence the occurrence of fraud	Fraud risk factor category
Management bias	Attitude
Degree of estimates and judgments in external reporting	Opportunity
Fraud schemes and scenarios common to the industry sectors and markets in which the entity operates	Opportunity or attitude
Geographic regions where the entity does business	Opportunity or attitude
Incentives that may motivate fraudulent behavior	Incentive
Nature of technology and management's ability to manipulate information	Opportunity
Unusual or complex transactions subject to significant management influence	Opportunity or attitude
Vulnerability to management override and potential schemes to circumvent existing control activities	Opportunity or attitude

Question 3.6.40
How does an entity consider fraud risk factors in identifying fraud risks?

Interpretive response: Once an entity identifies fraud risk factors, it evaluates whether those factors, individually or in combination, indicate that a fraud risk is present.

The SEC staff[3] has stated that "Management should recognize that the risk of material misstatement due to fraud ordinarily exists in any organization,

[3] 17 CFR Part 241 (Release No. 33-8810), Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934, p. 14.

regardless of size or type, and it may vary by specific location or segment and by individual financial reporting element.

For example, one type of fraud risk that has resulted in fraudulent financial reporting in companies of all sizes and types is the risk of improper override of internal controls in the financial reporting process. While the identification of a fraud risk is not necessarily an indication that a fraud has occurred, the absence of an identified fraud is not an indication that no fraud risks exist. Rather, these risk assessments are used in evaluating whether adequate controls have been implemented."

Once fraud risks have been identified, the entity designs control activities responsive to the fraud risks, including, but not limited to, the risk of management override of controls.

Question 3.6.50
How does management define and document assertion-level fraud risks?

Interpretive response: Generally, the identified fraud risks should be linked to a specific financial statement assertion or assertions. Without this link, it may be difficult to understand what controls should be designed or selected for evaluation to address the fraud risks.

In the unusual case where it is not possible to link the identified fraud risk to a specific financial statement assertion, management should consider whether the identified fraud risk is defined in an overly broad manner. If so, management should consider the need to redefine the fraud risk. If not, and the identified fraud risk truly has a pervasive effect on the entity's financial statements, management would need to develop an appropriately robust control response.

When assertion-level fraud risks are identified, the entity should be very specific about what the risk is. For example, if there is an incentive for management to increase revenue, specific opportunities for management to manipulate revenue, such as the following, should be identified (see Example 3.6.10):

- posting fictitious journal entries to record additional revenue (management override of controls);
- entering into side agreements with customers (e.g. an agreement with the customer to take delivery of goods before they are wanted or needed with an understanding that the goods can be returned after period-end or that the payment terms can be extended);
- marking items as shipped in the system when they have not yet been physically shipped; or
- manipulating estimates related to revenue (e.g. shipping transit time, performance obligations satisfied over time).

The more specific the risk, the better the entity is going to be able to design and monitor controls that are responsive to the risk. This risk assessment should be documented consistent with Question 3.5.80.

Example 3.6.10
Revenue-related fraud risks and related controls

The following table includes examples of fraud risks related to revenue and controls that may address those risks.

Fraud risks	Controls[1]
Posting fictitious journal entries to record additional revenue	Review by an objective party of all manual journal entries posted to the revenue account and a subledger-to-general-ledger reconciliation
Entering into side agreements with customers	Confirmations with customers to identify side agreements, or a post-period-end review of returns or aged receivables by appropriate personnel specifically looking for indicators of side agreements
Marking items as shipped in the system when they have not yet been physically shipped	Sweeps of loading docks and warehouse facilities or comparisons of shipping terms to customer requests by appropriate personnel
Manipulating estimates related to revenue	Review of key estimates by appropriate personnel, including comparison of key estimates to prior periods

Note:

1. See chapter 5 for considerations related to appropriate control design.

Keep in mind that if an entity has identified an assertion-level fraud risk, it is expected that there will be incremental effort to mitigate the risk – either additional controls added to mitigate the risk or specific changes to the design or operating effectiveness of existing controls. In the side agreements example above, entity personnel are likely constantly reviewing returns and aged receivables. But, in response to the fraud risk, the analysis should be specifically focused on returns or aged receivables that may indicate side agreements.

Section 4.7 discusses journal entry process understanding and identification of risk points, section 5.13 discusses controls responding to a fraud risk and section 5.14 discusses controls over journal entries and other adjustments.

Question 3.6.60
How is materiality considered in an entity's fraud risk assessment?

Interpretive response: When identifying and evaluating risks of fraud in the entity's financial reporting process and designing and evaluating relevant anti-fraud controls, management should consider:

- the quantitative materiality of any potential misstatements; and
- the qualitative effects the fraud could have.

The objective of effective ICFR is to prevent or detect, on a timely basis, a material misstatement due to fraud or error. Given that objective, it is important to acknowledge that risks of fraud generally require careful consideration and response in the form of appropriately designed controls even if the misstatements that could arise because of those fraud risks are lower than the quantitative measure of materiality. This is due to the qualitative considerations related to misstatements caused by fraud in the financial statements.

Qualitative considerations that an entity may consider as part of its fraud risk assessment include:

- intent to achieve a particular outcome, such as to meet analyst expectations;
- involvement in the fraud by members of senior management; and
- questions about the pervasiveness of the fraud and its effect on the reliability of the entire financial statements.

Question 3.6.70
How are those charged with governance involved in an entity's fraud risk assessment?

Interpretive response: The COSO Framework emphasizes the importance of those charged with governance overseeing the fraud risk assessment process. This is particularly important when it comes to the risk of management’s override of controls. In line with the COSO Framework, those charged with governance challenge management, depending on the circumstances, when performing this oversight.

For example, based on the results of the entity's risk assessment process, those charged with governances might exercise its oversight role by, on a periodic basis:

- selecting a sample of significant accounting estimates in the financial statements; and
- reviewing and challenging management's key judgments in these estimates.

Those charged with governance might perform similar oversight for the accounting and financial reporting of significant unusual transactions and other matters that may be prone to bias and override of controls.

Example 3.6.20
Refresh of the entity's fraud risk assessment process

Management and the Audit Committee take a fresh look at the entity's fraud risk assessment process. They determine that fraud risks have been historically 'covered' by the overall risk assessment activities conducted on an annual basis by Internal Audit. However, after reviewing the guidance included in the COSO Framework, management and the Audit Committee determine that to truly achieve Principle 8 (see Question 2.5.120):

- Fraud risk assessment should be integrated with the wider enterprise risk assessment process and conducted by the Risk Management Office.
- The process should include formal discussions with key personnel at the entity's corporate head office and all significant locations.
- The discussions with key personnel should consider the different types of fraud facing the entity and the various ways that a material financial reporting fraud could occur.
- In preparation for the discussions with key personnel, Risk Management Office personnel should analyze the 'fraud risk triangle' to help identify conditions in which fraud may occur.
- Findings from the fraud risk assessment meetings should be summarized in minutes.
- Identified fraud risks should be documented in a Risk and Control Matrix, evaluated for severity and linked with relevant controls.
- Results of the fraud risk assessment process should be revisited and reported to the Audit Committee on an at least annual basis.

3.7 Consideration of changes to ICFR

Question 3.7.10
Are changes to ICFR required to be evaluated?

Interpretive response: Yes. Principle 9 of the COSO Framework (see Question 2.5.180) requires management to have controls in place to early identify and communicate ICFR changes that have a significant effect on financial reporting, and to assess the risks resulting from those changes. The COSO Framework refers to such controls as an 'early warning system'.

Question 3.7.20

What types of changes to ICFR are required to be evaluated?

Interpretive response: Entities are required to assess the changes listed here and consider how such changes may affect their system of ICFR.

Changes in the…	Examples
External environment	• New laws • New accounting pronouncements • New stock exchange regulations
Business model	• New product launches • Geographical expansion • Restructuring
Leadership of the entity	• New executive leadership • Turnover in key financial reporting positions

Example 3.7.10

Entity-wide events with financial reporting risks and ICFR impact

The following table includes examples of entity-wide events and how they may affect financial reporting. These changes should be evaluated to determine if there are new PRPs that require a new or modified control response.

Event	Potential impact to financial reporting
Changes in GAAP	• changes in how underlying data is captured, generated, analyzed or reported • new RMMs • risks related to SAB 74 disclosures
Changes in third-party service providers	• changes to the way the third-party receives and provides data • changes to the way the third-party processes data
Changes in business strategy	• assets held for sale • triggering events for asset impairment • change in the entity's determination of materiality • new or modified revenue streams
Entrance into new geographic markets	• unknowns related to valuation of receivables • new risks for safeguarding of assets in new environment
Business combinations	• purchase price accounting • valuation of intangibles and other assets

Event	Potential impact to financial reporting
Other nonroutine transactions[1]	• approval of nonroutine transactions • new accounting treatment(s) • new RMMs
Changes in organizational structure	• change in reporting units
Deterioration of the results of operations	• triggering events for potential impairment • going concern assessment

Note:

[1] Examples of other nonroutine transactions include issuances of debt, restructurings, unusual sales transactions or related party transactions.

Other changes could have an affect directly on personnel including layoffs (RIFs), promotions, new hires and offshoring. These can all result in new control operators performing controls, and therefore focus should be given to their authority and competence as well as consideration of increased risks due to constrained resources. RIFs and other layoffs also may provide a fraud risk factor related to an increased risk of fraud due to disgruntled employees.

Example 3.7.20
Change in business model – entity's investment policy

Facts: An entity makes a change in its investment policy when senior management decides to invest in lower-grade securities to obtain a higher yield, and the board of directors approves the decision.

Analysis: This change should be identified and analyzed for any potential effect on ICFR. For example, investing in lower-grade securities may present significant valuation risks that previous investments in cash and cash equivalents did not – these risks will need to be understood and controlled. It is very likely that ICFR in the area of valuation of securities will need to be enhanced given the new risks.

Example 3.7.30
Change in external environment – COVID-19

As a result of COVID-19, entities may have been faced with new or exacerbated risks of misstatement to the financial statements. Such risks may range from:

- more traditional risks that simply did not represent risks of material misstatement in the previous years (such as impairment of certain long-lived assets); to

- risks that are unique to the current environment (such as appropriate recognition of funds received from various government assistance programs).

In addition, remote working conditions or, at some entities, employees' return to their workplaces, as well as employee turnover and lack of qualified employees in certain industries or geographic locations, may have a significant effect on entities' ICFR.

Example 3.7.40
Change in external environment – Russia-Ukraine war

The Russia-Ukraine war and related events are taking place at a time of global economic uncertainty and volatility, and the effects are likely to interact with and exacerbate current market conditions, including global demand, foreign exchange rates, interest rates and general liquidity. These effects may be felt by a broad range of entities with no direct exposure to Russia, Belarus or Ukraine and may carry through to the entities' financial statements and ICFR.

Potential direct and indirect effects of the Russia-Ukraine war may include, but not be limited to:

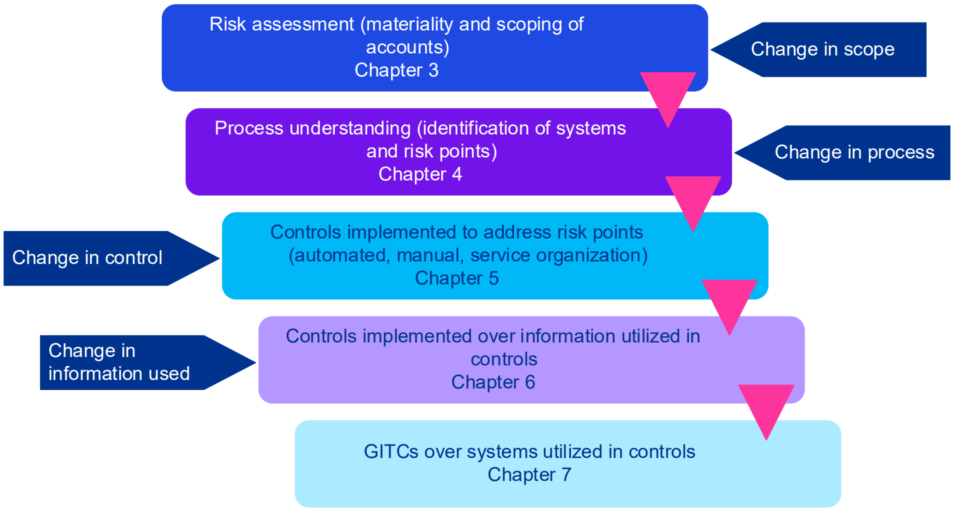
Direct effects	Indirect effects
• Destruction/closure/abandonment of facilities, which may not be recoverable due to act of war exceptions in insurance contracts. • Significant business interruption and lack of ability to operate due to: – loss of inventory; – inability to manufacture and/or procure key materials; – travel restrictions; – logistics disruptions; and unavailability of personnel. • Sanctions, laws, regulations and involuntary actions on the entity's ability to do business. • Inability to finance operations due to lack of access to capital or inability to access financial instruments located in certain countries.	• Rising commodity prices • Increased raw material costs • Supply chain disruptions and delays • Inflation • Labor shortages • Trade friction • Uncertain financial markets

Example 3.7.50
Change in external environment – climate risks

As part of the risk assessment process, an entity may need to consider the effect of evolving climate risks, such as transition risks (e.g. changes in legislation, the entity's operations, reduced availability of raw materials) or physical risks that may impact the entity's financial reporting (e.g. loss of information systems due to extreme weather events). Performing an effective risk assessment includes understanding whether the related process is designed to capture both internal and external factors that have financial reporting implications.

Question 3.7.30
How much of the ICFR process does a change in risk assessment impact?

Interpretive response: Risk assessment has a widespread effect – a change in risk assessment or the process could result in a change to the PRP and therefore necessitate a change in the process control activity. Management should evaluate the magnitude of a change to enable it to be properly considered and addressed as part of ICFR.


Risk assessment (materiality and scoping of accounts) Chapter 3
Change in scope
Process understanding (identification of systems and risk points) Chapter 4
Change in process
Change in control
Controls implemented to address risk points (automated, manual, service organization) Chapter 5
Change in information used
Controls implemented over information utilized in controls Chapter 6
GITCs over systems utilized in controls Chapter 7

See section 5.17 for guidance on changes in controls.

Example 3.7.60
Changes at an entity and their effect on ICFR

This example includes three change events at an entity and the effects on the entity's ICFR response depending on the likelihood of the event touching ICFR and the pace or magnitude of the change to ICFR.

Change event	Likely to result in a significant ICFR response	Likely to result in less significant or no ICFR response
Reduction in force (RIF)	• Large RIF spans across the entity or within the finance department.	• Small RIF is concentrated in an area that doesn't handle ICFR directly.

Change event	Likely to result in a significant ICFR response	Likely to result in less significant or no ICFR response
	- Potential change in process.	- Potential or no change in controls.
Entrance into new geographic market	- New market is expected to be one of high and relatively quick growth. - Potential change in scope.	- Growth of new market is expected to be slow and methodical. - Potential or no change in controls.
Change in a third-party service provider	- Third-party service provider handles processing of 50% of revenue transactions. - Potential change in process.	- Third-party service provider handles processing of legal claims where the entity has multiple methods to determine the complete population of legal claims. - Potential or no change in controls.

Practical tip

For larger changes, management may perform a change impact analysis, including affected areas, roles, controls and processes, and highest areas of resistance and risk. After this analysis, they can then outline a plan to address any identified risks.

Question 3.7.40
How often should changes to ICFR be evaluated?

Interpretive response: Continuous risk assessment is critical to respond to a changing business and control environment. Given the pace of change and how fluid current conditions are, there is likely a need to revisit the risk assessment determinations in some areas more than once throughout the year.

Practical tip

Having one of the following periodic controls can assist in identifying smaller changes in controls that can ultimately have a large effect on management's ICFR assessment:

- Each control owner attests to whether there have been changes in controls.
- Agendas for management or other committee meetings include a standing item to discuss and assess changes in controls.

Key takeaways

- Risk assessment is an iterative, cumulative process that requires a reassessment of initial conclusions based on evidence obtained throughout the assessment.
- Materiality should be determined based on those financial statement amounts and disclosures that could influence the decisions of the users of the financial statements.
- Management conducts risk assessment at all relevant levels within the entity, from the consolidated entity level down to the business process level. Appropriate members of management and other employees should be involved in the risk assessment process.
- Management determines the components of the group that are of quantitative or qualitative significance and their significant accounts as part of scoping.
- Fraud risk assessment should be comprehensive, cover various levels within the entity and involve appropriate members of management and employees.
- Risk assessment considers changes that could have an effect on ICFR. Identified changes are typically analyzed down to the process level.

4. Process understanding

Detailed contents

Examples

4.4 Considerations related to period-end financial reporting, including preparation of disclosures, in obtaining a process understanding and identifying risk points

Questions

4.5 Considerations related to estimates in obtaining a process understanding and identifying risk points

Questions

4.5.10 What is an accounting estimate?

4.5.20 How do estimates pose a risk to the financial statements?

4.5.30 What is estimation uncertainty?

4.5.40 Where does estimation uncertainty arise in accounting estimates?

4.5.50 What is ‘subjectivity’?

4.5.60 What is ‘complexity’?

4.5.70 What is 'management bias' and how does it affect accounting estimates?

4.5.80 What should management consider when identifying accounting estimates within their processes?

4.5.90 What controls should the entity have over the identification and oversight of estimates?

4.5.100 What are the primary elements of an estimate?

4.5.110 What does management understand related to the development of estimates?

4.5.120 How are risks identified as part of estimates?

4.5.130 What are the additional inherent risk factors considered in relation to accounting estimates?

4.5.140 What does management consider when evaluating whether the method may give rise to an RMM for the estimate?

4.5.150 What does management consider when evaluating whether the model may give rise to an RMM for the estimate?

4.5.160 What does management consider when evaluating whether an assumption may give rise to an RMM for the estimate?

4.5.170 What does management consider when evaluating whether the data may give rise to an RMM for the estimate?

4.5.180 How might management address estimation uncertainty?

4.5.190 How might the applicable financial reporting framework affect the related disclosures regarding estimation uncertainty?

4.5.200 What are common PRPs and controls related to whether disclosures for accounting estimates conform to the applicable financial reporting framework?

4.5.210 When might management use specialists or third parties (other than specialists) in developing an accounting estimate?

4.5.220 Are the risks for estimates different if management uses a specialist?

4.5.230 Does the entity identify risks over data generated by a specialist specifically for the entity's use in an estimate?

Examples

4.5.10 Documentation of understanding of the process for developing accounting estimates

4.5.20 Understanding elements and identifying PRPs in an estimate

4.6 IT considerations when obtaining a process understanding and identifying risk points

Questions

4.6.10 What are IT considerations when obtaining a business process understanding?

4.6.20 Why is understanding the overall IT environment important?

4.6.30 What is a better practice for documenting the understanding of IT systems?

4.6.40 What is included in an ISD?

4.6.50 Is management required to identify IT risks at the process level?

4.6.60 What effect do GITCs have on IT at the process level?

4.7 Considerations for journal entries and other adjustments while obtaining a process understanding and identifying risk points

Questions

4.7.10 Does obtaining a process understanding apply to the journal entry process?

4.7.20 What are potential risks associated with journal entries and other adjustments?

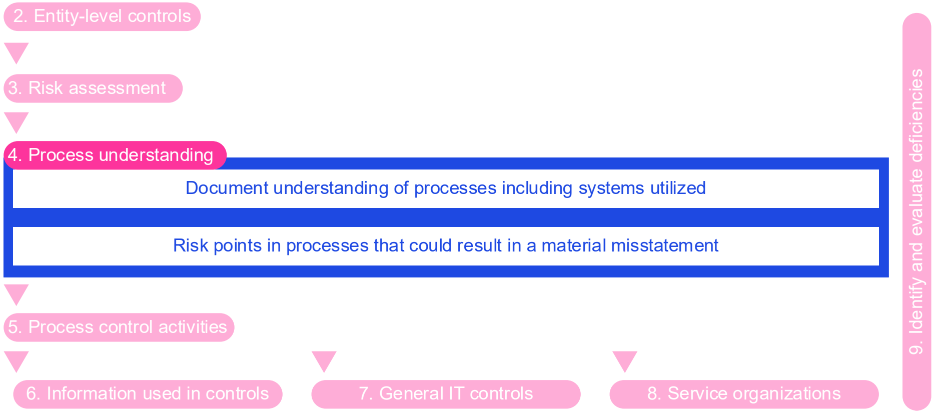
4.7.30 What are the risks related to automated and manual journal entries and other adjustments?

4.7.40 What are additional considerations related to the approval of journal entries?

Key takeaways

4.1 Management's ICFR journey

Obtaining an understanding of business processes and the financial reporting process is an important part of management's ICFR journey because it provides the basis for management to identify and assess process risk points (PRPs) and the related risks of material misstatement (RMMs). These activities facilitate the identification, design and implementation of appropriate control activities to address PRPs (see chapter 5). An inadequate understanding of a business process and the related RMMs and PRPs often can lead to inappropriate design and selection of controls, which in turn can result in deficiencies being identified in the later stages of an entity's ICFR.


2. Entity-level controls
3. Risk assessment
4. Process understanding
Document understanding of processes including systems utilized
Risk points in processes that could result in a material misstatement
5. Process control activities
6. Information used in controls
7. General IT controls
8. Service organizations
9. Identify and evaluate deficiencies

Identifying and documenting RMMs and PRPs

This chapter starts with explaining how management identifies RMMs and PRPs (see section 4.2). An RMM is a risk that could result in a material misstatement to the financial statements. A PRP is a point in the business process that a misstatement could, individually or in the aggregate, yield a material misstatement (including a misstatement due to fraud) to the financial statements. The PRP is the 'where' and the 'how' in the business process that a misstatement could be introduced. The RMM is the 'what' that could be misstated.

There are many inherent risk factors in individual transactions processed through (or in) an account or reflected in a disclosure that may be considered in determining if a PRP could result in an RMM. Those PRPs that could result in a material misstatement, individually or in combination with other misstatements, require an ICFR response.

PRPs that could result in RMMs should be documented in sufficient detail to identify the specific condition that would allow for a material misstatement to occur within the financial statements. In addition, the documentation for each PRP should link to a relevant financial statement assertion.

Obtaining and documenting process understanding

This chapter continues with management gaining an understanding of its business processes and preparing/maintaining appropriate documentation of that understanding (see section 4.3). There are many ways management may obtain this understanding; but, generally, performing a walkthrough is the most comprehensive method of doing so. In a walkthrough, a single transaction is followed from initiation through the entity's processes, including its information systems, until the transaction is reflected in the entity's financial records.

The documentation of process understanding should capture the flow of information through an entity's process and be of sufficient detail to provide understanding of the flow of information through the entity's processes (see section 4.3) and relevant IT systems (see section 4.6) and identify all relevant RMMs and PRPs associated with a particular process (see section 4.2). Chapter 5 addresses the identification, design and implementation of control activities to address relevant PRPs.

Considering the financial reporting process in process understanding

Management's process understanding also includes the period-end financial reporting process (see section 4.4). That process includes the activities an entity performs to close the books and make post-closing adjustments when preparing the individual financial statements (e.g. balance sheet, statement of income) and related disclosures.

Considering estimates in process understanding

As part of its process understanding, management identifies and evaluates the risks related to accounting estimates (see section 4.5). By their nature, accounting estimates are subject to factors that inherently drive risks of misstatement, such as estimation uncertainty, complexity and subjectivity. These factors also make estimates susceptible to management bias.

As part of the ICFR framework, management should identify where there are estimates or changes in estimates in their business processes. Once identified, management determines whether there is an RMM associated with the selection or application of the methods, assumptions or data.

Considering IT in process understanding

Understanding the flow of transactions into, through and out of the relevant IT systems is an integral part of management's process understanding (see section 4.6). Management identifies and documents the relevant PRPs related to IT at the assertion level where there is a reasonable possibility that they could result in or contribute to a material misstatement. Documentation of management's consideration of IT in its process understanding may be facilitated using IT System Diagrams (ISDs).

Considering journal entries in process understanding

Management obtains an understanding of business processes all the way through the recording of journal entries and uses this understanding to identify the RMMs and PRPs related to journal entries (see section 4.7). The potential risks related to journal entries include the existence of the underlying transactions, their accuracy and completeness and the potential for management override. An understanding of the recording of journal entries also includes consideration of any differences in the process for manual versus automated journal entries, including authorization of manual journal entries.

Abbreviations

We use the following abbreviations in this chapter.

COSO	Committee of Sponsoring Organizations of the Treadway Commission
GAAP	Generally accepted accounting principles
GITC	General IT control
ICFR	Internal control over financial reporting
ISD	IT System Diagram
PRP	Process risk point
RAFIT	Risk arising from IT
RM	Risk of misstatement
RMM	Risk of material misstatement
SEC	Securities and Exchange Commission

4.2 Identifying the process risk points

Question 4.2.10
What does management do after completing process understanding?

Interpretive response: After obtaining an understanding of the flow of transactions, management identifies the PRPs.

Question 4.2.20
What is a PRP?

Interpretive response: A PRP is a point in the business process that a misstatement could, individually or in the aggregate, yield a material misstatement (including a misstatement due to fraud) to the financial statements. The PRP is the 'where' and the 'how' in the business process that a misstatement could be introduced.

Every business process is likely to contain multiple PRPs. In addition, each identified RMM will have at least one PRP.

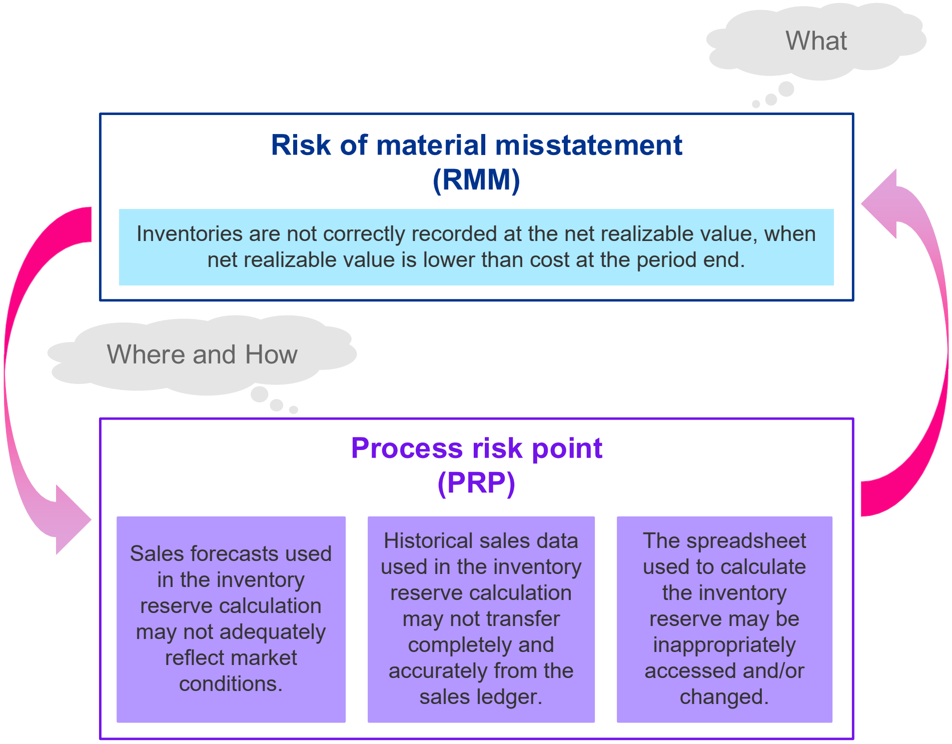
Question 4.2.30
What is the difference between an RM, an RMM and a PRP?

Interpretive response: RMs generally stem from the accounting framework, so they are generally the same for similar transactions across entities. RMs can become RMMs based on the specific factors of the entity, including size and volume of transactions. PRPs are the specific points where a material misstatement could be introduced by the process.

The RMM is the 'what' could be misstated, whereas the PRPs are the 'where' and the 'how' in the process an RMM can arise.

Example 4.2.10
Inventory illustration

In the diagram below, inventory is a significant account with an RM that has been identified as an RMM. The RM is based on the accounting standards and has been identified as an RMM due to the size and volume of transactions at the entity. In evaluating how the RMM could occur, the entity has identified process specific PRPs that are addressed by process control activities.



What

Risk of material misstatement (RMM)

Inventories are not correctly recorded at the net realizable value, when net realizable value is lower than cost at the period end.

Where and How

Process risk point (PRP)

Sales forecasts used in the inventory reserve calculation may not adequately reflect market conditions.

Historical sales data used in the inventory reserve calculation may not transfer completely and accurately from the sales ledger.

The spreadsheet used to calculate the inventory reserve may be inappropriately accessed and/or changed.

Question 4.2.40

Do all PRPs require an ICFR response?

Interpretive response: No. Only those PRPs that could result in a material misstatement, individually or in combination with other misstatements, require an ICFR response.

Question 4.2.50

What factors are considered in determining if a PRP could result in an RMM?

Interpretive response: Assessing the likelihood and magnitude of potential misstatements can help in determining if a PRP could result in an RMM. When the likelihood of a potential misstatement is more than remote and the magnitude is material, the PRP could result in an RMM.

The following are inherent risk factors in individual transactions processed through an account or reflected in a disclosure, or in the account or disclosure itself, that may be considered in determining if a PRP could result in an RMM:

- quantitative or qualitative significance, including:
  - 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;
- volume, complexity and homogeneity of activity;
- susceptibility to misstatement due to error or fraud;
- degree of accounting and reporting complexities;
- degree of subjectivity, including judgment in the recognition or measurement of financial information related to the risk;
- occurrence of change(s), including changes from the prior period, in characteristics of the account or disclosure;
- susceptibility to recent significant economic, accounting or other developments; and
- degree of uncertainty present.

Practical tip

Management should consider underlying GAAP when determining if there are additional RMMs within a process, particularly around infrequent and/or unusual transactions.

Question 4.2.60

Are internal controls considered when evaluating if a PRP is an RMM?

Interpretive response: No. The effects of internal controls are not considered when determining if a PRP could result in an RMM.

Question 4.2.70

How are PRPs identified?

Interpretive response: A PRP is not simply a risk that the data could be misstated. It also is not the absence of a control. Rather, a PRP is any condition that could allow material misstatements to enter the system or cause the data to lose its integrity. There are likely to be multiple PRPs in every business process.

PRPs also include a risk of unauthorized acquisition, use or disposition of assets that could result in a material misstatement of the financial statements.

There are many considerations in the identification of PRPs. For example:

- how data enters an IT system;
- how data is stored within an IT system, and the ways in which it may be accessed or transferred to another system;
- where in the process data is summarized, accumulated, subjected to calculations or otherwise manipulated;
- whether there are manual processes that affect the data (e.g. manual journal entries);
- when there are judgments made by management in determining whether or not to adjust data, and in determining the amount of any necessary adjustments; and
- how data is affected when it is summarized for inclusion in the financial statements (e.g. top-side entries during the period-end financial reporting process).

Question 4.2.80
How should PRPs that lead to RMMs be documented?

Interpretive response: PRPs that lead to RMMs should be documented in sufficient detail to identify the specific condition that would allow for a material misstatement to occur within the financial statements.

The specificity and clarity with which an identified risk is defined are key to management’s ability to design and operate controls that are appropriately responsive to that particular risk.

A properly defined and documented risk also is critical to the effective evaluation of the controls by management and external auditors. Failure to define risks with sufficient clarity often results in a missing control or a control that is not appropriately designed to address the actual risk.

In addition, the documentation for each PRP should link to a relevant financial statement assertion. Frequently, multiple PRPs link to the same relevant assertion. If a PRP does not link to a relevant assertion, it is likely not a relevant PRP for ICFR.

Example 4.2.20
Specificity and clarity of PRPs

The following are examples of common PRPs from the purchase-to-pay process where the initial PRP lacked specificity and clarity and the revised PRP provides sufficient specificity and clarity.

Initial	Revised
Accounts Payable and accrual balances (A/P and Accruals) are incomplete.	Invoices received after period-end relate to the current period but are not accrued for. [Completeness, Existence, and Accuracy of A/P and Accruals]
Expenditures are overstated.	Payment of duplicate vendor invoice numbers. [Existence of Expenses]
A/P is not accurately presented in the financial statements.	Receivables and A/P are offset and inappropriately reported under a net presentation. [Presentation of Receivables and A/P] Debits inappropriately exist within the A/P subledger and are netted against the ultimate credit recorded on the financial statements. [Presentation of A/P]
Selling, General, and Administrative (SG&A) expenses are incomplete.	Cash disbursements are coded to incorrect general ledger accounts. [Completeness, Existence, and Accuracy of SG&A expenses; Completeness, Existence, and Accuracy of PP&E] Vendor invoices are not submitted on a timely basis to the Accounting Department by various corporate departments. [Completeness of SG&A Expenses and A/P]

In each of these examples, the initial PRP is stated very generally. This may make it difficult to identify a specific control (or controls) that will mitigate the risk. In addition, a generic PRP may result in a risk of management missing relevant controls. By including more detail in the description of the risk, management and external auditors will be in a better position to identify and evaluate controls.

For example, the first revised PRP will put management in a better position to properly address the timely accounting for invoices received after period-end.

Example 4.2.30

Lack of specificity leads to ineffective design or assessment of controls

Management identifies and documents the following PRP: The statement of cash flows is incorrect.

To address the PRP, as documented, management may choose to rely on and evaluate the design and operating effectiveness of a control defined as ‘management’s review of the statement of cash flows.’ However, a properly designed review of the statement of cash flows may need to do more than just review the statement of cash flow’s ‘proof’ and tie numbers to the balance sheet. The review may need to include consideration of many other aspects of the statement of cash flows, such as key information about noncash transactions, foreign currency effects and items that are required to be reported gross.

The lack of specificity in the control may lead to management's review not identifying issues with the cash flow statement, including (but not limited to) the following:

- inaccurate or incomplete proof of the cash flow statement;
- inaccurate or incomplete tie-out of the numbers in the cash flow statement to the balance sheet;
- incomplete information about noncash transactions;
- improper consideration of foreign currency effects; and
- improper reporting of amounts gross that should be reported net.

Without more detailed PRPs related to the preparation and review of the statement of cash flows, management may not identify the right controls to address all relevant PRPs.

This example illustrates that a heavily aggregated or overly general PRP may lead management to design a control, or external auditors to select a control for evaluation, that appears to address the PRP when, in actuality, the control only addresses a portion (or none) of the potential for misstatement (i.e. the PRP).

4.3 Understanding the business process and performing walkthroughs

Question 4.3.10
Is management required to gain an understanding of business processes?

Interpretive response: Yes. An aspect of Principle 7 of the COSO Framework (see Question 2.5.100) requires understanding the business process activities and the flow of data from initiation to reporting. That aspect of Principle 7 is so critical to ICFR that it warrants its own chapter in this Handbook.

Obtaining an understanding of business processes as well as the financial reporting process provides important information used in identifying and assessing RMMs and where they can occur within the process – the PRPs. Management then designs appropriate control activities to address the identified PRPs.

For example, a thorough understanding of the revenue process helps management identify and understand:

- each type of revenue stream;
- where in the process there is reliance on IT systems; and
- related estimates in the process.

Inadequate understanding of a business process and the related PRPs often can lead to inappropriate design and selection of controls, which in turn can result in deficiencies being identified in the later stages of the ICFR assessment process.

As business processes are owned and operated by management, it is generally acknowledged that the business process is 'understood by management.' However, the knowledge of a business process, especially in larger or more complex entities, can be spread between a few to dozens of individuals who know only their part of the process. This is particularly true in processes with complex IT systems, estimates or transaction flows.

Complex business processes involving multiple individuals knowledgeable only about their part of the process can lead to the inappropriate identification of risks, which then leads to controls that are not properly designed to address RMMs. Discussion of understanding the process throughout this Handbook is focused on the centralization of that understanding by individuals that are performing risk assessment and designing controls to address identified PRPs.

Question 4.3.20

Is management required to document an understanding of business processes?

Interpretive response: Yes. As part of the COSO Framework, management is required to develop and maintain documentation of their business processes as part of their ICFR.

Effective documentation of business processes assists in:

- creating standards and expectations of performance and conduct;
- operating the process on a consistent basis;
- identifying PRPs;
- identifying estimates and related risks;
- capturing the design of internal controls;
- communicating the who, what, when, where and why of internal control execution;
- communicating processes to external auditors; and
- retaining knowledge.

Question 4.3.30

What is included in understanding a business process?

Interpretive response: When management obtains an understanding of a business process, they specifically understand:

- how the transactions are initiated, and how information about the transactions is recorded, processed, incorporated in the general ledger and reported in the financial statements;
- how information about events and conditions, other than transactions, is captured, processed and disclosed in the financial statements;
- which accounting records, specific accounts in the financial statements and other supporting records are involved in the business process, as well as how the information flows through IT system;
- which estimates are relevant to the business process; and
- which of the entity's resources, including the IT environment, are relevant to the business process.

Question 4.3.40

How is an understanding of business processes obtained?

Interpretive response: There are many ways an entity may obtain an understanding of a business process, including interviewing people who are involved in the process. Generally, a walkthrough is in the most comprehensive method for obtaining that understanding because following a transaction through the process validates what is described in an interview.

Question 4.3.50

What is a walkthrough?

Interpretive response: In a walkthrough, a single transaction is followed from initiation through the entity’s processes, including its information systems, until the transaction is reflected in the entity’s financial records. The person performing the walkthrough uses the same documents and technology used by those performing the process. It is important to follow the flow of information (or transaction data) by inspecting key documents, reports and third-party deliverables within the process.

Question 4.3.60

Is a walkthrough performed of the process as a whole, or just the controls that are in place?

Interpretive response: A walkthrough is performed of the process as a whole, and not just the individual control activities within the process. A walkthrough is about understanding the process, which is not the same as identifying RMMs and process control activities to mitigate those RMMs. However, the two are interrelated because understanding the process will lead to identifying RMMs and mitigating process control activities.

Concentrating the walkthrough procedures on just the previously identified controls ignores the possibility that additional RMMs exist between the identified points of control. If these RMMs are not identified, relevant controls are not designed and operated to mitigate those RMMs.

Practical tip

Management may find it helpful to include all relevant process and control owners in the applicable process walkthrough. This helps enable the walkthrough to include the entire process, rather than just the individual controls that are the responsibility of the specific control owner that participates in the walkthrough.

Question 4.3.70

Who is responsible for understanding the business process?

Interpretive response: The responsibility for obtaining an appropriate understanding of each relevant business process, the flow of information and PRPs belongs to the entity's management. That responsibility cannot be delegated to the external auditors. In fact, it may be impossible for the external auditors to properly identify and evaluate risks of misstatement of the financial statements and the related mitigating controls if management's own risk assessment process or documentation is missing or deficient.

Practical tip

Scheduling a joint walkthrough that includes management and the entity's external auditors may reduce the amount of time and effort incurred by process and control owners. In addition, ensuring all relevant parties are included in the walkthrough may reduce the number of follow-up questions and/or requests for additional documentation after the walkthrough is completed. Management may consider selecting a relevant transaction and asking for the supporting documentation in advance of the walkthrough to prepare their questions ahead of time and help obtain a thorough understanding.

Question 4.3.80

When does management obtain an understanding of the business process?

Interpretive response: Management obtains an understanding of business processes and the flow of transactions related to processes with likely RMMs early in the ICFR assessment process.

New information may come to light as the ICFR assessment process progresses throughout the relevant reporting period. If this happens, it may be necessary to revisit the preliminary determination of processes requiring a walkthrough. If additional potential RMMs are identified, it is then necessary to obtain an understanding of the related PRPs and whether there are process control activities in place to address those risks.

Similarly, during the ICFR assessment process, previously unidentified risks within a business process may come to light. If this happens, management may be required to supplement their understanding of the process and design and implement additional process controls to address the newly identified risks.

Business processes and the transaction flows are susceptible to change during the relevant reporting period. Such a change may occur after the initial understanding of the processes and transaction flows is obtained by management and the external auditors. For example, the entity may undergo a restructuring, experience turnover in personnel, implement new IT systems or reassign certain control responsibilities. When major changes occur, it is necessary for management to update its understanding of relevant business processes and any risks and controls that might have been affected by the changes. (See Question 4.3.190)

Question 4.3.90

How does management evidence their process understanding?

Interpretive response: Generally, flowcharting is the most effective manner for management to document their understanding of business processes, the flow of transactions, the relevant risks, and process control activities. Flowcharts, or flowcharts supplemented by a brief narrative, can substantially reduce or even eliminate the need for long, detailed process descriptions. The flowchart provides a condensed picture, while the narrative provides more detail and supplemental information. They can also help the entity comply with the objectives of Principles 7 and 10 of the COSO Framework (see Questions 2.5.100 and 5.2.50, respectively).

A flowchart graphically depicts steps and/or activities in a process, as well as key inputs and outputs. The purpose of a flowchart is to help identify the PRPs and the process control activities in place to address them. A flowchart does not need to be overly complex. Judgment is required to determine how much detail to include in a flowchart.

Practical tip

Narratives that are too long and detailed can make it more difficult to understand the end-to-end process. Using both a flowchart and a concise narrative can be the most effective way to document management’s understanding of a business process.

Question 4.3.100
What should be documented related to process understanding?

Interpretive response: The documentation of process understanding should capture the flow of information through an entity's process and be of sufficient detail to help management and the external auditors execute the following steps in the ICFR assessment process.

Step 1	Understand the flow of information through the entity's process
Step 2	Identify relevant IT systems through use of a flowchart or an ISD and understand the flow of information through IT systems
Step 3	Identify all relevant PRPs associated with a particular process
Step 4	Identify all relevant process control activities that address the relevant PRPs

As discussed in Question 4.3.90, management's documentation may take the form of a narrative or a flowchart, or a combination of the two.

Question 4.3.110
What type of questions should be asked in the walkthrough?

Interpretive response: At points within a process where important processing activities occur, the person performing the walkthrough places themself in the role of the process owners and control operators and asks the entity's personnel to explain what is required by the entity's prescribed procedures and controls.

Obtaining this explanation, combined with performing the other walkthrough procedures:

- allows management and external auditors to understand the process and identify:
  - important activities within the process;
  - potential opportunities for misstatement;
  - points at which a necessary control is missing or designed ineffectively;
- allows management and external auditors to understand the types of transactions handled by the process, particularly when the probing questions go beyond the narrow focus of the transaction used as the basis for the walkthrough; and
- may help identify indicators of fraud.

To corroborate information at various points in the walkthrough, the person executing the walkthrough might ask entity personnel to:

- describe their understanding of previous and successive steps in the process or control activities;
- demonstrate how they perform the activity or process control activity;
- describe what they are looking for to determine if there is an error (rather than simply asking them if they perform listed procedures and controls);
- explain what they do when they find an error;
- explain what kinds of errors they have found, what happened as a result of finding the errors, and how the errors were resolved;
- describe whether they have ever been asked to override the activity or controls and, if so, to describe the situation; and
- explain whether the transaction and the related process being discussed are typical of all transactions that flow through the process or whether other transactions follow a different process.

Question 4.3.120
Are IT systems included in walkthroughs?

Interpretive response: Yes. To fully understand the flow of transactions, it is necessary to understand how data enters an IT system, and is stored, processed and accumulated for use in the operation of controls and preparation of financial statements. It also is necessary to understand how data associated with the transactions flows through IT systems, including which applications, databases and other system components accept, maintain, manipulate and move the data. In other words, it is important to follow the transaction selected through the relevant IT systems, not around them.

Section 4.6 provides further discussion of IT specific considerations when performing a walkthrough.

Practical tip

A better practice is for relevant IT personnel to be part of the walkthroughs of business processes to enable a thorough understanding of the relevant IT systems to be obtained. This includes understanding the software or applications being used, the relevant network, database and application layers, and the related GITCs.

Question 4.3.130

Does obtaining a process understanding extend to service organizations?

Interpretive response: Yes. More and more entities use and depend on services provided by service organizations, and the COSO Framework recognizes this trend. It explicitly states that its goal is to address the extended business model of today's organizations – the entity itself, plus all service providers and other business partners who support the entity's control objectives.

The COSO Framework specifies that all relevant principles of internal control should be applied across that extended business model. Similarly, the SEC staff has stated that management's annual report on ICFR cannot be limited in its scope to exclude processes and controls performed by service providers engaged by the entity.

If services obtained from a third-party organization are part of the entity's financial reporting process, those services are part of the entity's ICFR. Management should consider the risks associated with the transactions processed by the service organization and the controls performed by them (and the entity itself) to manage those risks and determine how those controls affect the entity's ICFR.

The extent to which management addresses each service organization in their assessment of the effectiveness of ICFR (including obtaining an understanding of the business processes affected by the service organization and identifying the relevant risks and controls) depends on several factors, including:

- the significance of the transactions or information processed by the service organization to the entity's financial statements;
- the risk of material misstatement due to error or fraud associated with the business activities performed by the service organization;
- the nature and complexity of the services provided by the service organization and whether they are unique to the entity or highly standardized and used extensively by many;
- the extent of the delegation of authority to the service organization;
- the extent to which the entity's processes and controls interact with those of the service organization and whether the entity has controls in place that can independently verify that the objectives of effective ICFR are met; and
- the extent to which the entity depends on the internal controls of the service organization operating effectively.

Chapter 8 provides further discussion of service organizations' involvement in ICFR.

Question 4.3.140
Where does a walkthrough begin?

Interpretive response: A walkthrough begins where the transaction begins – in other words, where the transaction is initiated. For example, a walkthrough for the sales process begins where the customer submits an order.

Question 4.3.150
What parts of a process are included in a walkthrough?

Interpretive response: An understanding of the business process and the flow of transactions from initiation to reporting should be obtained for each relevant assertion of each significant account and disclosure that could cause the financial statements to be materially misstated. This includes how the transactions are initiated, authorized, processed and recorded.

For example, management would not just perform a walkthrough over the portion of the process related to the existence of inventory but would also need to include the portion of the process related to the accuracy and valuation of inventory, which could be a different part of the process.

Obtaining an understanding of the business process and flow of transactions from beginning to end is required for both routine processes, such as sales or procurement, as well as for significant unusual transactions, such as business combinations or impairment of goodwill, that could cause the financial statements to be materially misstated.

In addition, one business process may include several significant accounts and disclosures. For example, a revenue process for a commercial enterprise may cover not only revenue, but likely also cover such accounts as deferred revenue, accounts receivable and sales returns.

Question 4.3.160
How does management consider variations in processes when performing a walkthrough?

Interpretive response: There may be many different variations within a process, such as different revenue streams, order entry methods, payment methods or delivery methods. When determining whether the objectives of a walkthrough may be achieved through selection of a single transaction (versus multiple transactions), management considers whether any unique PRPs exist.

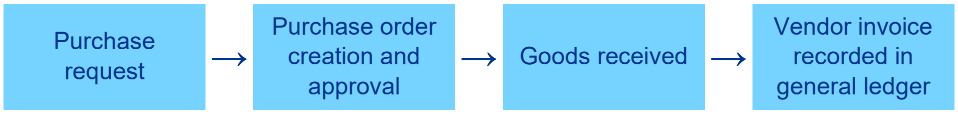
Management also considers the various data elements that may be used to determine the relevant assertions over the significant accounts associated with the business process that is the subject of the walkthrough. Various data elements may source from different places within and outside the entity and may require selection of multiple transactions within a process to achieve the objectives of an effective walkthrough.

The following example includes different scenarios where variations in the process effect the nature and extent of walkthroughs performed.

Example 4.3.10
Determining the scope of a walkthrough

Scenario 1: Purchasing process

Before performing a walkthrough related to the purchasing process, the internal audit manager considers how best to perform the walkthrough and what pertinent questions to ask of the process owners. She considers the risks inherent in the purchasing process and decides to choose a transaction that was already recorded in the general ledger. She follows that transaction through the following process by inspecting documentation and inquiring of various employees who participated in the processing of the transaction.


Purchase request
Purchase order creation and approval
Goods received
Vendor invoice recorded in general ledger

The following is a list of relevant questions posed to the process owners.

- What happens next in the process?
- Where does the information come from?
- Does the information always come to you the same way?
- Has anyone ever asked you to handle the transaction in a different manner?
- Are there differences in the way you process a purchase order depending on the item purchased? For example, do you process a purchase order for inventory different from one for office supplies?
- Who decides which general ledger accounts the transactions should be recorded in?
- Have you ever found an error, and if so, what did you do to address the error?

By asking these questions, the internal audit manager determines that there are different processes (and, therefore, likely different opportunities for misstatement) depending on what the entity is purchasing. She also determines that there are occasions when (for legitimate reasons) similar transactions go through different processes. Therefore, she identifies the need to walk through various iterations of the process to fully understand the different ways that transactions are processed. Only by performing this expanded walkthrough could she identify all relevant PRPs.

Scenario 2: Retail and online sales processes

A retailer sells a product on its website and through several retail locations. It is unclear whether both types of transactions go through the same or different processes, which may affect the PRPs to be addressed. In this case, it would be appropriate to select both an internet sales transaction and a retail location sales transaction for which to perform walkthroughs and follow each transaction until the two processes merge.

Scenario 3: Bank account origination process

A commercial bank offers a customer multiple options for initiating a transaction, such as a customer deposit account. This account can be opened by a customer through the bank's website, at a bank branch location or through the US mail. Regardless of the option the customer chooses, the bank receives the same information and processes that information in the same manner. Because there are no unique PRPs related to the different ways a customer deposit account may be opened, following a single transaction through the account origination process might achieve the objective of performing a walkthrough of that process.

Question 4.3.170

How does management consider multiple physical sites when performing a walkthrough?

Interpretive response: An entity may have multiple physical sites (e.g. warehouses or retail locations), which is not to be confused with multiple subsidiaries. These sites may or may not have control activities that are homogenous and/or centrally controlled and operated.

Homogeneous

Locations may have homogeneous control activities across multiple physical sites when there are consistent related IT systems and similar processes, PRPs and RMMs. They are also subject to the same entity-level controls. Careful consideration should be given in determining whether control activities at locations are homogeneous.

If multiple physical sites' control activities are determined to be homogeneous, it may be possible to conclude that walkthroughs at each location are unnecessary after considering:

- the effectiveness of the entity's risk assessment and monitoring processes;
- the effectiveness of entity-level controls developed by management in response to its risk assessment;
- the assessment of risk of controls failing in the process;
- the results of other procedures performed by management or internal audit relevant to the locations including compliance assessments and operational audits; and

- the knowledge obtained in the previous year's process understanding, including the nature and extent of any deficiencies within ICFR.

In most instances, it may be necessary to perform a walkthrough or other procedures at multiple physical sites to support the assertion that the control activities at the locations are in fact homogeneous. Determining homogeneity is a matter of judgment and requires careful consideration of the relevant facts and circumstances.

Centrally controlled

Multiple physical sites have control activities that are centrally controlled if transactions and related control activities for these sites are processed centrally based on information provided by each site.

If multiple physical sites are determined to have control activities that are centrally controlled, it may be most effective to perform a walkthrough at the central location. Based on the walkthrough, management determines whether the process at the central location sufficiently addresses the relevant risks at the individual physical sites.

Neither homogeneous nor centrally controlled

In the case of multiple physical sites where control activities are neither homogeneous nor centrally controlled, walkthroughs may need to be performed at each site that (individually or when aggregated with others) gives rise to the risk of a material misstatement of the entity's financial statements.

Question 4.3.180
Can control activities that were originally determined to be homogeneous not actually be homogeneous?

Interpretive response: At various points during the ICFR assessment, evidence may arise that suggests that control activities originally determined to be homogeneous may not actually be homogeneous. Such evidence may include:

- business understanding obtained in the current year that indicates that the processes and related controls are not consistently designed;
- differences in the design of controls at locations selected for direct testing as part of monitoring activities;
- deficiencies in the operating effectiveness at only one or some of the locations selected for direct testing as part of monitoring activities that are determined to be isolated to those locations; or
- indications from other sources (e.g. Internal Audit site visits that were not ICFR related) that the design of controls may be different or operating ineffectively at locations not selected for testing.

When contrary evidence arises, management considers whether more evidence is needed to affirm or disaffirm the original conclusion that the control activities are homogeneous.

Once sufficient evidence has been obtained, if management ultimately concludes the control activities are not homogeneous, the assessment of control activities at the individual locations may need to be reconsidered to determine if control activities at those locations are appropriately designed and operated. If exceptions are identified at a location(s), management should reconsider if the determination of homogeneity remains appropriate for **all** locations, not just the location(s) with the exception.

Question 4.3.190

How often is the understanding of a business process updated?

Interpretive response: On an annual basis, management should take appropriate steps to sufficiently:

- consider potential changes in the process, including the introduction of new IT systems or information, a change in the business environment or a change in key personnel; and
- update the process understanding and related documentation (e.g. flowcharts, narratives).

Various events and conditions that are relevant to the entity when preparing its financial statements may indicate that RMMs exist in a process or changes have occurred in the process. For example, a breach of loan covenants (event) may affect the presentation of the loans in the financial statements and require additional disclosures. For another example, changes in income tax laws or rates that affect the recognition and measurement of income taxes (condition) may indicate that RMMs exist when the entity applies the new tax laws or rates.

Many material weaknesses in ICFR originate from an inadequate risk assessment process to identify changes in a process. Processes change over time due to a variety of factors including changes in personnel, changes in the way transactions are processed, and changes in technology. As these changes occur, new PRPs may arise. If the new PRPs are not identified and managed through relevant controls on a timely basis, they may lead to undetected errors in the entity's financial reporting.

Even slight changes made to business processes over time, if they are not understood and assessed on a timely basis, can render the existing suite of controls (in the aggregate) inadequate and lead to a material weakness in the entity's ICFR.

As illustrated in Example 4.3.20, management may establish a policy and parameters in determining the extent of procedures necessary to update their understanding of a business process.

Example 4.3.20

Management factors risk into the extent of procedures performed to update the understanding of a business process

A manufacturing entity determines that it will classify each process (e.g. sales order process, treasury process) into categories based on the types of transactions performed, the degree of change from the prior year, the degree of judgment involved in the process, and the importance of the related significant accounts to the financial statements.

For processes related to sales and inventory that are believed to have a higher risk of changes in the processes, management decides to perform a walkthrough each year to update their understanding of the processes, determine the PRPs, and confirm that the controls in place are still appropriately designed and operating effectively.

For processes related to fixed assets, cash and prepaid expenses, management decides to perform an annual evaluation to determine whether any external or internal influences might have caused changes to the processes or presented new PRPs. If they determine that there are no such changes, a walkthrough is performed every two years instead of every year. Management documents the key inquiries made of process owners to corroborate their understanding and conclusion.

Question 4.3.200

How often are walkthroughs performed by management?

Interpretive response: As illustrated in Example 4.3.20, there may be some business processes for which management performs the walkthroughs on an annual basis due to higher risks of error or fraud present in those processes and/or the changes made to those processes. In contrast, there may be other business processes for which management performs the walkthrough every few years due to the insignificant nature of the risks related to those processes and management's determination that the processes were unchanged in the last year.

If a walkthrough is not performed over a business process by management, a robust assessment is crucial to determine there are no changes in the process that would affect the determination or PRPs and necessitate new or modified controls. Considerations in determining whether a walkthrough should be performed in the current year include:

- there is a significant change to the entity's process in the current period as compared to the prior period;
- a change in accounting standard or accounting policy that affects the process;
- new control owner(s) or turnover of control operator(s) in the process;

- a history of audit misstatements in the process;
- a history of control deficiencies in the process;
- the process contains a higher risk of error or fraud; and/or
- the process to record a significant unusual transaction.

4.4 Considerations related to period-end financial reporting, including preparation of disclosures, in obtaining a process understanding and identifying risk points

Question 4.4.10

Does obtaining a process understanding apply to the period-end financial reporting process, including preparation of disclosures?

Interpretive response: Yes. The period-end financial reporting process is a critical process that exists for all entities. The period-end financial reporting process includes the activities an entity performs to close the books and make post-closing adjustments when preparing the individual financial statements (e.g. balance sheet, statement of income) and related disclosures (collectively referred to as the financial statements). This process generally operates after the business processes and related process control activities designed to record individual transactions have been executed.

The period-end financial reporting process is the last process to occur before the financial statements are issued. Therefore, it is important for the entity to have well designed and effective period-end financial reporting controls as errors or fraud in the period-end financial reporting process may override effective control activities that occur throughout the entity's other processes.

Question 4.4.20

What are the processes and procedures in the period-end financial reporting process?

Interpretive response: The process starts with the general ledger that is used to record the accumulation of transactions from all business processes. The process ends when the entity issues or reports its final financial statements. The period-end financial reporting process includes:

- the consolidation process (if applicable);
- foreign currency translation (if applicable);
- selection and application of accounting policies or principles;

- initiating, authorizing, recording and processing of journal entries and other adjustments (see section 4.7); and
- preparation, review and approval of individual financial statements and related disclosures (see Question 4.4.40).

Question 4.4.30

What is included as part of the understanding of the preparation, review and approval of the financial statements, including disclosures?

Interpretive response: Understanding should include, among others, the process of preparing the current and comparative period financial statements, identifying financial statement disclosure requirements (e.g. earnings per share), identifying and assessing reportable segments, identifying non-routine transactions requiring disclosure in the notes to the financial statements, preparing financial statement disclosures, assessing going concern assumptions, and identifying and assessing the impact of any subsequent events.

Question 4.4.40

How is the understanding of the preparation of financial statement disclosures obtained?

Interpretive response: Obtaining an understanding of the process to prepare financial statement disclosures typically straddles both business processes and the period-end financial reporting process.

Financial statement disclosures usually use information that flows through the underlying business processes (e.g. sales information that will be needed to prepare the revenue disclosures required by ASC 606). As such, obtaining an understanding of the information, the PRPs related to the input, integrity and extraction or manipulation of the information and the related controls is best integrated with the understanding of the related business process. At the same time, inclusion of the information into the financial statements in the form and content prescribed by the accounting standards (e.g. revenue disaggregated into categories that depict how revenue and cash flows are affected by economic factors) typically requires further analysis, breakdown or aggregation of the data. This may be part of the period-end financial reporting process that has incremental PRPs from the underlying business process.

Question 4.4.50
Is a walkthrough of the period-end financial reporting process the same as other business processes?

Interpretive response: No. For most business processes, a walkthrough involves following a 'single transaction' from initiation to the recording of the transaction in the entity's transaction processing systems. However, a walkthrough of the period-end financial reporting process and its sub-processes will not necessarily involve following a 'single transaction' through the process in the same way, because the period-end financial reporting process involves the entering of transactions into the entity's general ledger and consolidation systems and the reporting of the accumulation of transactions in the financial statements, including related disclosures.

Therefore, a walkthrough of the period-end financial reporting process follows the flow of data from the general ledger and consolidation systems to the consolidated financial statements and related disclosures for a particular financial reporting period.

Practical tip

To understand the complete flow of information, it may be effective to confirm management's understanding by looking at the final financial statements, including disclosures, and tracing the consolidated information back to the respective information sources.

4.5 Considerations related to estimates in obtaining a process understanding and identifying risk points

Question 4.5.10
What is an accounting estimate?

Interpretive response: An accounting estimate (or 'estimate') is a measurement or recognition in the financial statements of (or a decision to not recognize) an account, disclosure, transaction or event that generally involves subjective assumptions and estimation uncertainty.

Accounting estimates vary widely in nature and management makes them when monetary amounts cannot be directly observed.

Question 4.5.20

How do estimates pose a risk to the financial statements?

Interpretive response: By their nature, accounting estimates, and their elements, are subject to factors that inherently drive risks of misstatement, such as estimation uncertainty, complexity and subjectivity. These same factors also make estimates susceptible to management bias.

Estimates can vary in their degree of complexity but can involve complex processes and methods.

Question 4.5.30

What is estimation uncertainty?

Interpretive response: Estimation uncertainty is the susceptibility of an accounting estimate and related disclosures to an inherent lack of precision in measurement. Estimation uncertainty is an inherent risk factor and arises when there are constraints on the availability of knowledge (or data) necessary to develop an estimate, which limits the precision of an estimate.

As estimation uncertainty increases, so too does the risk of material misstatement to the financial statements.

'Estimation uncertainty' is also referred to as 'measurement uncertainty.'

Question 4.5.40

Where does estimation uncertainty arise in accounting estimates?

Interpretive response: Estimation uncertainty is commonly associated with the assumptions used to develop an accounting estimate; however, the other elements of an accounting estimate can also give rise to estimation uncertainty.

For example, there may be subjectivity or judgement in determining an appropriate method/model to use in determining an accounting estimate, leading to estimation uncertainty. There also may be subjectivity and judgement in selecting a data set or deciding if it is appropriate for certain data to be excluded from the population, which can lead to estimation uncertainty.

Estimation uncertainty can also be related to an accounting estimate through the aggregate effect of the uncertainty that arises through the individual elements.

Question 4.5.50
What is 'subjectivity'?

Interpretive response: Subjectivity is the quality of being based on or influenced by personal feelings, tastes or opinions. In accounting estimates, subjectivity is an inherent risk factor and reflects the inherent limitations around the knowledge or data reasonably available related to an accounting estimate.

As subjectivity increases, so does the risk of material misstatement to the financial statements.

In some cases, the applicable financial reporting framework reduces the subjectivity by providing requirements for making the judgment (e.g. the minimum amount within a range is recorded for a loss contingency when no amount within a range is a better estimate than any other amount).

Management judgment is generally necessary in determining the appropriateness of the elements used to make an accounting estimate, which can lead to management bias. As subjectivity increases, so does the susceptibility of the elements to management bias.

Question 4.5.60
What is 'complexity'?

Interpretive response: Complexity is the quality of being intricate or complicated. In accounting estimates, complexity is an inherent risk factor and stems from how an accounting estimate is made.

As complexity increases, so too does the risk of material misstatement to the financial statements.

Question 4.5.70
What is 'management bias' and how does it affect accounting estimates?

Interpretive response: Management bias can be thought of as a lack of neutrality by management in preparing an accounting estimate. Management bias is considered with the selection of the various elements of an estimate, as it relates to an estimate, and the aggregate of all accounting estimates.

Management bias can be unintentional, or it can be intentional (fraud).

Question 4.5.80

What should management consider when identifying accounting estimates within their processes?

Interpretive response: As part of obtaining an understanding of a business process, management should identify if there are estimates or changes in estimates. This includes consideration of:

- the entity's transactions or other events and conditions that may give rise to the need for, or changes in, accounting estimates to be recognized or disclosed in the financial statements, including conditions that affect the recoverability of assets;
- the requirements of the applicable financial reporting framework related to accounting estimates (including the recognition criteria, measurement bases, and the related presentation and disclosure requirements) and how they apply in the context of the nature and circumstances of the entity and its environment; and
- regulatory factors relevant to the entity's accounting estimates, including, when applicable, regulatory frameworks.

Management should have processes and controls in place to identify those transactions, events and conditions that may give rise to the need for accounting estimates to be recognized or disclosed in the financial statements.

Question 4.5.90

What controls should the entity have over the identification and oversight of estimates?

Interpretive response: The entity should have entity-level controls in place related to estimates that address:

- how the entity's board of directors exercises oversight over management's process for making accounting estimates;
- how management identifies the need for, and applies, specialized skills or knowledge related to accounting estimates, including with respect to the use of a specialist and other qualified external information sources (e.g. a pricing service for information used to price investment securities); and
- how the entity's risk assessment process identifies and addresses risks related to accounting estimates, including susceptibility to management bias and fraud.

See chapter 2 for further considerations for entity-level controls.

Question 4.5.100
What are the primary elements of an estimate?

Interpretive response: Estimates have three primary elements.

Methods	Assumptions	Data
A method is a measurement technique used by management or management's specialist to make an accounting estimate in accordance with the relevant measurement basis. A method may include application of a model or models.	Assumptions represent judgments, decisions or assessments made in areas that involve a degree of subjectivity or uncertainty. Assumptions that are important to the recognition or measurement of the estimate are referred to as 'significant assumptions.'	Data is equivalent to 'information.' Accordingly, data may be comprised of multiple 'data elements.' In the case of accounting estimates, data elements may be used as either a direct input to the method or model or in developing an assumption.

As noted in Question 4.3.10, Principle 7 of the COSO Framework requires understanding the business process activities and the flow of data from initiation to reporting. When a business process contains an estimate, the understanding of the business process activities includes obtaining an understanding of each of the elements of the estimate.

Obtaining an understanding of each of the elements of the estimate provides important information used in identifying and assessing RMMs and the related PRPs within the estimate. Management then designs appropriate control activities to address the identified PRPs.

Question 4.5.110
What does management understand related to the development of estimates?

Interpretive response: When a business process involves an estimate, management should understand the process of how an estimate is developed including:

- how the relevant methods, assumptions, or data are identified, the sources of the relevant methods, assumptions and data (including IT systems and IT layers), and how changes that are appropriate in the context of the applicable financial reporting framework to the relevant methods, assumptions or data are identified;
- how the entity:
  - selects or designs and applies the methods used, including the use of models;

- selects the assumptions to be used, including consideration of alternatives, and identifies relevant assumptions; and
- selects the data to be used;

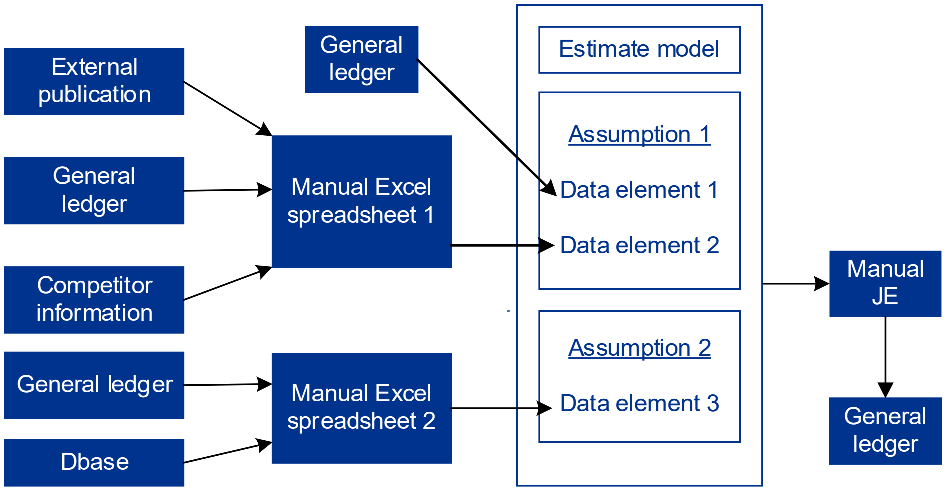
- how and when a retrospective review of the estimate is performed and how the entity responds to the results of the retrospective review;
- the degree of estimation uncertainty, including if there is a range of possible measurement outcomes;
- how the estimation uncertainty is addressed, including selecting a point estimate and related disclosures for inclusion in the financial statements;
- how the entity identifies when to use and apply specialized skills or knowledge related to accounting estimates; and
- how the entity analyzes the sensitivity of its relevant assumptions to change for critical accounting estimates.

This will assist management in determining where there are PRPs within the estimate that require a controls response.

Example 4.5.10

Documentation of understanding of the process for developing accounting estimates

Management may choose to include a diagram of the method/model, assumptions and data that are used to develop an accounting estimate similar to the following.



A diagram can help summarize the key aspects of how management develops and records an accounting estimate.

Question 4.5.120
How are risks identified as part of estimates?

Interpretive response: Once management obtains a granular understanding of how the estimate is developed (see Question 4.5.110), the following steps should be performed to identify the risks related to the process to determine an estimate.

Step 1	Identify the method and model used to measure the estimate. There may be multiple methods and models used to develop an estimate that management may consider when selecting a point estimate or range.
Step 2	Identify the population of assumptions that are used to measure the estimate.
Step 3	Identify the population of data that is used to measure the estimate – including data that is used directly in the method and data that is used as an assumption or to develop an assumption.
Step 4	Consider the quantitative and qualitative inherent risk factors and other risks (see Question 4.5.130), and whether the process to determine the estimate gives rise to an RMM. When doing so, consider the contribution of risk that each element contributes to the RMM for the estimate, individually and in combination with other elements.
Step 5	Identify the PRPs for each method and model, assumption or data element where an RMM was identified.

For more complex estimates like business combinations, this process can take time and likely will result in the identification of many elements and PRPs.

Once all PRPs are identified, management designs process controls activities to address the PRPs and GITCs to address any related risks arising from IT (RAFITs). The design of the process control activities (see chapter 5) and GITCs (see chapter 7) related to estimates follow the same criteria as other control activities.

Practical tip

To assist in designing control activities around estimates and ensuring that all identified PRPs associated with the elements individually and in combination with one another are identified and that related control activities are designed and implemented, management may use a template or spreadsheet to perform the steps above to identify the population of elements, those elements that result in an RMM and the related PRPs, and then map the PRPs to the related control activities.

Example 4.5.20
Understanding elements and identifying PRPs in an estimate

Steps 1-3: Management uses the straight-line method for the estimation of depreciation expense and identifies the following individual elements within the estimate.

Primary element	Method, assumption or data element
Method/model	Straight-line method/Automatically calculated in the Oracle Fixed Asset System
Assumption	Useful life
	Residual value
Data	Cost of asset
	In-service period
	Asset classification
	In-service date

Step 4: Management considers the contribution of risk that each of the above elements contributes to the RMM for the estimate, individually and in combination with other elements. For purposes of our example, management determines that there is an RMM associated with the application of the methods, assumption and data when used in the model.

Step 5: One of the PRPs management identifies is the following: The Fixed Asset system is not configured to accurately calculate depreciation expense.

Management is responsible for having appropriately designed controls in place and confirming they are operating effectively to address the PRP.

Question 4.5.130
What are the additional inherent risk factors considered in relation to accounting estimates?

Interpretive response: Management evaluates additional risk factors when determining if there is a RMM associated with an accounting estimate, which include:

- 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;

- the degree of uncertainty associated with the future occurrence or outcome of events and conditions underlying the relevant assumptions;
- if forecasts are important to the estimate, the length of the forecast period and degree of uncertainty about 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.

Question 4.5.140

What does management consider when evaluating whether the method may give rise to an RMM for the estimate?

Interpretive response: When evaluating whether the method may give rise to an RMM for the estimate, individually or in combination with the other elements, management considers the degree of complexity, subjectivity and estimation uncertainty associated with the method. There is a risk that the method selected is inappropriate.

Management should consider the following questions.

- Is the method appropriate to use for measurement under the applicable financial reporting framework (individually and in combination with the other elements used)?
- If the method used is not prescribed by the applicable financial reporting framework, is the method typically used for determining the estimate for the industry or business that the entity operates?
- If neither of the above, is the method reasonable to use under the facts and circumstances?
- Does the method rely on IT systems, and if so, what are the applicable IT system layers and how do they apply to the method?
- What are the assumptions and data used in the method? See Questions 4.5.160 and 4.5.170.
- What is the frequency at which an estimate is calculated, e.g. annually, every quarter, every quarter on a one-month lag, one-week lag?
- Is a service organization used, and if so, how does it affect the method?
- Does management use a specialist or third party (other than a specialist) to develop or select the method?

Management should also consider the following questions that may help when identifying bias or fraud risks factors.

- Are there alternative methods and were they considered, if available?
- Are judgments about which method(s) to use consistently applied?
- If the method has changed from the method used in the prior period, is the basis for change reasonable given the facts and circumstances, timely made, and appropriate to use for measurement?
- Are adjustments made to the output of the model appropriate and supported by sufficiently relevant and reliable information (see chapter 6)?
- Is there is a lag period between the calculation of an estimate and the reporting date in the applicable financial reporting framework?

Careful consideration of the above questions can help management identify the PRPs where an RMM associated with the selection of the method used in developing an estimate may occur. Key decisions about the selection of the method(s) and controls that address the risks should be documented.

For example, there are alternative methods available to management for determining the fair value of a reporting unit in a goodwill impairment analysis. There is a point in the process where management selects which of these methods to use, e.g. an income and/or market approach and how to weight them if multiple methods are used. Accordingly, the selection of the method(s) may give rise to an RMM given the different options that are available and the judgments that must be applied in deciding which method(s) are appropriate to use.

Question 4.5.150

What does management consider when evaluating whether the model may give rise to an RMM for the estimate?

Interpretive response: When evaluating whether the model may give rise to an RMM for the estimate, management considers the degree of complexity associated with the application of the methods, assumptions and data when used in the model. There is a risk that the application is inappropriate.

Management should consider the following questions.

- Is the calculation of the estimate in accordance with the method selected?
- Is the calculation mathematically accurate?
- Has the integrity of the assumptions and data been maintained when used in the model?

Careful consideration of the above questions can help management identify the PRPs where an RMM associated with the application of the methods, assumptions and data when used in the model may occur. Key information about the application and controls that address the risks should be documented.

Continuing with the goodwill impairment analysis example, management has selected the discounted cash flow (DCF) income approach (the method) to develop the fair value of its reporting units. Application of the DCF method is performed using Microsoft Excel (the model). There is a point in the process where management inputs the assumptions and data into the Excel spreadsheet(s) either manually or automatically and the DCF is calculated based on the formulas that have been inserted into the cells within the spreadsheet(s). Accordingly, the input of the relevant assumptions and data into the Excel spreadsheet(s), the integrity of the assumptions and data when used in the various formulas and the mathematical accuracy of the calculation(s) may give rise to an RMM (e.g. the assumptions and data could be transposed when entered, the formulas could be inconsistent with the DCF method and/or the formulas could contain errors).

Question 4.5.160

What does management consider when evaluating whether an assumption may give rise to an RMM for the estimate?

Interpretive response: When evaluating whether an assumption may give rise to an RMM for the estimate, individually or in combination with the other elements, management considers the degree of complexity, subjectivity and estimation uncertainty associated with the assumption. There is a risk that the assumption selected is inappropriate.

Management should consider the following questions.

- Is the assumption appropriate/reasonable to use for measurement under the applicable financial reporting framework (individually and in combination with the other elements used)?

- If dependent on management's intent and ability, is the assumption consistent with the following factors?

  - the entity's history of carrying out its stated intentions;
  - the entity's written plans or other relevant documentation, such as budgets or minutes;
  - the entity's stated reasons for choosing a particular course of action;
  - the entity's ability to carry out a particular course of action, which includes consideration of whether:

    - the entity has the financial resources and other means to carry out the action;
    - legal, regulatory or contractual restrictions could affect the entity's ability to carry out the action; and
    - the entity's plans require the action of third parties and, if so, whether those parties are committed to those actions?

- Is the assumption consistent with other sources of information, including:

  - relevant industry, regulatory, and other external factors, including economic conditions;
  - the entity's objectives, strategies and related business risks;

  - existing market information; and
  - historical or recent experience, considering changes in conditions and events affecting the entity?

- If used in other estimates, is the assumption consistent or otherwise supported?

- Does the assumption rely on IT systems, and if so, what are the applicable IT system layers and how do they apply to the assumption?

- Is a service organization used, and if so, how does it affect the assumption?

- Does management use a specialist or third party (other than a specialist) to develop or select the assumption?

- What data is used to derive the assumption? See Question 4.5.170.

Management should also consider the following questions that may help when identifying bias or fraud risks factors.

- Are there alternative assumptions and were they considered, if available?

- Were judgments about which assumption(s) to use consistently applied?

- If the assumption was changed from that used in the prior period, what was the basis for change and is it reasonable given the facts and circumstances, made timely, and appropriate to use for measurement)?

- Is the assumption sensitive to variation?

- Does the assumption involve unobservable data or adjustments to observable data?

- Does the assumption rely on the entity's intent or ability to carry out specific course of action?

Careful consideration of the above questions can help management identify the PRPs where an RMM associated with the selection of an assumption used in developing an estimate may occur. Key decisions about the selection of the assumption(s) and controls that address the risks should be documented.

Continuing with the goodwill impairment analysis example, when determining the fair value of its reporting units using the DCF model, there is a point in the process where management estimates the future cash flows for a certain discrete projection period. Accordingly, the selection of the revenue growth assumption for a particular reporting unit, among other assumptions, may give rise to an RMM, e.g. the revenue growth assumption could be inconsistent with the same assumption when used in other estimates for the entity, it could be inconsistent with management’s intent and ability for operating the reporting unit, or it could be inconsistent with recent conditions or events affecting the reporting unit.

Question 4.5.170

What does management consider when evaluating whether the data may give rise to an RMM for the estimate?

Interpretive response: When evaluating whether the data may give rise to an RMM for the estimate, individually or in combination with the other elements, management considers the degree of complexity, subjectivity and estimation uncertainty associated with the data. There is a risk that the data selected is inappropriate.

Management should consider the following questions.

- How are the data and data elements used, including what is the source of the data?
- Is the data appropriately understood or interpreted by management?
- Is the data sufficiently relevant (i.e. sufficiently precise and detailed), to use for measurement under the applicable financial reporting framework (individually and in combination with the other elements used)?
- Is the data sufficiently reliable, which includes:
  - If internal data, is it complete and accurate?
  - If external and not a source document, is it from a reputable, qualified, and objective source?
- Does the data rely on IT systems, and if so, what are the applicable IT system layers and how do they apply to the data?
- Is a service organization used to develop or select the data, and if so, how does it affect the data?
- Does management use a specialist or third party (other than a specialist) to develop or select the data?

Management should also consider the following questions that help when identifying bias or fraud risks factors.

- Is there alternative data and was it considered, if available?
- Were judgments about which data to use consistently applied?
- If the data was changed from that used in the prior period, what was the basis for change and is it reasonable given the facts and circumstances, made timely, and appropriate to use for measurement?

Careful consideration of the above questions can help management identify the PRPs where an RMM associated with the data used in developing an estimate may occur. Key decisions about the selection of the data and controls that address the risks should be documented.

Continuing with the goodwill impairment analysis example, when determining the fair value of its reporting units using the DCF method, there is a point in the process where management must decide which data to use either directly in the method or in an assumption. Accordingly, the selection of the carrying value of the reporting unit, among other data, may give rise to an RMM, e.g. the carrying value of the reporting unit could have nonoperating assets or liabilities reflected in the carrying amount of the reporting unit, or equity method investments that would result in adjustments to the fair value of the reporting unit.

Question 4.5.180

How might management address estimation uncertainty?

Interpretive response: Management addresses estimation uncertainty by developing controls over the:

- selection of an appropriate point estimate; and
- ensuring appropriate disclosures are made in their financial statements regarding estimation uncertainty.

The point estimate is the amount selected by management for recognition or disclosure in the financial statements.

Said another way, the point estimate is the output of management's process to record or disclose an estimate in the financial statements after all data and assumptions have been selected and applied to the method/model, including any adjustments to the output method/model. This process includes management considering where estimation uncertainty, subjectivity and/or complexity affects the elements of an estimate and the resulting range of measurement outcomes.

To select a point estimate, management may:

- record the output of a model directly in the financial statements; or
- before recording the point estimate in the financial statements:
  - adjust the output of the model;
  - weight the outputs of multiple models; or
  - select from within a range of possible outcomes.

As part of addressing estimation uncertainty, management considers the range of possible outcomes, as well as other specific matters and designs controls to address and consider these matters, such as:

- alternative methods, relevant assumptions or sources of relevant data that are appropriate in the context of the applicable financial reporting framework;

- possible alternative outcomes, e.g. performing a sensitivity analysis to determine the effect of changes in the data or assumptions on an accounting estimate; and

- the outcome of accounting estimates made in previous periods, responding to differences.

Question 4.5.190

How might the applicable financial reporting framework affect the related disclosures regarding estimation uncertainty?

Interpretive response: The applicable financial reporting framework may prescribe disclosures or disclosure objectives related to accounting estimates that:

- describe the amount as an estimate;
- explain the nature and limitations of the process for making an estimate, including the variability in reasonably possible outcomes;
- describe significant accounting policies related to an accounting estimate;
- describe significant or critical judgments, including significant forward-looking assumptions or other sources of estimation uncertainty;
- describe the method of estimation used, including any applicable model and the basis for its selection; and
- describe the information that has been obtained from models, or from other calculations used to determine estimates recognized or disclosed in the financial statements, including information relating to the underlying data and assumptions used in those models.

Depending on the circumstances, relevant accounting policies may include matters such as the specific principles, bases, conventions, rules and practices applied in preparing and presenting accounting estimates in the financial statements. In certain circumstances, additional disclosures beyond those explicitly required by the financial reporting framework may be necessary to achieve fair presentation, or in the case of a compliance framework, for the financial statements not to be misleading.

Management is responsible for implementing properly designed controls to support the appropriate disclosure of estimates in accordance with the applicable financial reporting framework.

Question 4.5.200

What are common PRPs and controls related to whether disclosures for accounting estimates conform to the applicable financial reporting framework?

Interpretive response: PRPs related to whether disclosures for accounting estimates conform to the applicable financial reporting framework are entity specific; however, given the nature of the risk, PRPs may include:

- management has not taken the appropriate steps to understand the required disclosures;
- management's understanding of the disclosure requirements is incorrect;

- management has not taken the appropriate steps to make the disclosures; and
- how management made the disclosures is incorrect.

To address the related PRPs, the entity may have a control that evaluates the disclosure requirements for an accounting estimate to determine what disclosures are required under the financial reporting framework. Additionally, the entity may have a control that reviews the disclosures individually and, in the aggregate, to validate that the disclosures are accurate, complete and fairly presented in accordance with the financial reporting framework.

Question 4.5.210

When might management use specialists or third parties (other than specialists) in developing an accounting estimate?

Interpretive response: Management may choose to involve specialists or third parties (other than specialists) when they lack the knowledge or skills necessary, especially when:

- the matter requiring estimation is very specialized;
- the financial reporting framework requires a method/model that is very technical by nature; or
- the transaction or event requiring an accounting estimate doesn't occur frequently or is unusual.

Question 4.5.220

Are the risks for estimates different if management uses a specialist?

Interpretive response: No. When management uses a specialist in the development of an estimate, there is no difference in how risks are identified or controls are developed to address the risks.

For example, with a business combination, management may provide historical customer data to a specialist for them to develop an attrition rate. The specialist will perform modifications to the data and then will calculate the attrition rate based on that data. In addition, they will use the attrition rate in the calculation of fair value. Management is responsible for the completeness and accuracy of the data being used in the attrition rate calculation, including the risks related to the manipulation and the calculation of the attrition rate. Management is also responsible for the attrition rate that was developed being properly transferred into the fair value calculation, the method used to calculate the attrition rate and the mathematical accuracy of the calculation.

Practical tip

Whenever a new estimate is developed, such as a business combination estimate, management should develop appropriate control activities *during* the process as opposed to trying to put control activities in place *after* the estimate's development, with a focus on the completeness and accuracy of the information used.

Question 4.5.230

Does the entity identify risks over data generated by a specialist specifically for the entity's use in an estimate?

Interpretive response: Yes. Data generated by specialists for the entity's use in an estimate is generally calculated using external or internal information provided by management. For example, mortality tables created specifically for an entity typically use historical entity-specific data. As it is developed specifically for the entity's use, it is considered internal information (see Question 6.4.10). Therefore, to address the reliability of the mortality tables, the completeness and accuracy of the information used in the model to create the table, as well as the end user computing risk in the model (i.e. mathematical accuracy, manipulation risk) need to be addressed. In some cases, management can obtain the models and calculations to have control activities over these risks. However, in other cases a specialist's model is proprietary. Even when this is the case, management is still required to determine the completeness and accuracy of the data.

This discussion is relevant to information developed by both internal and external specialists. For example, if the entity's own engineering department calculates an estimated cost to rebuild a building as part of a fair value estimate, the risks around the data, assumptions and the model used would need to be considered and addressed consistent with an estimate developed by the entity's accounting department or by an external valuation specialist hired by the entity.

Practical tip

Other individuals in the entity with specific knowledge and expertise may assist the accounting team with developing an estimate used in financial reporting. These individuals typically are unfamiliar with the requirements for controls. As such, it is management's responsibility to verify that process control activities are being performed and the appropriate documentation is retained to evidence the design and effective operation of the process control activities (consistent with chapter 5) and the use of information in those controls.

4.6 IT considerations when obtaining a process understanding and identifying risk points

Question 4.6.10
What are IT considerations when obtaining a business process understanding?

Interpretive response: IT considerations include understanding:

- the overall IT environment and risks that may exist at the entity level; and
- the flow of transactions through each relevant financial statement process, including through IT systems.

Question 4.6.20
Why is understanding the overall IT environment important?

Interpretive response: It is important to understand the overall IT environment to properly identify IT risks at the process level. This is because flowcharts or narratives that document the flow of information through a particular process are activity-based. As a result, they often do not fully articulate the multiple layers of IT embedded in the process, or the controls management has in place to address the risks, including the completeness and accuracy of relevant data elements flowing through the process.

Question 4.6.30
What is a better practice for documenting the understanding of IT systems?

Interpretive response: An understanding of IT systems used by the entity, including how information flows into, through, and out of the relevant IT systems, may be facilitated using ISDs.

ISDs are not flowcharts; rather, they are diagrams that depict the different layers of an entity's IT environment. ISDs show relevant applications, databases, operating systems and other network infrastructure. In addition, they will often show how service organization systems interact with the entity's internal IT systems.

The ISD is a diagram of the IT systems and a framework that helps management and external auditors gain an adequate understanding of IT when walking through a business process to identify relevant PRPs. See Example 7.2.20.

Question 4.6.40
What is included in an ISD?

Interpretive response: The ISD considers the application, the database that stores the data and the underlying operating systems, including IT components. There may be additional components relevant to the ICFR assessment, such as scripts, interfaces and customized application programming interfaces.

Each aspect of the ISD is important for purposes of management and the external auditors:

- obtaining an adequate understanding of the business processes that rely on IT;
- identifying relevant PRPs; and
- informing their judgment when it comes to identifying the relevant GITCs that support the automated controls that are relied on in the ICFR assessment to mitigate PRPs identified within each business process.

Question 4.6.50
Is management required to identify IT risks at the process level?

Interpretive response: Yes. Understanding the way IT is used in the process and identifying and addressing IT risks is not optional.

The entity must identify and document the relevant PRPs in the process at the assertion level where there is a reasonable possibility that these PRPs could result in or contribute to a material misstatement. This includes the PRPs related to IT. Failure to sufficiently understand IT risks is a deficiency that needs to be evaluated for severity and could result in a material weakness.

Walkthroughs and other procedures can provide an understanding of how IT affects the entity's flow of information and allows management and the external auditors to consider IT risks (e.g. a PRP related to the data as it flows through the IT system) when identifying likely sources of misstatement. There is a potential PRP related to the completeness and accuracy of data whenever:

- data enters the system;
- data is stored and can be accessed in the system or a database;
- data is moved from one system to another; and
- data is summarized, accumulated or subjected to calculations.

When performing walkthroughs, there is no requirement to review the IT system/application code. Ordinarily, the walkthrough can be completed by interviewing the relevant process owners, inspecting system documentation, and tracing a transaction through the process. However, because there is often complexity involved with IT infrastructure, both management and the external auditors should seek assistance from someone with the proper IT skill set when planning and/or executing walkthroughs of processes that rely on IT.

Chapter 7 provides further discussion of IT control activities.

Question 4.6.60
What effect do GITCs have on IT at the process level?

Interpretive response: The effectiveness of GITCs has a pervasive effect on automated controls or manual controls that rely on information from IT systems at the process and transaction level, and within entity-level controls. Because of this, it is important to consider GITCs when assessing IT risks.

Chapter 7 provides further discussion of IT control activities.

4.7 Considerations for journal entries and other adjustments while obtaining a process understanding and identifying risk points

Question 4.7.10
Does obtaining a process understanding apply to the journal entry process?

Interpretive response: Yes. Management should understand business processes all the way through the recording of journal entries.

Question 4.7.20
What are potential risks associated with journal entries and other adjustments?

Interpretive response: The following table captures potential risks associated with journal entries and related questions for management in understanding the process of recording journal entries and identifying related PRPs that require controls that are appropriately designed and operated.

Potential risks	Questions for management
The existence of transactions underlying journal entries and other adjustments	How does management determine that each automated and manual journal entry and other adjustment represents a valid transaction that is appropriately

Potential risks	Questions for management
	supported (i.e. what is management's process for obtaining appropriate approval of journal entries)?
The accuracy of journal entries and other adjustments	How does management determine that each automated and manual journal entry and other adjustment is recorded for the appropriate amounts and to the appropriate general ledger accounts or financial statement line items?
The completeness of journal entries and other adjustments	How does management determine that all automated and manual journal entries and other adjustments that should be recorded are recorded and are recorded in the correct period?
Management override of journal entries and other adjustments	How does management determine that all relevant automated and manual journal entries and other adjustments that have been posted have been appropriately approved and/or reviewed?

Section 5.14 discusses control considerations related to the risks associated with journal entries and other adjustments.

? Question 4.7.30

What are the risks related to automated and manual journal entries and other adjustments?

Automated journal entries

For automated journal entries, routine financial transactions can be initiated, authorized and accumulated via automated IT applications and posted through automated journal entries from subsystems to the general ledger. The risks generally relate to the proper transfer of journal entries between systems and the configuration of the IT application to post complete and accurate amounts during the appropriate period to the appropriate general ledger accounts.

Manual journal entries

Manual journal entries, which are initiated by an individual and manually entered into the system, or which at any point in the process may be modified or otherwise impacted by human intervention, would generally have an increased risk of misstatement related to management override risk and completeness, existence and accuracy risks.

Identifying all manual journal entries may be challenging and involves a detailed understanding of the IT applications involved in the journal entry process. Management should obtain an understanding of the sources of journal entries, how the system processes and posts journal entries, and the capability for manual changes to be made to journal entries during or after the posting process. For example, in an automated journal entry process, is it possible that manual changes could be made to the entry either during or after the posting process without being subject to additional review?

How an entity defines manual journal entries may also impact the relevant controls in place to address management override. For example, some IT applications are highly configurable such that many different types, sources, system users or transactions may involve manual intervention, and a simple or static definition of 'manual' may not be sufficient to identify all such journal entries. In this case, identifying the manual entries may require recurring monitoring and revision throughout the period.

Other adjustments

Other adjustments are adjustments to amounts reported in the financial statements that are not reflected in formal journal entries. For example, they may be reflected in consolidating adjustments, report combinations or reclassifications. Other adjustments may give rise to management override risk as well as completeness, existence and accuracy risks.

Question 4.7.40

What are additional considerations related to the approval of journal entries?

Interpretive response: When obtaining an understanding of the IT environment, management should consider who has access to post a journal entry, and whether approval of the journal entry is enforced within the IT system, manually obtained outside of the IT system, or through some combination of the two. Provided next are three common IT scenarios for approving journal entries.

Automated approval: Park and post

A park and post system restricts access to prepare and approve journal entries and requires authorized approval before posting. If operating effectively, this system typically offers the strongest control to address the risk of management override that journal entries are posted that have not been approved and/or reviewed before posting.

For this system, management needs to understand and assess whether access controls are in place to restrict access to separately prepare and approve journal entries. When evaluating this control, management considers whether the IT system is configured to prevent a preparer from approving their own journal entry and restrict edits to the entry after it has been approved.

Manual review and approval before posting: System restricts preparer and approver from posting

In this scenario, all manual journal entries are subject to a control involving review and approval by an individual who is separate from the preparer before posting the entry in the system.

Compared to a park and post system, there may be a greater risk of management override that journal entries are posted that have not been reviewed and approved. However, systematically restricting posting access to individual(s) other than the preparer and reviewer/approver, such as a data entry clerk who is segregated from the preparer and reviewer/approver, may help mitigate the risk.

When evaluating the sufficiency of controls under this scenario, management considers the following questions.

- Is the poster independent of the preparer and reviewer?
- Does the poster validate that the journal entry was approved before posting?
- Are access controls operating effectively to segregate access to prepare, review/approve and post journal entries?

Manual review and approval before posting: System does not restrict preparer and approver from posting

Similar to the previous scenario, all manual journal entries are subject to a control involving review and approval by an individual who is separate from the preparer before posting the entry in the system. However, a preparer or reviewer/approver has access to post journal entries. Therefore, a risk exists that an entry is posted that has not been subject to the review/approval control.

This scenario is riskier than the previous two scenarios, giving rise to the following additional considerations.

- Absent automated access controls, does the entity have policies to manually enforce segregation of duties between the preparer and reviewer/approver, and the reviewer/approver and poster?

- How does management address the risk that the journal entry review/approval has been circumvented?

- How does management know the population of journal entries subject to the manual review control is complete?

Key takeaways

- The understanding of a business process should cover the entire process, from initiation through recording in the financial statements, to identify all PRPs that may lead to the identification of key controls that address RMMs.
- While the period-end financial reporting process operates after business processes have been executed, understanding the process to prepare financial statement disclosures typically straddles both business processes and the period-end financial reporting process. Obtaining an understanding of the information used in disclosures is best integrated with the understanding of the related business process.
- When a business process includes an estimate, management's understanding of the process includes each of the elements of the estimate and identification of the related PRPs.
- Management's understanding of the process includes identification of IT systems as well as any information that is used in the process.
- Flowcharts are the best way to evidence process understanding and the flow of information, as well as document identification of PRPs and the key controls that address them.
- Management considers any changes to the business process and updates their process understanding at least annually, and whenever key changes occur.
- Business process understanding should include journal entries, including potential risks and approval considerations, to support accurate and complete financial records and mitigate the risk of management override.

5. Process control activities

Detailed contents

Examples

Questions

Examples

Questions

Examples

Questions

Examples

Questions

Questions

5.14.20 What types of control activities can address the risk of completeness associated with journal entries and other adjustments?

5.14.30 What types of control activities can address the risk of existence and accuracy associated with journal entries and other adjustments?

5.14.40 What is the risk of management override of controls?

5.14.50 How is the risk of management override addressed?

5.14.60 What types of control activities can address the risk of management override associated with journal entries and other adjustments?

5.14.70 Can other indirect control activities address journal entry risks?

5.15 Controls responding to going concern, significant unusual transactions, and related parties

Questions

5.15.10 Are there special considerations for control activities over the risk related to an entity's ability to continue as a going concern?

5.15.20 What are significant unusual transactions?

5.15.30 What kind of controls over SUTs does management need to have in place?

5.15.40 Why are there special considerations for controls related to SUTs?

5.15.50 Are there special considerations for controls over related party relationships and transactions?

5.15.60 What are examples of controls that may be in place to address the completeness of related parties?

5.15.70 When management asserts a transaction occurred at arm's length, what terms of the transaction is that assertion referring to?

5.15.80 What controls can management design and operate to address the risk of an inappropriate assertion that a related party transaction is at arm's length?

5.16 Controls executed on a sample basis

Questions

5.16.10 Can controls be designed to be executed on a sample basis?

5.16.20 When might it be appropriate to design controls to operate on a sample basis?

5.16.30 What method is used to select the sample size to be used in a control?

Example

5.17 Considerations when there are changes to controls

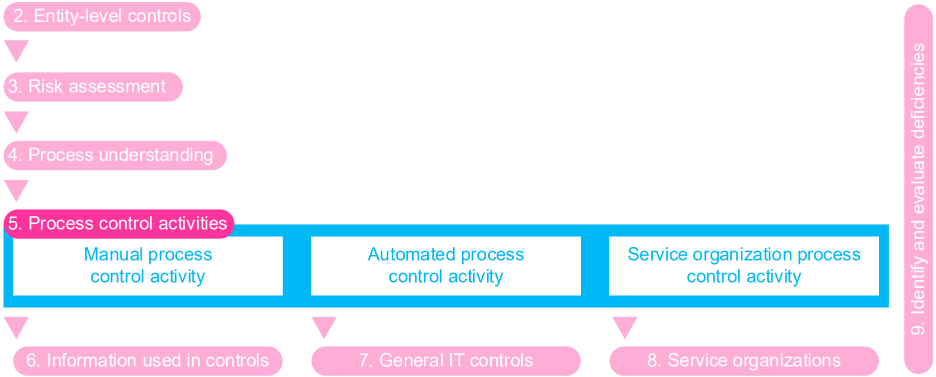
Questions

5.18 Monitoring procedures over process control activities

Key takeaways

5.1 Management’s ICFR journey

Control activities in the context of management’s ICFR are focused on identifying the policies and procedures established to mitigate (either directly or indirectly) risks of material misstatements (RMMs) in the entity’s business processes and the period-end financial reporting process. While all parts of management’s ICFR journey are important, the proper selection and development of control activities is vital to effective ICFR. See section 5.2 for more information. This chapter begins with an overview of the Control activities component of ICFR, which includes process control activities and GITCs. The focus of the chapter is process control activities. GITCs are addressed in chapter 7.


2. Entity-level controls
3. Risk assessment
4. Process understanding
5. Process control activities
Manual process control activity
Automated process control activity
Service organization process control activity
6. Information used in controls
7. General IT controls
8. Service organizations
9. Identify and evaluate deficiencies

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).

An entity’s ICFR is effective when it provides reasonable assurance that its financial statements are reliable and prepared in accordance with the applicable financial reporting framework. Accordingly, process control activities should be designed and operated at a ‘would’ level of assurance – they ‘would’ (i.e. probably will) mitigate an identified PRP and, therefore, prevent, or detect and correct on a timely basis, a material misstatement in the financial statements. See section 5.3 for more information.

The following considerations in designing a process control activity are a central focus of this chapter.

Consideration	Description
Control objective	The objective of a process control activity is the risk it is intended to mitigate - i.e. the relevant PRPs the control activity addresses. All other considerations involved in designing a process control activity are driven by this objective. See section 5.5 for more information.
Nature and type of control	'Nature' refers to whether the process control activity is manual or automated. 'Type' refers to whether the process control activity is preventive or detective. See section 5.6 for more information.

Consideration	Description
Frequency	An important consideration in determining the appropriate frequency of the control's operation (e.g. annually, daily, recurring, ad hoc) is whether it would achieve its objective in a timely manner. See section 5.7 for more information.
Authority and competence of the control operator	If the control operator does not have the requisite authority and competence to operate (and, if necessary, correct the results of) a manual process control activity, the control cannot achieve its objective (i.e. it would be ineffective). See section 5.8 for more information.
Judgment involved	A process control activity must consider the judgment and subjectivity involved in achieving its objective and setting the appropriate parameters for identifying and evaluating outliers. See section 5.9 for more information.
Level of precision	The level of precision is essentially the size of a potential misstatement the control activity would prevent, or detect and correct on a timely basis, when it operates effectively. A control is deemed to be sufficiently precise when the operation would prevent or detect a material misstatement. See section 5.10 for more information.
Investigation and resolution process	A manual process control activity should include appropriately designed and documented steps performed by the control operator to investigate and resolve outliers. See section 5.11 for more information.
Information used in the performance of the process control activity	Information is usually used when performing a manual process control activity (e.g. system reports, manually prepared spreadsheets, queries). Assessing the relevance and reliability of this information is critically important to ICFR, because controls that rely on information cannot achieve the control objective and address the related PRP if the information is not relevant and reliable. See chapter 6 for more information.

Given their nature, additional considerations may apply to the design and operation of process control activities related to the following:

- **fraud risks,** such as the misappropriation of assets, fraudulent financial reporting, corruption and other illegal acts, and management override of controls (see section 5.13 for more information);
- **journal entries and other adjustments,** which may be used as part of management's override of controls (see section 5.14 for additional information); and
- **going concern, significant unusual transactions and related parties,** such as considerations related to:
  - forecasts used in management's going concern assessment;
  - the potential for management to be incentivized to achieve a specific accounting treatment for a significant unusual transaction; and

  - identifying related parties, transactions with related parties and whether such transactions occur on an arm's length basis (see section 5.15 for more information).

This chapter also discusses whether controls can be executed on a sample basis (see section 5.16) and how changes in controls affect an entity's ICFR (see section 5.17).

This chapter ends with discussion on how the effectiveness of process control activities is monitored by the entity, including the use of direct testing involving reperformance, inspection and/or observation of the control together with inquiry (see section 5.18). If it is determined that a process control activity is ineffective in its design and/or operation, management concludes a deficiency exists and performs the necessary evaluation and remediation activities (see chapter 9).

While the focus of this chapter is on process control activities, there are multiple concepts discussed that are applicable for entity-level controls and GITCs as well. The following terminology is used in this Handbook:

- **controls** include entity-level controls and control activities; and
- **control activities** include process control activities and GITCs.

Abbreviations

We use the following abbreviations in this chapter.

ACL	Allowance for Credit Losses
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CUEC	Complementary user entity control
GITC	General IT control
ICFR	Internal control over financial reporting
PCAOB	Public Company Accounting Oversight Board
PRP	Process risk point
RAFIT	Risk arising from IT
RMM	Risk of material misstatement
SEC	Securities and Exchange Commission
SOC	System and Organization Controls

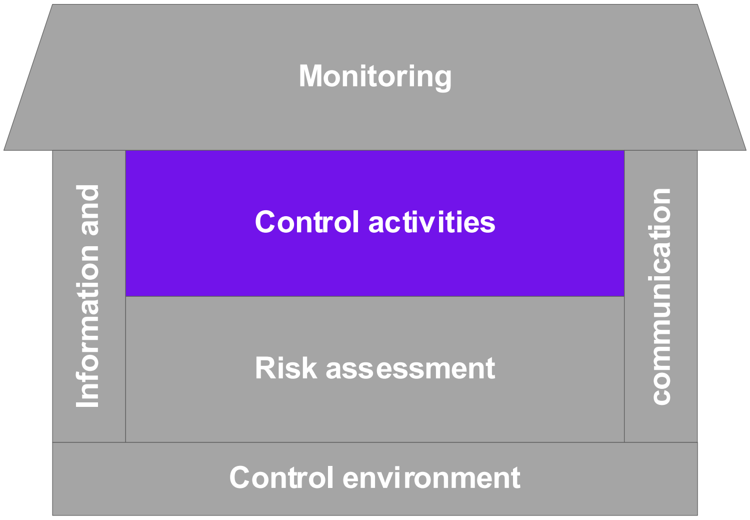
5.2 Control activities component of ICFR

Question 5.2.10
What is the control activities component of ICFR?

Interpretive response: Per the COSO Framework: "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."

Question 5.2.20
What is the relevance of the control activities component of ICFR?

Interpretive response: The control activities component of ICFR is relevant because, per the COSO Framework: "control activities serve as mechanisms for managing the achievement of an entity's objectives and are part of the process by which objectives are achieved." The control activities performed in this component of ICFR mitigate the identified RMMs.



See chapter 2 for discussion of the other ICFR components.

Question 5.2.30

What are the principles in the COSO Framework related to the control activities component of ICFR?

Interpretive response: There are three principles necessary for an effective control activities component of ICFR. Meeting all three principles demonstrates that controls have been designed and implemented effectively to meet their objectives.

Control activities	
Principle 10	The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
Principle 11	The organization selects and develops general control activities over technology to support the achievement of objectives.
Principle 12	The organization deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Source: COSO Internal Control – Integrated Framework (2013).

Question 5.2.40

How do control activities interact with the other components of ICFR?

Interpretive response: Control activities complement the other components of ICFR. For example:

- proper design and implementation of control activities are supported by an effective risk assessment (see chapter 3);
- determining that the control activities operate as intended is supported by monitoring (see section 2.7);
- providing control operators with the information to properly operate control activities is supported by appropriate levels of information and communication (see section 2.6 and chapter 6); and
- a robust control environment lays the foundation for an effective system of ICFR (including control activities) (see section 2.4).

Question 5.2.50

What is the importance of an entity selecting and developing control activities that contribute to the mitigation of risks to acceptable levels (Principle 10)?

Interpretive response: Per the COSO Framework, “control activities help to ensure that risk responses that address and mitigate risks are carried out.” The proper selection and development of process control activities is vital in ensuring that RMMs are properly mitigated.

Question 5.2.60

How does an entity demonstrate that it has met Principle 10?

Principle 10: The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Interpretive response: Demonstrating that the entity has met Principle 10 requires the following:

- proper risk assessment (see chapter 3);
- proper identification of relevant business processes that require control activities (see chapter 3) and obtaining an understanding of those processes (see chapter 4);
- consideration of entity-specific factors and characteristics that create risks to the achievement of objectives, including the environment, complexity, nature, and scope of the entity’s operations, which are embedded in the entity’s risk assessment (see chapter 3), process understanding (see chapter 4) and design of controls (this chapter); and
- proper design of process control activities to respond to identified PRPs (see Question 5.3.10), including a mix of control activity types and considering the level of the entity at which the control is applied, as well as appropriate segregation of duties.

An effective way to demonstrate the proper design of a process control activity is through a detailed reconciliation of its attributes to each aspect of the related PRP(s) to demonstrate that the risks are addressed by the control. Design of process control activities is covered concurrently with Principle 12 in section 5.4.

Question 5.2.70

What is the importance of an entity selecting and developing GITCs (Principle 11)?

Interpretive response: The reliability of technology within business processes, including automated process control activities, depends on the selection, development, and deployment of effective GITCs. GITCs support proper deployment of IT systems, as well as proper continued operation of those systems. GITCs also address integrity risk for information used in control activities.

Question 5.2.80

What are GITCs?

Interpretive response: 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 control activities; and
- the integrity of data and information within the entity's IT systems.

The entity’s IT processes manage:

- access to programs and data;
- program changes;
- program acquisition and development; and
- computer operations.

The IT environment encompasses the IT systems the entity uses as part of its financial reporting and business processes, including the layers of technology (application, database, operating system and network), the IT processes and the IT organization.

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

Chapter 7 provides more information about GITCs and related concepts.

Question 5.2.90

How does an entity demonstrate that it has met Principle 11?

Principle 11: The organization selects and develops general control activities over technology to support the achievement of objectives.

Interpretive response: Demonstrating that the entity has met Principle 11 requires:

- proper identification of integrity risks for information used in controls (see Question 6.4.110);
- proper identification of relevant IT layers and risks arising from IT (RAFITs) for automated process control activities (see section 7.2); and
- proper design and operation of GITCs to respond to the identified RAFITs (see section 7.3).

Question 5.2.100

What is the importance of an entity deploying control activities through policies that establish what is expected and in procedures that put those policies into action (Principle 12)?

Interpretive response: Control activities are built into business processes and employees' day-to-day activities, which occurs through:

- the policies that communicate expectations as part of the control activities; and
- the relevant procedures that put those policies into action.

The policies establish the responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside. Deployment of the policies outlines the timing, process for corrective action and competence of the personnel who perform the control activities. The policies are important to guide the performance of control activities throughout the entity.

Question 5.2.110

How does an entity demonstrate that it has met Principle 12?

Principle 12: The organization deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Interpretive response: Demonstrating that the entity has met Principle 12 requires proper documentation of policies, procedures and operation of controls. The documentation, at a minimum, should clearly identify:

- the individuals responsible for each process and executing each relevant control;
- the specific procedures the control operator is expected to perform in executing the control; and
- how outliers identified in the performance of the control are to be investigated and resolved.

5.3 Process control activities

Question 5.3.10
What are process control activities?

Interpretive response: Process control activities directly support the actions to mitigate transaction processing risks in an entity's business processes. 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 at a ‘would’ level of assurance (see Question 5.3.20).

Question 5.3.20
What is a 'would' level of assurance?

Interpretive response: For a control to function properly as a process control activity, it needs to be designed and operated in a manner to confidently support that it ‘would’ (i.e. probably will) prevent, or detect and correct on a timely basis, a material misstatement in response to the risk being addressed.

Unlike entity-level controls (see Question 2.3.20) that operate at a ‘could’ level of precision (see Question 2.3.40), process control activities are selected and developed by an entity to directly mitigate the identified risks to the achievement of financial reporting objectives to acceptable levels. An entity’s ICFR is effective when it provides reasonable assurance (i.e. a high level of assurance) regarding the reliability of the financial statements and their preparation in accordance with the applicable financial reporting framework – meaning process control activities must be designed and functioning to make it ‘probable’ the entity will achieve its financial reporting objectives. Absolute assurance is not possible due to limitations inherent in all systems of internal control, such as human error, judgment uncertainty, and events outside management’s control.

Example 5.3.10
'Could' vs 'would' level of assurance provided by controls

Scenario

Management has identified a PRP where invoices from vendors are not properly reconciled with other purchasing documentation prior to recording in the entity's ERP system, resulting in invoices being processed for which the purchase price or quantity does not agree to the purchase order and/or receiving document. This PRP is related to the risk of material misstatement that the operating expense account is not complete or accurate.

To address the PRP, management is considering whether to implement the following two controls:

- control A: a monitoring control that reviews fluctuations in the operating expense account balances year over year to identify unusual fluctuations that may warrant further investigation; and
- control B: a preventive control whereby the entity's ERP system performs, prior to recording the expense and/or making payment, a three-way match between the purchase order, invoice, and receiving document with a threshold of tolerance for potential discrepancies defined by management. Any discrepancies above the threshold are flagged by the system and investigated and resolved through a separate manual control activity (see Question 5.6.70) before the vendor invoice is processed and recorded.

Analysis

Due to the level of aggregation at which control A is designed to operate (fluctuations in the balance of the entire operating expense account), the design of the control does not support that it 'would' (i.e. probably will) identify, investigate and resolve discrepancies between vendor invoices, purchase orders and receiving documents. The control 'could' identify such issues but that is not the appropriate level of assurance to serve as a process control activity and address the identified PRP. Control A could, however, be an appropriate entity-level control that, for example, monitors the effectiveness of process control activities within the purchasing process (see Question 2.3.20).

On the other hand, control B, which is designed to operate systematically at the individual transaction level, is designed in a manner that 'would' prevent a material misstatement resulting from the incorrect recording of purchase transactions when the vendor invoice does not agree to the purchase order or the receiving document. The design of control B directly addresses the identified PRP and, therefore, mitigates the risk that the transactions in the operating expense account are not processed completely and accurately (i.e. at the assertion level within the process).

Question 5.3.30

What is the difference between a process control activity and a process?

Interpretive response: Management should think about the process as the actual steps necessary to record an amount in the financial records in accordance with the applicable financial reporting framework. In contrast, process control activities are the specific actions taken along the way to mitigate risks introduced during the process. Said differently, processes are 'how' an entity records transactions and process control activities are the different checks performed throughout the process to prevent or detect misstatements that could occur along the way. Process control activities can be manual or automated.

Question 5.3.40

Why does management differentiate process activities from control activities?

Interpretive response: Understanding the difference between activities that introduce risks and those that mitigate risks is a key first step to understanding the process and flow of transactions.

Blurring the lines or misunderstanding the distinction between process activities and control activities hinders the proper understanding of the process and flow of transactions. A lack of proper understanding of the process could lead to insufficient identification of the related PRPs that require a control response or misunderstanding of whether a process control activity addresses the related risk. Process control activities can be designed appropriately only when the risks created by the process activities that they are designed to mitigate are clearly understood and articulated.

Consider the following example of the relationship between process activities and control activities.

Process activities	PRP	Control activities to address the identified risk
Customers place their purchase orders electronically. These orders are captured in the entity's ERP system and are processed for fulfilment.	Customers could exceed their established credit limit.	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. Manual follow-up is performed for each unprocessed purchase order.

Question 5.3.50

Could two or more process control activities address the same PRP?

Interpretive response: Yes. Multiple process control activities can address the same PRP. This can occur where there are both preventive and detective controls in a process over the same PRP.

Question 5.3.60

Can one process control activity address multiple PRPs?

Interpretive response: Yes. One process control activity can address multiple PRPs when that activity is designed to adequately address each PRP. However, management should carefully evaluate how the process control activity responds to each PRP and clearly capture how it is designed to address each PRP.

For example, an entity may have a process control activity that includes the comprehensive review of:

- the presentation of the cash flows statement in accordance with a cash flows checklist; and
- the reconciliation of balances to supporting documentation.

The entity may have designed this control to address the following PRPs.

- The cash flows statement is not mathematically accurate.
- Cash payments and receipts related to debt are not completely and accurately entered in the cash flows workbook, presented gross, or classified as financing activities.
- Cash payments for investments in property, plant and equipment are not completely and accurately entered in the cash flows workbook or classified as investing activities.

This control activity may be appropriately designed to address each PRP if the cash flows checklist includes specific steps requiring the control operator to recalculate the mathematical accuracy of the statement, agree the reported balances of debt cash transactions to supporting documentation and evaluate whether they are properly presented on a gross basis and classified as financing activities, and agreeing payments for investments in property, plant and equipment as presented in the cash flows statement to supporting documentation and verifying they are classified as investing activities.

Question 5.3.70
Does management identify PRPs related to activities at a service organization?

Interpretive response: It depends. If the process activities at a service organization are part of the entity's ICFR (see Question 8.2.30), then management is responsible for understanding the process and identifying PRPs within the process. This allows management to properly consider whether the service organization has appropriate process control activities in place to mitigate the PRPs. Management also identifies PRPs and related controls, including complementary user entity controls (CUEC), around the relevant handoffs of data between the entity and the service organization.

Management may also implement process control activities at the entity to address PRPs related to the process activities carried out by the service organization. This may be necessary when process control activities at the service organization that are necessary to address the identified PRPs are missing, are not appropriately designed, or do not operate effectively.

Chapter 8 provides further information on service organizations and ICFR.

5.4 Design, documentation, and implementation of relevant process control activities

Question 5.4.10
When is a process control activity properly designed?

Interpretive response: A properly designed process control activity is capable of effectively preventing, or detecting and correcting on a timely basis, material misstatements, either individually or in combination with other process control activities.

A properly designed process control activity is effective when it:

- satisfies the entity'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 on a timely basis, a material misstatement.

Question 5.4.20

What does ‘implementation’ of a process control activity mean?

Interpretive response: The ‘implementation’ of a process control activity means that the control exists, and the entity is using it. It can also be used interchangeably with ‘operation’, meaning the continued operation of a control activity.

Question 5.4.30

What is considered when designing a process control activity?

Interpretive response: This table sets out and describes the items considered when designing a process control activity. The considerations in the table should also be present in the documentation of each process control activity. Some considerations only apply to manual process control activities, where indicated. See Question 2.3.60 for the considerations for entity-level controls and Question 7.3.30 for the considerations for GITCs.

Consideration	Description	Section
Control objective	The risks, including fraud risks, the control is intended to mitigate - i.e. the relevant PRPs the process control activity addresses. This is achieved using control attributes.	5.5
Nature and type of control	'Nature' refers to whether the process control activity is manual or automated. 'Type' refers to whether the process control activity is preventive or detective.	5.6
Frequency	The frequency with which a manual process control activity is performed, which could be: • annually; • quarterly; • monthly; • weekly; • daily; • recurring; or • ad hoc.	5.7
Authority and competence of the control operator (see Question 5.4.40)	The level of competence and authority necessary to operate a manual process control activity (i.e. is the right person performing the control activity?).	5.8
Judgment involved	The subjectivity involved in determining whether something is an outlier and/or whether that outlier is correct/reasonable in operating a manual process control activity.	5.9

Consideration	Description	Section
Level of precision	The level of precision, including the criteria/thresholds for investigation, used to identify outliers.	5.10
Investigation and resolution process	The documented steps performed by the control operator to investigate and resolve outliers identified in operation of a manual process control activity.	5.11
Information used in the performance of the control	The information used when performing the manual process control activity (e.g. system reports, manually prepared spreadsheets, queries), including the relevant data elements (see Question 6.2.40).	5.12

If it is determined that a process control activity is ineffective in its design and/or implementation, management should:

- conclude that there is a deficiency;
- evaluate the control deficiency (see chapter 9); and
- remediate the control deficiency or identify a compensating control activity (see section 9.6).

Question 5.4.40
What is a control operator?

Interpretive response: 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.

5.5 Designing and documenting a control: Control objective

Question 5.5.10
How are controls designed to achieve the control objective?

Interpretive response: To effectively design a control to achieve the control objective(s), the control should include specific attributes directly responsive to the objective(s). These attributes should be clearly documented as part of the control's design documentation. All controls have at least one control attribute.

A control's objectives are different depending on the type of control.

Type of control	Objective
Entity-level control	To address a principle of COSO, individually or with other entity-level controls (see chapter 2).
Process control activity	To mitigate a relevant PRP that relates to a relevant RMM (this chapter).
GITC	To mitigate a RAFIT (see chapter 7).

Question 5.5.20
What are control attributes?

Interpretive response: Control attributes are the specific procedures performed by the control operator that make up the control. Control attributes are the parts of the control that address its objective.

Question 5.5.30
Do all controls have attributes?

Interpretive response: Yes. All controls have at least one attribute. Depending on how a control is defined by the entity, it may have more than one attribute.

Question 5.5.40
Are all parts of a control considered control attributes?

Interpretive response: No. Control attributes do not include steps that are part of the 'process', but not part of the control. For example, if the control operator reconciling A to B is important to achieving the control objective, then that step is a control attribute. If, on the other hand, saving the completed reconciliation to a particular file folder is not important to achieving the control objective, then that step is not a control attribute.

Question 5.5.50

What level of detail is needed in identifying and documenting control attributes?

Interpretive response: Control attributes need to be sufficiently detailed for the control operator to understand what is expected of them in executing the control and for a third party (e.g. external auditor) to be able to reperform the control attributes.

Question 5.5.60

What does ‘sufficiently detailed’ mean as it relates to identifying and documenting control attributes?

Interpretive response: ‘Sufficiently detailed’ means the control attributes are described in specific terms that align with the actual procedures or steps in the control that the control operator performs. What is expected of the control operator should be clearly described in the control attribute. Vague language should be avoided.

For example, words like ‘reasonable’ or ‘appropriate’ do not provide a sufficient level of detail, nor does simply indicating that the control operator performs a ‘review.’ Instead, control attributes should articulate how the control operator judges whether something is ‘reasonable’ or ‘appropriate’ or what specific conditions the control operator contemplates or evaluates when performing a ‘review.’

Practical tip

When documenting the design of controls that require a control operator to review something and make an evaluation, avoid using the term ‘review’ in describing the control. This will help identify the specific steps or attributes the control operator is expected to perform in executing the control.

In addition, when considering whether a control attribute is sufficiently detailed, management may want to ask themselves the following question: “If another person needed to perform this control in the absence of the current control operator, would they know exactly what to do, what criteria/thresholds to apply to identify items that may require further investigation, and how to resolve such items in order to achieve the control’s objective?”

Example 5.5.10
Defining reasonableness in the context of the control attribute

Scenario

Management has documented the following process control activity: A reconciliation of the construction-in-progress (CIP) detail to the fixed asset rollforward is performed and evaluated monthly.

As part of documenting the design of this process control activity, management has identified the following control attribute:

> The control operator evaluates the reconciliation for reasonableness.

Analysis

The attribute identified by management is unclear about how the control operator determines whether each reconciling item is reasonable. Consider the following modification to this attribute:

> The control operator evaluates whether:
> - each item on the manual listing of CIP additions was properly capitalized; and
> - each item continues to represent CIP or if it was placed into service.

With the modified attributes, it is easier to understand what the control operator is looking for in determining reasonableness.

Example 5.5.20
Identifying and documenting control attributes – review of a fixed assets reconciliation

Scenario

Management has documented the following process control activity: On a quarterly basis, the control operator reviews the reconciliation of the fixed assets subledger to the general ledger.

Analysis

Although this process control activity appears to be a straightforward reconciliation review, it contains several attributes that should be separately identified when documenting the design of the control. Doing so facilitates consideration of how each part of the process control activity addresses the identified PRP(s).

Breaking apart the process control activity above and focusing on avoiding using the word ‘review’ may result in identifying the following attributes to be performed.

Attribute 1: The control operator agrees the fixed asset subledger amount to the fixed asset reconciliation.

Attribute 2: The control operator agrees the fixed asset general ledger amount to the fixed asset reconciliation.

Attribute 3: The control operator recalculates any differences between the general ledger amounts and the subledger amounts.

Attribute 4: The control operator identifies all outliers (e.g. differences greater than $10,000) and determines whether they have been appropriately resolved by the preparer of the reconciliation.

Example 5.5.30

Identifying and documenting control attributes – review of a physical inventory reconciliation

Scenario

Management has documented the following process control activity: A physical inventory reconciliation is reviewed each month by the plant controller.

Analysis

Similar to Example 5.5.20, there may be several attributes associated with this control that should be separately identified when documenting the control's design, such as the following.

Attribute 1: The control operator agrees quantities per the final physical inventory count sheets to the reconciliation. (Other process control activities operate over the physical inventory observation, resulting in the final count sheets.)

Attribute 2: The control operator agrees the pre-adjustment subledger balance to the reconciliation.

Attribute 3: The 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.

Attribute 4: The control operator agrees the result of the reconciliation to the adjusting journal entry and checks that the quantities in the post-adjustment subledger agree to the count sheets.

Example 5.5.40

Identifying and documenting control attributes – review of goodwill revenue forecast

Management has documented the following process control activity: Management reviews the revenue forecast used in the assessment of goodwill impairment for a reporting unit.

Analysis

This process control activity description is unclear about exactly what the control operator is reviewing, how the review is performed, what information is used in the review, and how any outliers are identified. Another individual performing this same process control activity would be unlikely to perform the same procedures and come to the same conclusions given this vague control description. Controls that involve judgment typically involve more attributes as well as multiple sources of information (see section 5.12 for further consideration of information used in controls). In addition, the controls may require various levels of precision, which are identified in the documentation of the individual attributes.

To facilitate consistent operation of the process control activity at the 'would' level of precision (see Question 5.3.20), management documents the following detailed attributes and focuses on avoiding the use of the word 'review'.

Attribute 1: The control operator agrees the historical data presented on the forecast spreadsheet to the prior year financial statements (i.e. the control operator validates the completeness and accuracy of data used in the operation of the control activity by agreeing it to its source).

Attribute 2: The control operator sets an expectation for Year 1 revenue growth based on examining the following internal and external information:

- 3-year historical growth for the entity's peer group;
- 12-month prospective growth forecast for the entity's peer group (when available);
- industry analysts' 12-month revenue forecast; and
- the internal sales group's revenue goals by product line, and a comparison of past sales goals with actual sales results.

Attribute 3: The control operator sets an expectation for Years 2-5 revenue growth based on examining the following internal and external information:

- 5-year historical entity-specific and industry-specific growth trends;
- the internal sales group's revenue goals by product line; and
- a comparison of past sales goals with actual sales results.

Attribute 4: The control operator compares the revenue growth forecast for the terminal value to the 10-year average rate of inflation and investigates and resolves differences greater than 0.5 percentage point.

Attribute 5: The control operator compares the actual forecast for each of the periods listed with the expectation and investigates outliers that differ by more than $10 million or 1.5% of the expectation. Outliers are investigated and resolved with persuasive supporting evidence or adjustment to the forecast.

Question 5.5.70

How should management document how the design of a control addresses its objective?

Interpretive response: When documenting the design of a control, management should include a link between the attributes of the control and the PRPs they are addressing. This supports the design of the control addressing the relevant PRPs and assists with writing the attributes in sufficient detail to clearly evidence how the attribute is addressing the risk.

When writing attributes, it is important to achieve the right balance between too much information and not enough information. The attribute(s) should guide the control operator through the steps involved in performing the process control activity. Start by writing out the steps the control operator is expected to complete as they perform the control. Then, remove any parts that do not apply to the control's performance, including those related to the 'process' and not the control.

When considering whether an attribute is sufficiently detailed, consider asking the following question: If another person needed to perform this control in the absence of the current control operator, would they know exactly what to do, what criteria/thresholds to apply to identify items that may require further investigation, and how to resolve such items to achieve the control's objective?

A best practice to evidence how controls address the control objective is a risk and controls matrix that links:

- the RMM;
- the underlying PRPs that can lead to the RMM; and
- the specific process control activities and attributes that address the PRPs.

This matrix can be shared with external auditors for alignment on the population of identified risks and related controls. Management can also use flowcharts (see Question 4.3.90) to evidence the link of PRPs to the process control activities.

5.6 Designing and documenting a control: Nature and type

Question 5.6.10
What is the 'nature' of a control?

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

Question 5.6.20
What are manual controls?

Interpretive response: Manual controls are controls performed by people.

Question 5.6.30
What are automated controls?

Interpretive response: Automated controls are controls performed by an IT system. Automated controls are executed (e.g. extending prices on invoices, performing edit checks) the same way until:

- the program logic (including the tables, files or other permanent data used by the control) is changed; or
- the automated control is otherwise overridden.

Question 5.6.40
How do IT systems perform automated controls?

Interpretive response: IT systems perform automated controls using system configurations that apply business logic governing data input, processing and output. These configurations may be programmed into any of the layers of technology that comprise an IT system (see Question 7.2.10).

Question 5.6.50

Are manual or automated controls more suitable to address certain control objectives?

Interpretive response: Yes. The following diagram captures factors that may point to either an automated or manual control being more suitable to address a specific control objective.

Automated Control

- No judgment or discretion are necessary.
- High volume of recurring transactions.
- Situations where errors are easy to define.

Manual Control

- Judgment and discretion are necessary.
- Large, unusual or non-recurring transactions.
- Changing circumstances where a control response outside the scope of an existing automated control is necessary.
- Circumstances where errors are difficult to define, anticipate or predict.
- Monitoring the effectiveness of automated controls.

Question 5.6.60

Are there any additional risks to consider when designing and implementing manual controls?

Interpretive response: 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 human error and simple mistakes. Management cannot assume that a manual control will be applied consistently each time it is performed.

Question 5.6.70

Can a manual control have an automated component?

Interpretive response: No. Manual controls often rely on or use the output of a separate automated control. While these activities might seem to be only one control, they are two distinct controls addressing different objectives.

Example 5.6.10
Separate manual and automated control activities

Scenario

Data is flowing from one system to another, and an automated process control activity is in place to support the completeness and accuracy of the data transfer. If a data transfer fails, a control operator receives a notification of the failure, and investigates the error and resolves it.

Analysis

There is an automated process control activity that addresses the PRP that data is not completely and accurately transferred from one system to another.

There is a separate manual process control activity that addresses the PRP that failures in the data transfer are not properly investigated and resolved, resulting in the data not being completely and accurately transferred.

Question 5.6.80
Are there additional considerations when designing and documenting a process control activity that is automated?

Interpretive response: Yes. When a process control activity is automated, management needs to identify and respond to RAFITs by:

- identifying the relevant layers of technology that the automated process control activity relies on and determining what RAFITs within each of those layers could impact effective operation of the automated process control activity; and
- identifying and evaluating the design and implementation of relevant GITCs that address the RAFITs.

Like with manual process control activities, documenting the level of precision when the control is designed to identify outliers is also important (see Question 5.10.10).

Chapter 7 provides further discussion of RAFITs and GITCs.

Practical tip

If an automated process control activity does not have effective GITCs that address the identified RAFITs, the automated process control activity cannot be relied on to operate effectively. GITCs are vital to the effective operation of automated process control activities, which makes identifying the relevant IT layers and the related GITCs vital to effective ICFR.

Question 5.6.90

What are the different categories of automated process control activities?

Interpretive response: The following table lists examples of different categories of common automated process control activities and example controls for each category. However, there may be additional types of automated process control activities that do not fall in the categories listed.

Category	Example
System access control activities, including those enforcing segregation of duties	• 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 an order. • Access to approve claim payments between $10,000 and $25,000 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 control activities	• The system is configured to approve invoices that match the invoice to the purchase order and the 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 assign accounts receivable transactions completely and accurately to an aging bucket based on the invoice due date. • The system is configured to completely and accurately report suspended purchase orders because of a customer exceeding their credit limit. • The system is configured to completely and accurately accumulate and report transactions based on product type.
Interface control activities	• The system is configured to produce an error when the number of records processed does not agree to the number of records shown in the interface file header record. • The system is configured to add general ledger account codes completely and accurately to transactions based on interface mapping rules.

Category	Example
	- The system is configured to produce an error log of interfaced transactions that could not be processed due to missing data elements.

Question 5.6.100
What are the different types of controls?

Interpretive response: Controls are either preventive or detective. It is important for entities to have a mix of both types.

Question 5.6.110
What are preventive controls?

Interpretive response: Preventive controls are proactive. They help reduce the risk of errors or fraud before they occur.

An example of a preventive control is an automated process control activity that requires an expenditure to be approved before posting and payment.

Question 5.6.120
What are detective controls?

Interpretive response: Detective controls identify errors or fraud after they have occurred.

An example of a detective control is a manual process control activity where a control operator reviews all expenditures at the end of the month and verifies that they were approved before posting and payment.

Practical tip

Preventive controls generally are considered stronger than detective controls because they stop the fraud or error from occurring. Management should consider which type of control is more appropriate when designing controls to address their objective.

5.7 Designing and documenting a manual control: Frequency

Question 5.7.10
What is the frequency of a manual control?

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

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

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

Question 5.7.20
Can a control be performed on an ad-hoc basis?

Interpretive response: Yes. A control may be performed only when a certain type of transaction or activity occurs. An example of an ad-hoc control is a process control activity to evaluate the appropriateness of accounting for new debt agreements when they occur.

Certain compensating controls (see section 9.6) may also be designed to operate on an ad-hoc basis to address the same objective (i.e. same PRP for process control activities) as a deficient control.

Question 5.7.30
What's the relationship between frequency and achieving the control objective?

Interpretive response: The appropriate frequency of a control's performance is considered in relation to the control objective. The precision of a control increases when the frequency and consistency of its performance increases.

When management evaluates whether a control is appropriately designed, they should ask: Does the control operate at a frequency that would achieve its objective in a timely manner? For a process control activity, the frequency should result in the prevention or detection of a material misstatement on a timely basis.

Management should document the frequency of the control's operation and how that frequency achieves the control objective.

One aspect of the control objective that may influence the frequency of the control's operation is whether the control relates primarily to income statement accounts or balance sheet accounts.

- **Income statement accounts.** Such accounts are reported on a cumulative basis, which should be reflected in the frequency of the control's operation along with the nature of the risk the control is addressing. For example, a recurring control over the approval of expenditures properly addresses the magnitude of expenditures and responds to the cumulative nature of recognizing the expenditures in the income statement.
- **Balance sheet accounts.** Such accounts are reported at a point-in-time, which should be reflected in the frequency of the control's operation (at least as of period end) along with the nature of the risk the control is addressing. While a control may be focused on a balance sheet account, it may also support the related income statement accounts, which should be reflected in the frequency of the control's operation. Two contrasting examples follow.
  - Management implements an annual inventory count. This may be an appropriate frequency due to the existence of other controls over the movement of inventory throughout the period that reduce the risk surrounding the one-time performance of the count.
  - Management implements a monthly control over accounts receivable. This may be an appropriate frequency due to the risks related to accounts receivable, the nature of the control also supporting revenue accounts and the allowance for credit losses, and the need to identify outliers on a timely basis.

Example 5.7.10
Frequency of a process control activity in relation to its objective

Scenario

An entity has a process control activity to detect improper access to a folder with information used in the preparation of financial statements. However, the process control activity only operates annually.

Analysis

The frequency of the process control activity may not be sufficient to meet the control objective as it may not detect improper access in a timely enough manner to prevent the potential manipulation of the information and a misstatement in the financial statements.

Example 5.7.20
Frequency of a process control activity in relation to its precision

Scenario

On an annual basis, the CFO reviews the entity's marketing expenses for completeness, existence and accuracy. The designed precision of that review is equal to the risk tolerance (see Question 3.4.40) established for the marketing expense account.

Analysis

Assuming the entity reports its financial results only once a year, the review control is sufficiently precise as the maximum error in the marketing expense account that the control might 'miss,' if effectively executed, would be limited to the risk tolerance established for the account. However, if the same review control operated at the same level of precision four times a year using quarterly marketing expense information, there would be a risk of 'missing' an error in the annual financial statements as large as four times the established risk tolerance. Therefore, the quarterly review control should be designed with a greater level of precision than the annual review. In this example, it would be more appropriate for the CFO's quarterly review to involve a level of precision that is one quarter of the established risk tolerance for the marketing expense account.

5.8 Designing and documenting a manual control: Competence and authority

Question 5.8.10
What does it mean for a control operator to have 'authority'?

Interpretive response: In a system of internal control, the authority of a control operator (see Question 5.4.40) relates to their ability to sufficiently challenge process owners and, where necessary, correct the process outcomes. When a control operator does not have the authority within the organization to enforce the control's operation or correct its results, the control cannot achieve its objective and, therefore, is ineffective.

Question 5.8.20
How is the control operator’s authority assessed?

Interpretive response: Authority of the control operator is assessed by obtaining an understanding of the entity’s organizational structure. The control operator must have the ability to sufficiently challenge process owners in a way that would influence their behavior.

Example 5.8.10
Authority of a control operator

Scenario

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

Analysis

Based on the entity's structure, Accounting Associate does not have the right level of authority to sufficiently challenge the legitimacy of a journal entry because they wouldn't be able to challenge a supervisor about a questionable journal entry posted by that supervisor. Therefore, the process control activity is not designed effectively to address the PRP.

Question 5.8.30
Why is a control operator’s competence important?

Interpretive response: 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 activity the way it was designed, the control may not be able to achieve its objective.

Question 5.8.40
When is the competence of a control operator considered and how is it assessed?

Interpretive response: Competence of the control operator is considered when designing a control and identifying the control operator.

Management should consider a variety of factors in assessing a potential control operator's competence, including their:

- educational level;
- prior experience with the subject matter of the control;
- prior work results (e.g. any deficiencies or misstatements in prior periods related to their areas of responsibility); and
- qualifications, licensing, membership in a professional body and other forms of external recognition.

Management should also consider the relevance of the control operator's capabilities to the control's subject matter, and whether there are circumstances that may threaten the control operator's objectivity.

Example 5.8.20
Competence of a control operator

Scenario

The Tax Department prepares the entity's income tax provision and identified specific PRPs related to the entity's valuation allowance. When designing a control to address the PRPs, management determined to require a member of the Accounting Department outside of the Tax Department to perform specific procedures over the valuation allowance analyses prepared by the Tax Department.

Management identified that the Director of Accounting is a CPA with experience in both preparing and auditing tax provisions while working for a public accounting firm. Further, the Director of Accounting has been employed with the entity for a number of years and participates in the monthly management meetings where information relevant to risks related to the recoverability of the entity's deferred tax assets is discussed.

Analysis

Management concludes that the Director of Accounting possesses the competence to perform the control over the entity's valuation allowance analysis.

Question 5.8.50
How are authority and competence considered when there are multiple control operators?

Interpretive response: It depends on whether each of the multiple control operators are performing the control or the multiple control operators are performing the control as a group.

When there are multiple control operators (e.g. a homogeneous control performed in multiple locations), all the control operators should have the necessary authority and competence to effectively perform the control.

When there are multiple control operators performing the control as a committee or a group, the aggregation of the group members should have the necessary authority and competence to effectively perform the control. In this situation, there may be different perspectives and experiences among the multiple control operators that, collectively, result in the appropriate competence and authority to effectively perform the control.

Practical tip

When the control operators have consistent roles/titles, management can consider and review the job, experience and education requirements of the related job description for that role/title to assist in assessing the authority and competence of the group of control operators.

Question 5.8.60

How is the authority and competence of the control operator affected when a control involves judgment and complexity?

Interpretive response: As the level of judgment required by, and/or complexity of, a manual control increases, so does the level of authority and competence needed of the control operator. The greater the degree of judgment and complexity, the greater the control operator's knowledge, skills and experience must be to effectively perform the control.

Practical tip

The root cause of deficiencies in complex controls or controls involving judgment is often related to the control operator not having the appropriate competence or authority to perform the control activity. This could include the control operator not having the appropriate experience or not being privy to information and decisions made within the business to appropriately identify outliers. It could also include the control operator not having the right authority to address any identified outliers.

Critical to the appropriate design of a control is whether the control operator has the appropriate experience and awareness of relevant information and decisions within the entity that may affect the control’s performance. When there are changes in control operators due to layoffs, business combinations and turnover, management should pay close attention to how those changes affect the operation of complex controls and controls involving judgment.

Question 5.8.70

Can management use a third-party or a specialist as a control operator?

Interpretive response: 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. Also, an entity may not have internal resources with the technical expertise to effectively execute controls over a particular area of accounting or financial reporting (e.g. complex tax transactions, derivative accounting). As a result, the entity may retain an external party to assist with process and control activities in those areas.

When a third-party or specialist is used as a control operator, management retains responsibility for:

- supervising the third party or specialist; and
- understanding and evaluating the third party's or specialist's work in designing, implementing and operating the control.

If management uses a third-party, including a specialist who is not employed by the entity, to operate a control, they should document their consideration of the third-party's competence by considering:

- the knowledge, skill, and ability of the third party; and
- the nature and complexity of the area that the third party was asked to address.

Question 5.8.80

Can management use a service organization as a control operator?

Interpretive response: Yes. In many cases, management may use a service organization to assist with certain of the entity's processes and functions.

For example, many entities outsource their payroll function to service providers. When a process or function is outsourced to a service organization, management remains responsible for that process or function. To carry out that responsibility, management may either:

- rely on the service organization to maintain relevant controls to prevent or detect material misstatements; or
- design and implement their own controls at the entity that prevent or detect material misstatements.

If management is relying on a service organization to perform controls and receives a SOC 1 Type II report from the service organization (see Question 8.4.30), management does not need to separately consider the authority and competence of the control operators at the service organization. The authority and competence of the service organization's control operators is evaluated by its service auditor in connection with issuing the SOC 1 Type II report. However, any communicated exceptions identified in the service auditor's report related to the authority or competence of the control operators at the service organization should be evaluated by management.

If management tests the controls at the service organization or implements their own controls at the entity related to the processes and functions performed by service organization, then the authority and competence of the control operators need to be assessed by management.

Chapter 8 provides in-depth discussion about management's responsibilities over service organizations.

5.9 Designing and documenting a manual control activity: Judgment

Question 5.9.10

What challenges arise when a control attribute involves judgment?

Interpretive response: When judgment is involved in a control attribute, it introduces challenges in elaborating on:

- the subjectivity involved in the control attribute; and
- the 'triggers' embedded in the judgmental element that may lead to the identification and investigation of outliers.

Control activities involving judgment are often used in complex areas with the potential for a higher RMM, which may increase the amount of evidence needed to show how the control is designed, implemented and operating. This is particularly true in situations where a third party (such as an external auditor) assesses the effectiveness of the entity's controls. At the same time, gathering and maintaining more evidence may present additional challenges for a control involving judgment.

Practical tip

In the words of the COSO Framework, controls "cannot be performed entirely in the minds of senior management without some documentation of management's thought process and analyses." It may be most effective for control operators to retain such documentation concurrently with the performance of a control involving judgment. To do so, the control operator could document their thought process, including how they identified and resolved outliers, or what led them to not identify any outliers.

Question 5.9.20

How is it determined if a control activity involves judgment?

Interpretive response: Determining whether a control activity involves judgment is done at the attribute level. A control attribute involves judgment if there is judgment or subjectivity in:

- applying the criteria for investigation (see Question 5.10.60);
- identifying outliers (see Question 5.11.30); or
- determining whether the item subject to the control is correct/reasonable for any individual control attribute.

In addition, use of expectations in a control attribute indicates the involvement of judgment.

In many cases, when judgment is involved in the underlying accounting for the transaction (e.g. use of an estimate), there is likely to be judgment involved in the related control activities.

Question 5.9.30

Do all control activities involve judgment?

Interpretive response: No. Many controls are binary and don’t involve judgment – e.g. a three-way match process control activity compares objectively determinable data elements among various source documents. But many other control activities involve the control operator making decisions about what constitutes an outlier or how to resolve an outlier.

Control activities may include a combination of control attributes, some involving judgment and others not involving judgment.

In determining whether a control attribute involves judgment, it can be helpful to consider whether:

- a simple automated control activity could perform the control attribute; or
- the control attribute requires a person to think and make decisions.

If a simple automated control activity could perform the control attribute, it is unlikely that judgment is involved. But, if a control attribute requires a person to think and make decisions, it likely involves judgment.

In addition, words like determines, evaluates and considers can indicate that the control attribute involves judgment. Conversely, words like agrees, calculates or validates may be indicators of control attributes that do not involve judgment.

Example 5.9.10

Identifying judgment in a control activity – margin analysis

Scenario

Management has a manual process control activity over revenue and cost of sales with the following control attributes.

Attribute 1: For each customer, the Assistant Controller agrees the total amount of revenue and cost of sales for current year to date and prior year to date in the margin analysis calculation spreadsheet to a report of revenue and cost of sales generated from the ERP system.

Attribute 2: The Assistant Controller determines the criteria used in the control to identify items for follow-up and investigation and concludes that an outlier will be identified if there are changes in margin greater than 5% and $1 million per customer or aggregate changes over $10 million.

Attribute 3: The Assistant Controller identifies all outliers meeting the criteria above.

Attribute 4: The Assistant Controller investigates all outliers and provides explanations and supporting documentation for the variances.

Attribute 5: The Assistant Controller checks the mathematical accuracy of the margin analysis spreadsheet.

Analysis

Attributes 2 and 4 involve judgment due to the subjectivity involved in executing the attributes. Attributes 1, 3 and 5, all are simple tasks that could be performed by a system. No judgment is required to complete them because they are not subjective.

Example 5.9.20

Identifying judgment in a control activity – fixed asset reconciliation

Scenario

Management has a manual process control activity over a fixed asset reconciliation with the following control attributes.

Attribute 1: The Assistant Controller reconciles the fixed asset system subledger report to the general ledger.

Attribute 2: The Assistant Controller agrees the CIP additions amount per the reconciliation to the manual listing of CIP additions.

Attribute 3: The Assistant Controller evaluates the reconciling items for reasonableness by assessing whether:

- each item on the manual listing of CIP additions was properly capitalized; and
- each item continues to represent CIP or was placed into service.

Analysis

Attributes 1 and 2 do not involve judgment as the criteria for investigation are not subjective (i.e. the fixed asset subledger + CIP additions either agrees with the general ledger balance or it does not). Attribute 3 involves judgment due to the decisions made by the control operator in determining whether the identified items were properly capitalized and represent CIP.

Question 5.9.40

Are there different considerations related to judgment when the control activity is associated with an estimate?

Interpretive response: No. However, estimates are often complex and involve risks specific to each element of the estimate (i.e. the methods, assumptions and data underlying the estimate). Therefore, multiple controls are often necessary to address the risks associated with an estimate. Some of these controls may involve judgment, and some may not.

5.10 Designing and documenting a control activity: Precision

Question 5.10.10

What is precision in the context of a process control activity?

Interpretive response: Precision is essentially the size of a potential misstatement the control activity would prevent, or detect and correct on a timely basis, when it operates effectively.

Considering a control activity's precision includes evaluating whether the control activity is designed to operate at a 'would' level (see Question 5.3.20).

Question 5.10.20
Is precision considered for all process control activities?

Interpretive response: Yes. Precision is an important consideration for **all** process control activities. The determination of precision involves evaluating the factors in Question 5.10.30.

Question 5.10.30
What are the primary factors used in determining the level of precision for a process control activity?

Interpretive response: The following are the primary factors used in considering the level of precision for a process control activity.

- **Level of aggregation.** A process control activity performed at a more granular level is generally more precise than one performed at a higher level. For example, an analysis of revenue by location or product line is more precise than an analysis of total entity revenue.

- **Consistency of performance.** A process control activity consistently and routinely performed with predefined frequency is generally more precise than one performed sporadically. In addition, a process control activity that operates only over certain transactions or items (e.g. on a sample basis (see section 5.16) or over transactions/items above a certain dollar value) is less precise than a control that operates over the entire population due to both the decreased frequency of the control's operation as well as the risks inherent in the population of transactions/items that are not subject to the control. In this situation, management should assess the residual risk inherent in the population not subject to the control and whether it may represent a risk of material misstatement.

- **Predictability of expectations.** Some process control activities use Key Performance Indicators (KPIs) or other information to develop expectations about reported amounts. The precision of those process control activities depends on the ability of the control operator to develop sufficiently precise expectations to highlight potentially material misstatements.

- **Criteria for investigation.** The threshold for identifying and investigating deviations or differences from expectations relative to materiality (or the inherent imprecision of the estimate), indicates a process control activity's precision.

A control is deemed to be sufficiently precise when the operation of the control would prevent, or detect and correct on a timely basis, a material misstatement.

Example 5.10.10
Determination of precision – review of purchases

Scenario

An entity's materiality for the current year is $2 million. In response to a PRP, the entity has a control in which the Purchasing Manager reviews and approves all purchases over $1 million to ascertain that all purchases are for valid business purposes and the amounts are accurate in that they are within $10,000 of the expected cost based on the Purchasing Manager's knowledge and previously approved purchase orders. As part of assessing the control's design, management notes a significant volume of purchases, the vast majority of which are below $1 million.

Analysis

The following is an analysis of each of the factors used in determining the right level of precision for a process control activity.

- Level of aggregation. The control is performed at the individual transaction level, so there is no aggregation.
- Consistency of performance. The control is performed on each occurrence over the threshold of $1 million. However, given that there are few transactions above the threshold, there is a low frequency of occurrence for the control. Overall consistency of performance is potentially lower due to the decreased frequency and the high volume (and aggregate value) of transactions not subject to the control in relation to the entity's materiality.
- Predictability of expectations. The control does not involve developing expectations.
- Criteria for investigation. Relative to materiality and the value of the purchase transactions subject to the control activity, the control includes a reasonably low threshold for identifying and investigating deviations.

Based on this analysis, the control may not be sufficiently precise to detect a material misstatement because there is more than a remote chance that a material misstatement exists, in the aggregate, in the population of purchases not reviewed. This is due to the high threshold for the control's operation in relation to the assessed materiality, which results in a low frequency of occurrence for the control and a large population of purchases not subject to the control (both in terms of the volume of transactions and the aggregate dollar amount).

Example 5.10.20

Determination of precision – purchase order price comparison

Scenario

An entity's materiality for the current year is $2 million. The entity begins using an automated control activity to compare prices on all purchase orders to the price master file. This check produces a report of every extended variance over $10. A separate manual control activity requires the purchasing supervisor to investigate all variances noted.

Analysis

The following is an analysis of each of the factors used in determining the right level of precision for the manual process control activity related to the purchasing supervisor's investigation of the variances.

- Level of aggregation. The control is performed at the individual transaction level, so there is no aggregation.
- Consistency of performance. There is a separate automated control that compares all purchase orders with no threshold. This manual control is performed on each variance over the threshold. There are multiple items a day on the variance report, so there is a high frequency of occurrence resulting in a higher consistency of performance.
- Predictability of expectations. The control does not involve developing expectations.
- Criteria for investigation. There is a low threshold for identifying and investigating deviations.

Based on this analysis, the control would likely be precise enough to address the identified PRP due to the low threshold for investigation applied at the individual transaction level. However, the volume of transactions and related dollar amount of transactions not subject to the control (i.e. below the $10 variance threshold) should still be considered to determine if the criteria for investigation is sufficiently precise.

Question 5.10.40

What if a process control activity is not sufficiently precise?

Interpretive response: A process control activity does not sufficiently address the risk(s), and therefore is deficient, when it:

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

The precision of the process control activity should either be modified to a sufficiently precise level, or a sufficiently precise compensating control should be implemented.

Question 5.10.50

How is the development of expectations evidenced?

Interpretive response: The development of expectations is evidenced by preparing sufficiently detailed documentation defining the related control attribute, including what the expectations are and how they were developed. As noted in Question 5.5.50, it is important that documentation of control attributes be sufficiently detailed for the control operator to have a clear understanding of what is expected of them in executing the control.

Example 5.10.30

Control attributes that involve expectations

Scenario

Management has documented the following process control activity: Management reviews the revenue forecast used in the assessment of goodwill impairment for a reporting unit, through performance of the following attributes:

Attribute 1: The control operator sets an expectation for Year 1 revenue growth based on examining the following internal and external information:

- 3-year historical growth for the entity's peer group;
- 12-month prospective growth forecast for the entity's peer group (when available);
- industry analysts' 12-month revenue forecast; and
- the internal sales group's revenue goals by product line, and comparison of past sales goals with actual sales results.

Attribute 2: The control operator sets an expectation for Years 2-5 revenue growth based on the following internal and external information:

- 5-year historical entity-specific and industry-specific growth trends;
- the internal sales group's revenue goals by product line; and
- comparison of past sales goals with actual sales results.

Attribute 3: The control operator compares the actual forecast for each of the periods listed with the expectation and investigates outliers that differ by more than $10 million or 1.5% of the expectation. Outliers are investigated and resolved with persuasive supporting evidence or adjustment to the forecast.

Analysis

Attributes 1 and 2 are instances where a control attribute involves development of expectations.

Attribute 3 covers both the identification of outliers based on the expectations developed in Attributes 1 and 2, and the investigation and resolution of these outliers. It is also common for these concepts to be split into two attributes, one for the identification of outliers and another for the resolution of those outliers.

Question 5.10.60
What are criteria for investigation?

Interpretive response: Criteria for investigation are the thresholds or characteristics used in the operation of the control activity to identify outliers, – i.e. items that require further investigation and/or resolution (see Question 5.11.10).

For some control activities, there may be no threshold or characteristics applied such that any difference identified is investigated and resolved. For other control activities, there may be a pre-defined quantitative threshold, a variable quantitative threshold, or qualitative characteristics that result in some, but not all, differences being identified as outliers and then investigated and resolved.

The established criteria for investigation influence how precisely a control activity is designed to operate.

Question 5.10.70
Why is it important to establish criteria for investigation when designing a control activity?

Interpretive response: It is important to establish criteria for investigation because, without established criteria, it is difficult to determine whether:

- the control is precise enough to prevent, or detect and correct on a timely basis, a material misstatement;
- the control is performed consistently; and
- the control appropriately addresses the identified PRP(s).

Question 5.10.80
Are the criteria for investigation of a control activity documented?

Interpretive response: Yes. The criteria for investigation should be clearly documented for all control activities, regardless of whether judgment is involved.

The criteria for investigation are often not obvious in the control description. When objective criteria for investigation have not been explicitly documented, it is challenging for:

- a control operator to know how to execute the control activity; and
- those responsible for the entity's monitoring activities (e.g. the internal audit department) to understand whether the 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.

Question 5.10.90

How are precision and criteria for investigation applied in the operation of a control?

Interpretive response: All process control activities have precision. One of the factors influencing precision is the criteria for investigation which can be pre-defined or variable. The criteria for investigation should be applied consistently each time the control is performed.

Control operators can choose to perform the process control activity at a higher level of precision (i.e. lower threshold for investigation) than documented in the design of the control. However, if they perform it at a higher threshold for investigation (i.e. lower level of precision) than was determined by management when designing the control activity, the control is no longer operating at the set precision and there would be a control deficiency.

For example, a control over a bank reconciliation requires all differences greater than $10,000 to be investigated (i.e. the set precision). However, the control operator determines for one bank reconciliation that they want to investigate a difference of $5,000. This would still be appropriate because it is less than the predetermined threshold for investigation. However, if there is a difference of $12,000 that is not investigated, the control activity would not be operating as designed and there would be a control deficiency.

Question 5.10.100

What is a threshold?

Interpretive response: A threshold is the criteria that is used to identify items that require further investigation. Thresholds can take a variety of forms but are typically either quantitative or qualitative in nature (see Questions 5.10.110 and 5.10.130, respectively).

Question 5.10.110

What are quantitative thresholds?

Interpretive response: Quantitative thresholds are numerically defined, such as by dollar amount (e.g. $10,000) or percentage (e.g. 5%). Quantitative thresholds can be either ‘pre-defined’ or ‘variable’ in nature (see Question 5.10.120).

Question 5.10.120

What are ‘pre-defined’ and ‘variable’ quantitative thresholds?

Interpretive response: A pre-defined quantitative threshold **does not** change throughout the year and would be consistent during each instance of a control activity’s performance. This threshold is typically based on a specific numerical value or range, such as a percentage or dollar amount. For example, a pre-defined quantitative threshold for accounts receivable may be set at 5% of total revenue.

A variable quantitative threshold changes based on the circumstances of the control’s performance. The control operator may need to set dynamic criteria for a control to operate at the ‘would’ level of assurance. Adjustments to the threshold may be in response to changes in external and internal factors – e.g. the nature or subject matter of the control activity. For example, a variable quantitative threshold for inventory may be set based on the demand for a particular product or the time of year.

Whether predefined or variable, quantitative thresholds should be clearly defined and documented in the control attributes.

Question 5.10.130

What are qualitative thresholds?

Interpretive response: A qualitative threshold is used to identify items for investigation and does not involve a quantitative amount or percentage.

When a qualitative threshold is used, there is an expectation that it would outline a range of acceptable differences to produce a ‘trigger point’ at which the control operator would be required to investigate outliers. Qualitative thresholds need to be ‘measurable’ – they need to be finite and reperformed by others. Example 5.10.40 provides examples of measurable qualitative thresholds.

Practical tip

When asked, control operators sometimes struggle to identify a specific precision for the control activity that they execute, and state that precision is based on differences that appear abnormal to them when exercising their professional judgment and experience. While there can be variable precision, the nature of that precision still needs to be specified.

When articulating the precision of a process control activity for purposes of defining a control attribute, a control operator might consider asking themselves questions such as the following.

- What is the smallest amount of a difference that I would investigate when executing the control activity?
- What would trigger follow-up on an item included in my review?

Questions like these can help identify and articulate a quantitative or qualitative precision for a control activity. For a qualitative precision, understanding what specific attributes would be investigated and why, assists in defining the precision. If there is no set precision, the process control activity likely does not operate consistently and, therefore, is not appropriately designed.

Example 5.10.40
Qualitative thresholds

Process control activity description: The General Counsel (GC) evaluates the following, all of which are included within a quarterly package prepared by the legal finance team:

- a Claims Status Report (CSR) printed from the eCounsel database;
- the summary of the accrual for legal contingencies; and
- the disclosures associated with legal contingencies.

The following table lists the control attributes for this process control activity, all of which involve a qualitative threshold. The qualitative thresholds are further analyzed to explain the documentation that should be prepared by the GC to capture how they applied the qualitative thresholds.

Control attribute	Analysis
Attribute 1: The GC inspects detailed support for each claim identified in the CSR, including: • information received from external counsel; • relevant case law or judgments; and • legal opinions/letters used to support ongoing judgments and estimates regarding the claim (if applicable).	See analysis for Attributes 2 and 3 below.

Control attribute	Analysis
Attribute 2: The GC assesses the relevance of the information inspected (detailed support in Attribute 1) by: - evaluating the timeliness of the information; and - determining whether the information is relevant to the current claims in the database (such as how closely aligned case law is to the entity's cases).	Evaluating the timeliness of the information likely involves a qualitative threshold that could depend on the type of case. In their documentation, the GC specifies why a certain timeframe was used to determine whether the CSR information was either 'timely' or 'untimely'. Evaluating the relevance of case law to current claims also involves a qualitative threshold. In their documentation, the GC specifies how they determined whether particular case law is aligned with the entity's cases.
Attribute 3: The GC assesses the reliability of the information inspected (detailed support in Attribute 1) by evaluating: - the source of the information (e.g. a reputable law firm); - the nature of the information (e.g. a formal legal opinion is more reliable); and - the complexity of the information.	The evaluations performed all use a qualitative threshold. In their documentation, the GC specifies or explains: - how they determined that a law firm was considered reputable and reliable; - what type of information was received, and how it was assessed for reliability; and - the complexity of the information and its effect on the information's reliability.
Attribute 4: The GC evaluates the estimated probability of an unfavorable outcome and whether the range of potential losses is estimable and appropriate, which includes assessing any changes to the probability determination or the estimated range of potential losses based on the latest information available.	The GC's evaluation of the estimated probability of an unfavorable outcome uses a qualitative threshold. This evaluation requires careful analysis of the information supporting the claims. In their documentation, the GC supports their conclusion on the estimated probability by evaluating that probability against the supporting information. The GC's estimate of the range of potential losses is often a qualitative metric. In their documentation, the GC supports their conclusion on the estimate of the range of potential losses by evaluating that range against the qualitative information used in their determination (from Attribute 1).

Question 5.10.140

What are management review controls and how is their precision considered?

Interpretive response: Management review controls (MRCs) involve a member of management or another employee reviewing information contained in underlying documents, reports or other information produced by the entity to reach or evaluate a conclusion affecting an entity's financial reporting.

Information that management or another employee may review includes variance reports, exception reports, detailed calculations supporting financial statement balances or disclosures, and reports containing management estimates or judgments. MRCs are generally control activities.

Overall, the design, documentation and operation of MRCs is no different than that of other manual controls. However, when MRCs are being evaluated by management or external auditors, it is often more difficult to obtain sufficient evidence about their design and operating effectiveness compared to other controls. This increased difficulty is attributable to the level of inherent judgment and subjectivity exercised in performing MRCs. Additionally, because MRCs often are used in more judgmental and complex areas that have the potential for a higher RMM, more persuasive evidence is required to demonstrate the design and operating effectiveness of the control.

The concept of precision is important for MRCs when considering the objective of the control and the nature and types of potential misstatements the MRC is intended to address. Without understanding the precision at which an MRC functions, it is not possible to understand whether the control sufficiently addresses the relevant financial reporting risks.

The adequacy of design, documentation and evaluation of MRCs has been under significant regulatory scrutiny in recent years. The SEC staff has stated that some MRCs might not be designed to operate at an appropriate level of precision[4]. The PCAOB has also highlighted significant auditing practice issues in this area identified in its inspections of external audit firms, specifically as it relates to assessing precision of MRCs[5]. The SEC staff has stated that the practice issues identified by the PCAOB may extend beyond audit execution in that they may be indicative of underlying deficiencies in management's controls and assessments[6].

See Appendix E for interactive PDF, Precision in practice – Documenting precision of controls, which summarizes guidance specific to evaluating and

[4] Brian Croteau, SEC Deputy Chief Accountant, Panel Discussion on Current Topics in ICFR Before the 2015 AICPA National Conference on Current SEC and PCAOB Developments, December 2015.

[5] PCAOB Staff Audit Practice Alert No. 11, Considerations for Audits of Internal Control Over Financial Reporting, October 2013.

[6] James Schnurr, SEC Chief Accountant, Remarks Before the UCI Audit Committee Summit, October 2015.

documenting the precision of internal controls in the ACL process and can be used to support management as they design and implement and also execute their controls.

5.11 Designing and documenting a manual control activity: Investigation and resolution

Question 5.11.10
What is an outlier?

Interpretive response: An outlier is an item that meets the criteria for investigation established in the control activity's design. Entities often define the criteria for investigation based on items that fall outside a range of acceptable differences from the expectations inherent in the control activity's design.

Question 5.11.20
Is an outlier a misstatement?

Interpretive response: Not necessarily. Outliers do not necessarily lead to misstatements. Rather, they trigger the control operator to perform further investigation to:

- determine whether the outlier:
  - is appropriate;
  - is an error that needs correction; or
  - otherwise indicates that the related account balance contains an error that needs correction; and
- determine whether further information or activities are needed to resolve the matter.

Question 5.11.30
How are outliers identified?

Interpretive response: Outliers are identified by appropriately applying the established criteria for investigation (see Question 5.10.60 and Example 5.11.10).

Example 5.11.10
Fixed asset reconciliation – identification of outliers

Scenario

An entity has a control activity with the following as one of its control attributes: The control operator investigates any differences between the fixed asset subledger and the general ledger greater than $10,000.

During the operation of the control attribute, the control operator identified the following.

$	Balance
Fixed asset subledger	1,140,000
General ledger	1,163,000
Difference	**(23,000)**

Analysis

The control operator identifies the difference of ($23,000) as an outlier because it exceeds the $10,000 threshold set in the design of the control attribute.

Question 5.11.40
Are all outliers investigated?

Interpretive response: Yes. All outliers are required to be investigated to confirm whether they are appropriate, represent an error or otherwise indicate that the related account balance contains an error. If the control operator does not investigate all outliers, the control would not operate effectively.

Example 5.11.20
Fixed asset reconciliation – investigation of outliers

Scenario

This scenario is a continuation of Example 5.11.10.

Analysis

The control operator used the fixed asset subledger and the general ledger detail to further understand and resolve the identified outlier. The control operator noted the following.

$	Fixed asset subledger	General ledger
Balance, March 31, 20X1	1,000,000	1,000,000
Additions: IT equipment	-	23,000
Additions: Machinery	140,000	140,000
	1,140,000	**1,163,000**

During the control operator's investigation, they identified that the IT equipment had not been added to the fixed asset subledger. The control operator evaluated whether the IT equipment had been appropriately recorded to the general ledger by obtaining the associated purchase invoices.

Question 5.11.50

Are all outliers resolved?

Interpretive response: Yes. All outliers must be resolved by concluding whether each outlier is either appropriate or an error.

Example 5.11.30

Fixed asset reconciliation – resolution of outliers

Scenario

This scenario is a continuation of Example 5.11.20.

Analysis

Based on their investigation, the control operator determined that the IT equipment was appropriately recorded to the general ledger in the correct period. As a result, the control operator updated the fixed asset subledger to include the additions of IT equipment during the period.

After updating the fixed asset subledger, the control operator re-ran both the fixed asset subledger and the general ledger. A comparison of the two produced an exact match of $1,163,000. As a result, the control operator determined that further investigation was not required.

Question 5.11.60

What should be documented related to the identification and resolution of outliers?

Interpretive response: Sufficient documentation should be maintained by the control operator to evidence:

- the criteria for investigation in the performance of the control;
- the outliers that were identified in applying the criteria for investigation to the population of items subject to the control; and
- how the outliers were resolved.

Documentation of how outliers were resolved should include evidence of follow-up actions taken by the control operator and the conclusions reached related to each outlier, including whether potential misstatements were appropriately investigated and whether corrective actions were taken as needed.

Practical tip

Sometimes management's familiarity with the control and the related business process may unintentionally result in their preparation of limited documentation related to the identification and resolution of outliers. Management should guard against this result by carefully considering and being mindful of the external auditors' requirement under relevant professional standards to gather sufficient, appropriate evidence of the design and operating effectiveness of control activities. While management's documentation might be viewed as sufficient for their own assessment of ICFR, consideration should be given to whether sufficiently detailed documentation exists for an external auditor to conclude on the design and operating effectiveness of management's control activities.

Question 5.11.70

What if no outliers are identified in the performance of a control activity?

Interpretive response: Depending on the level of aggregation of a control activity, there may be differing amounts of outliers identified. Some control activities, such as those performed at a transaction level, may identify many outliers on a regular basis. Other controls, such as those performed at the financial statement caption level, may rarely identify outliers.

When a control operator performs a control activity that rarely (or never) identifies any outliers, they, along with management, should first evaluate:

- whether the control operator appropriately performed the control; and
- whether any outliers should have been identified (e.g. the control operator is aware of a change in the business that should have been identified as part of the performance of the control but was not).

Next, the control operator, along with management, should consider if the control activity is designed effectively with a sufficient precision to prevent, or detect and correct, a material misstatement in a timely manner related to the PRP it is intended to address.

Careful consideration should be given when no outliers are identified because this may indicate that the control activity is not designed at the appropriate level of precision and, therefore, is deficient.

Practical tip

In instances where a control activity operates, but does not identify any outliers, contemporaneous documentation of the control's operation should be prepared, including what criteria for investigation have been applied and how they have been applied. This documentation supports the control operating as designed, which is needed when a third party (such as internal or external auditors) is assessing the effectiveness of the entity's ICFR. Absent this documentation, when no outliers are identified, no evidence exists to support the control operating at a 'would' level of precision.

Like with other factors, appropriate documentation also assists future control operators in determining how to identify and handle outliers by understanding the full design and operation of the control.

5.12 Designing and documenting a manual process control activity: Information

Chapter 6 covers the identification and evaluation of information used in the performance of a control activity.

5.13 Controls responding to a fraud risk

Question 5.13.10
Is it necessary to design control activities to address fraud risks?

Interpretive response: Yes. When a fraud risk has been identified by the entity that creates a reasonable possibility of a material misstatement of the financial statements, the entity should design a control activity to address that risk.

Principle 8 of the COSO Framework requires organizations to consider the potential for fraud in assessing risks to the achievement of objectives (see Question 2.5.120). Principle 8 identifies four types of fraud that require consideration:

- misappropriation of assets;
- fraudulent financial reporting;
- corruption and other illegal acts; and
- management override of controls (see Question 5.14.40).

The SEC has stated the following in SEC Release No. 33-8810: "Management should recognize that the risk of material misstatement due to fraud ordinarily exists in any organization, regardless of size or type, and it may vary by specific location or segment and by an individual reporting element."

While the design and implementation of controls over fraud risks should consider all the previous guidance provided in this chapter, there are additional considerations when management is designing a controls response to fraud risks and operating the related controls. These considerations are discussed in the following questions. See Appendix B for example fraud risk factors.

Question 5.13.20
What is an anti-fraud control?

Interpretive response: 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
- an entity-level control (see section 2.3) that supports the effective functioning of process control activities that directly address an identified risk of fraud.

Anti-fraud controls should be designed to:

- mitigate incentives for, and pressures on, management to falsify or inappropriately manage financial results;
- prevent, deter and detect fraud (e.g. controls to promote a culture of honesty and ethical behavior); and
- mitigate specific risks of fraud (e.g. process control activities to address risks of intentional misstatement of specific accounts or misappropriation of assets such as cash or inventories).

Question 5.13.30
What activities generally require anti-fraud controls?

Interpretive response: Anti-fraud controls are often necessary in the following scenarios:

- significant unusual transactions, particularly those that result in late or unusual journal entries;
- the period-end financial reporting process, including posting of non-standard journal entries and adjustments;
- transactions with related parties, including significant related party transactions outside the entity's normal course of business; and
- accounting estimates that give rise to increased risks of material misstatement due to their complexity, subjectivity and estimation uncertainty.

Question 5.13.40
What are control activities that address the risk of misappropriation of assets?

Interpretive response: Control activities that address the risk of misappropriation of assets are also referred to as control activities over the safeguarding of assets. Management puts these control activities 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 PRPs are identified related to such unauthorized activity, management should identify the process control activities that mitigate those PRPs (see Example 3.2.10 for example risks related to safeguarding of assets).

Common examples of control activities over the safeguarding of assets include:

- segregating duties;
- comparing the results of physical cash, security and inventory counts with accounting records on a periodic basis;
- enforcing appropriate management approval before an employee executes a contract that binds the entity to certain obligations; and
- enforcing appropriate authorization for access to computer programs and data files.

Safeguarding control activities do not physically protect assets or prevent bad business decisions. Their objective is to mitigate RMMs due to the misappropriation of assets.

5.14 Controls responding to a risk related to journal entries and other adjustments

Question 5.14.10
How are risks related to journal entries and other adjustments considered when designing control activities?

Interpretive response: Due to the different types of journal entries and other adjustments (e.g. on-top (i.e. topside) and post-close adjustments), there are various types of related risks (as discussed in Question 4.7.30) that management should address through appropriately designed control activities.

Often a combination or suite of process control activities working together is necessary to address the PRPs related to journal entries and other adjustments. For example, there may be a process control activity involving the independent review and approval of manual journal entries and supporting documentation before the entry is recorded in the system. This process control activity is generally designed to address the existence and accuracy of the transaction recorded through the journal entry. However, because of the risk of management override of this control, it is generally necessary to have a separate process control activity that verifies that all entries that were posted were in fact subject to the upfront review and approval control.

The general risks related to journal entries and other adjustments are the following.

- All journal entries and other adjustments that should have been recorded were not recorded (completeness).
- Journal entries and other adjustments recorded do not represent a true transaction of the entity or have not been recorded accurately to appropriate accounts (existence and accuracy).
- Management may override controls through posting of journal entries and other adjustments (fraud risk).

While the design and implementation of controls related to journal entries and other adjustments should consider all the previous guidance provided in this chapter, there are additional considerations when management is designing a control to respond to risks involving journal entries and other adjustments and operating the related control activities. These considerations are discussed in the following questions.

Question 5.14.20

What types of control activities can address the risk of completeness associated with journal entries and other adjustments?

Interpretive response: Completeness of journal entries and other adjustments is generally addressed through various control activities involved in the period-end financial close and reporting process. These control activities are often designed to mitigate the risk that journal entries and other adjustments that should have been recorded were not recorded. Examples of such control activities include:

- completion of a closing procedural checklist designed to determine that all appropriate journal entries and other adjustments have been recorded;
- comparison of reports summarizing all manual journal entries posted during the period to a list of standard manual journal entries required for each reporting period; and
- verification that there are no ‘pending’ or unposted entries in the system when review and approval controls over journal entries are automated.

Account reconciliation process control activities demonstrate that the detailed subledger account (or other data source) reconciles with the general ledger control account. However, the effectiveness of these process control activities to address the completeness of journal entries and other adjustments is dependent on the precision of the control activity and the nature and magnitude of accounts subject to the control.

Question 5.14.30

What types of control activities can address the risk of existence and accuracy associated with journal entries and other adjustments?

Interpretive response: In most instances, a mix of both manual and automated controls should be used to address the PRPs related to the existence and accuracy of journal entries and other adjustments. The factors discussed in Question 5.6.50 should be considered when determining the appropriate nature of the controls to design and implement.

The following table includes examples of automated and manual controls that can address the risk of existence and accuracy associated with journal entries and other adjustments. Automated control activities would also require relevant GITCs to support their effective operation.

Automated control activities	Manual control activities
• Control activities over the interface between subledger systems and the general ledger. • Configuration control activities preventing modifications to journal entries after posting or requiring re-approval if modified. • Configuration control activities preventing journal entries from posting without approval from a separate party. • Configuration control activities to provide completeness and accuracy checks over the number of journal entries, the dollar amounts and relevant general ledger accounts. • Configuration control activities preventing a manual journal entry from being posted if it is out of balance (i.e. debits do not equal credits), includes invalid account numbers or is coded to a closed or future accounting period.	• Reconciliation between subledger systems and the general ledger. • Review and approval of the manual journal entry and supporting documentation by an appropriately knowledgeable supervisor independent of the preparer to validate the existence of the transaction and the accuracy of dollar amounts, general ledger accounts and accounting period. • Review and approval of other adjustments included on an adjustment schedule and the related supporting documentation by an appropriately knowledgeable supervisor independent of the preparer to validate the existence of the underlying transaction or activity and the accuracy of dollar amounts, general ledger accounts and accounting period.

Practical tip

When the review of a manual journal entry is intended to address the existence and accuracy of the amounts being recorded to the general ledger, then the review needs to also evaluate the completeness and accuracy of the underlying information supporting the journal entry.

Question 5.14.40
What is the risk of management override of controls?

Interpretive response: The risk of management override of controls relates to the risk that internal controls that otherwise appear to be well-designed and effective may be overridden by management. Because management is in a unique position to perpetrate fraud due to their ability to manipulate accounting records directly or indirectly, the risk of management override of controls is considered in any control environment.

Examples of how management may override controls include:

- creating, or instructing an employee to record, fictitious manual journal entries to circumvent the regular process for approving and recording journal entries or other adjustments;
- applying bias when making estimates and judgments; and
- accounting for significant unusual transactions in a manner inconsistent with their substance and/or the requirements of the applicable financial reporting framework.

Question 5.14.50
How is the risk of management override addressed?

Interpretive response: As part of the design of an effective system of internal control, management should consider the risk of management override and design and implement controls that:

- are performed by control operators who are not subject to management influence;
- include appropriate segregation of duties to reduce opportunities for an individual within the organization to both perpetrate and conceal fraud; and/or
- prevent or detect the recording of inappropriate journal entries and other adjustments.

Question 5.14.60

What types of control activities can address the risk of management override associated with journal entries and other adjustments?

Interpretive response: The risk of management override of controls generally is associated with manual journal entries and other adjustments. This risk is usually not sufficiently covered through the controls over the existence and accuracy of journal entries and other adjustments and needs to be addressed separately.

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

- a separate manual journal entry control where the control operator, who is independent from the journal entry process, validates the following for the population of all recorded manual journal entries:
  - each journal entry was reviewed and approved by an appropriate approver;
  - the amounts recorded in the general ledger and the accounts in which they were recorded, among other key data elements of the journal entry, agree to what was initially approved; and
  - there is a valid business purpose for the journal entry;
- a separate control over other adjustments where the control operator, who is independent from the other adjustments process, validates the following for the population of all other adjustments:
  - each other adjustment was reviewed and approved by an appropriate approver;
  - the amounts and impacted accounts, among other key data elements of the other adjustment, agree to what was initially approved; and
  - there is a valid business purpose for the other adjustment;
- an automated control that prevents executive management from independently initiating, authorizing or recording journal entries or other adjustments within the IT system;
- an automated control that prevents users from independently initiating, authorizing and recording journal entries or other adjustments within the IT system without approval from a separate party;
- automated control activities that prevent changes, or require re-approval when changes are made, to relevant information before or after a journal entry or other adjustment has been posted, such as changes in the identity of the user that created or posted a journal entry or other adjustment, or account; and

- other indirect control activities, such as account reconciliation controls or analytical reviews of posted journal entries for trends or unusual or high-risk entries, or monitoring controls.

Practical tip

Recall the importance of implementing and operating controls to address the relevance and reliability (completeness and accuracy) of information used in controls. The same considerations apply to information used in controls over journal entries and other adjustments (e.g. reports or listings of all recorded manual journal entries and other adjustments). Also recall that for automated controls to be relied on throughout the period, related general IT controls that support their continued and consistent operation are required.

Question 5.14.70

Can other indirect control activities address journal entry risks?

Interpretive response: It depends. Other indirect types of journal entry controls, such as account reconciliations or analytical reviews of posted journal entries for trends or unusual or high-risk entries, are commonly insufficient on their own to address risks related to journal entries but may be effective when operated together with other controls.

These controls may function together with other controls as part of a suite of controls in place to address the risk of management override of controls in certain circumstances. If management is planning to rely on other indirect control activities, careful consideration is needed as it may be difficult to conclude such controls operate at a 'would' level of precision (see Question 5.3.20) to address the related risks, given they are not performed over each instance of a relevant activity within the process.

Management may consider the following questions to evaluate whether these other indirect control activities respond to the risk of management override of controls.

- Do account reconciliation controls cover the relevant balance sheet and income statement accounts and validate those reconciliations were performed completely and accurately for the period?

- When and by whom are account reconciliation controls performed? For example, are they performed by individuals whose duties are appropriately segregated from the journal entry process, and are they performed after the control activities at the process level have been completed, but before the financial information is reported?

- Is the objective of the account reconciliation control to validate that the balance includes only activity that derives from appropriately controlled business processes? For example, is the balance reconciled to the output of the related process-level controls pertaining to the account?

- Is the precision of the reconciliation control sufficient to prevent, or detect and correct on a timely basis, a material misstatement? For example, is the dollar threshold below which reconciling items require no further evaluation sufficiently precise when considering aggregation over time and across accounts?
- If any adjustments are made resulting from the account reconciliation controls, are these subject to appropriate review and approval?
- When executing an analytical review of posted journal entries, are the criteria for what constitutes a journal entry requiring further review clearly defined? Has management performed sufficient analysis to conclude that the other posted journal entries are not 'high-risk,' individually or in the aggregate?
- Is information used in the analytical review or other monitoring controls complete and are specific data elements used in the control deemed to be accurate through the effective operation of other controls?
- Where certain accounts or portions of the journal entry population are not subject to review, has management evaluated and concluded on the level of risk present in this remaining population? For example, when the controls involve sampling or a dollar threshold over which journal entries are reviewed, management should consider the remaining population and evaluate whether the risk in this population has been sufficiently reduced via monitoring and/or other controls.

5.15 Controls responding to going concern, significant unusual transactions, and related parties

Question 5.15.10

Are there special considerations for control activities over the risk related to an entity's ability to continue as a going concern?

Interpretive response: Yes. As part of the risk assessment process, management's assessment of going concern may lead to the determination that there is an RMM related to either:

- an inappropriate conclusion on the entity's ability to continue as a going concern; or
- inadequate financial statement disclosures related to the entity's ability to continue as a going concern.

If either of those RMMs is present, appropriate process control activities must be designed and implemented to address the related PRPs. Question 3.2.40 discusses risk assessment related to an entity's ability to continue as a going concern.

While the design and implementation of controls over going concern should consider all the previous guidance provided in this chapter, there may be additional considerations when management is designing a controls response to going concern risks and operating the related control activities.

Specifically, proper control activities should be designed and implemented related to the entity's going concern assessment, including:

- the completeness of events and conditions identified that may raise substantial doubt;
- the preparation of forecasts of the entity's financial condition and liquidity (or the effect on those forecasts of plans to mitigate the conditions and events that give rise to a going concern uncertainty);
- the reasonableness of assumptions used in the forecasts;
- the completeness and accuracy of information used; and
- the appropriateness of relevant disclosures.

Because of the considerations likely involved in the going concern assessment, the related control activities may include control attributes that require judgment (see section 5.9). In addition, because some of the control activities related to the entity's going concern assessment may operate with a low frequency (annually or less frequently if risks of material misstatement related to the entity's going concern assessment are not identified in a given period), management should confirm the design of the controls is appropriate in the specific circumstances of the entity and its going concern assessment. In addition, operators of these control activities may lack experience with their execution or subject matter. Therefore, additional and timely monitoring procedures over the design and operation of these controls may be necessary.

Related to process control activities over preparation and use of forecasts of the entity's financial condition and liquidity, management may be able to leverage existing processes and control activities over projected financial information used in other areas of its financial reporting.

Practical tip

Management should have control activities in place each period in which a risk related to the going concern assessment is identified through management's risk assessment. However, the nature, extent, and precision of the control activities should reflect the significance of the risk identified. As with any other control activities, management should consider the objective (i.e. PRPs being addressed) and the required precision when designing the control(s).

Question 5.15.20

What are significant unusual transactions?

Interpretive response: A significant unusual transaction (SUT) is a significant transaction that is outside the normal course of business for the entity or that otherwise appears to be unusual due to its timing, size, or nature.

Examples of significant unusual transactions include:

- business combinations executed by an entity that is not regularly acquisitive;
- issuance of debt, or refinancing of existing debt, under a new vehicle or agreement with terms not typical to the entity;
- a long-lived asset impairment trigger within an entity that does not regularly have such triggers;
- restructuring charges; and
- unusual sales transactions (e.g. large one-off sales contracts with terms that differ from normal sales).

Question 5.15.30

What kind of controls over SUTs does management need to have in place?

Interpretive response: While SUTs may not occur in every reporting period, management should have controls in place to timely identify SUTs when they occur. Monitoring for and identification of SUTs are usually elements of the entity's risk assessment process (see chapter 3).

However, certain process control activities may also identify the existence of SUTs. Examples include controls where management reviews and approves:

- arrangements/transactions with third parties above a certain amount defined in the entity's policies;
- arrangements/transactions with related parties above a certain amount defined in the entity's policies;
- arrangements/transactions for which key terms and conditions are inconsistent with entity policies (e.g. modified credit terms, atypical liability terms);
- arrangements/transactions with regulators or counterparties to settle claims/litigation;
- arrangements/transactions that include options, embedded derivatives, or other similar features; and
- cross-border intercompany arrangements/transactions subject to transfer pricing rules.

Once a SUT has been identified, management should identify and assess the RMMs and PRPs related to the SUT and design specific process control activities to respond to those risks, considering all the previous guidance provided in this chapter.

Question 5.15.40

Why are there special considerations for controls related to SUTs?

Interpretive response: Given the unique nature, size, and complexity of SUTs, they often present a higher RMM to the entity's financial statements. This is because there may be:

- incentives for management to conclude on a specific accounting treatment;
- greater manual intervention for data collection and processing;
- complex calculations or accounting principles;
- difficulty in implementing effective processes to account for the transactions (due to their nonroutine nature); and/or
- related party involvement.

In addition, the processes and process control activities for an individual SUT are often not part of the entity's historical or ongoing operations. If the entity does not have an instance of a SUT during a year, the related process control activities will remain dormant and there will be no instance for which to evaluate the operating effectiveness of the controls. This may increase the risk that the process control activities will not operate as designed, or that the design of the controls will no longer be adequate, when a SUT does take place and needs to be accounted for and reported by the entity. Furthermore, because of the unique nature of many SUTs, entities often design and implement new process control activities to respond to the risks related to these transactions. These new process control activities often have higher risks associated with their operating effectiveness because they do not have a consistent history of performance or because they will be performed by control operators who are not as experienced with the risks related to the SUT. Therefore, additional and timely monitoring over the process control activities related to SUTs may be necessary.

Question 5.15.50

Are there special considerations for controls over related party relationships and transactions?

Interpretive response: Yes. Management is required to have controls in place over the identification of relationships that result in related parties as well as transactions with the identified related parties. If there are risks identified related to transactions with related parties, management should design and implement process control activities to address those risks.

Furthermore, if management has made an assertion in the financial statements that a transaction with a related party was conducted at 'arm's length' (see Questions 5.15.70 and 5.15.80), a process control activity should be designed and implemented to address the risk that an assertion of arm's length is not appropriate.

Question 5.15.60

What are examples of controls that may be in place to address the completeness of related parties?

Interpretive response: The following are examples of controls that may be in place to address the completeness of related parties.

- Quarterly review for completeness of the listing of related parties that is maintained by the entity's legal department by tying back to source documentation, which includes director and officer questionnaires and new transactions executed during the period with entities or persons that were identified as related parties.
- A comparison of the related party transactions is performed year-over-year and fluctuations over a set amount are investigated.
- Annually, management performs a data search for the names of related parties within the sales and expense populations to identify related party transactions.

Question 5.15.70

When management asserts a transaction occurred at arm's length, what terms of the transaction is that assertion referring to?

Interpretive response: Without disclosure to the contrary, there is a general presumption that related party transactions are not consummated at arm's length because the requisite conditions of competitive, free-market dealings may not exist. However, when management makes an assertion that a transaction was conducted at terms equivalent to those prevailing in an arm's-length transaction, they are asserting that all the terms of the transaction are at arm's length, not just the price. This includes credit terms, contingencies, warranties, etc.

Question 5.15.80

What controls can management design and operate to address the risk of an inappropriate assertion that a related party transaction is at arm's length?

Interpretive response: Management may design and operate controls that provide the following evidence:

- other similar or identical transactions conducted by management between the entity and unrelated parties with identical terms;
- a report from management's specialist that has evaluated or determined a market value for the transaction and shows the transaction's terms are consistent with that market value; and
- other similar transactions conducted outside the entity by other parties in an open market with identical terms.

It may be difficult for management to substantiate their arm's length assertion of the transaction's terms unless the entity routinely engages in similar transactions with unrelated entities. This difficulty does not negate the need for substantiation.

5.16 Controls executed on a sample basis

Question 5.16.10

Can controls be designed to be executed on a sample basis?

Interpretive response: Using a sampling technique in the design and execution of controls may be acceptable. Although the use of sampling is not specifically discussed in the COSO Framework, the approach is not explicitly prohibited.

The COSO Framework requires management to use judgment in designing, implementing, and executing internal controls, based on the results of their thorough risk assessment process to respond to identified and assessed RMMs. Such risk assessment may lead management to conclude that certain controls designed and implemented to be operated on a sample basis can respond effectively to an identified risk. However, these instances are expected to be rare and require careful consideration by management.

Practical tip

If management is planning to rely on a control activity that operates on a sample basis to address a PRP, it is recommended to discuss the use of sampling with the external auditors before implementation to obtain agreement that sampling is appropriate. It may be difficult to conclude that a sampling process control activity operates at a 'would' level of precision (see Question 5.3.20) to address the PRP(s), given it is not performed over each instance of a relevant activity within the process.

Question 5.16.20

When might it be appropriate to design controls to operate on a sample basis?

Interpretive response: Generally, sampling in controls should be limited to lower risk areas due to sampling risk. Sampling risk is the risk of reaching an incorrect conclusion because the conclusion reached based on a sample may be different than if the same procedures were applied to 100% of the population. Management should support their risk assessment and the sampling approach used in controls with robust documentation that considers the following:

- **Whether the control that operates on a sample basis is monitoring the effectiveness of other controls or is the primary response to an identified PRP.** Sampling is often more supportable when it is used in controls that monitor the effectiveness of other control activities. For example, management may design a control to count inventory on a sample basis because that control is monitoring the design and operating effectiveness of controls over inventory movements recorded in the perpetual inventory listing.

- **Nature of the process.** When the processes are complex, not routine, contain historical errors or control deficiencies, it may not be appropriate to consider sampling in the design of controls. For example, management may determine that sampling is inappropriate in processes that contain critical accounting policies or processes where one or more deficiencies were identified in the current and/or prior years. Overall, sampling is most effective when errors are not expected to exist in the population. When a sampling approach is used and exceptions are identified, management generally either reconsiders whether a sampling approach is appropriate or extrapolates the errors identified.

- **Residual population.** By nature, sampling is defined by drawing conclusions about an entire population by testing only selected items from that population. Sampling is most appropriate when the sample selection subject to the control is:

  - highly representative of a homogenous set of transactions; or

  - designed such that enough of the population is covered and a reasonable conclusion can be drawn that there is a remote risk of material misstatement in the residual population.

- **Risk of error associated with the account or disclosure addressed by the control.** As mentioned earlier, sampling in controls should be limited to lower risk areas.

- **Competence of the control operator.** In general, sampling in controls should be limited to areas where the control operator has demonstrated competence.
- **Nature of the control.** When the control is complex or involves significant judgments, it may be inappropriate to consider sampling in the design of the control.
- **Nature of the transactions.** Transactions that are subject to the control that operates on a sample basis should be more routine in nature. For example, transactions that result from complex calculations often have multiple inputs, each of which may present a possibility for error. Verification checks, binary confirmations or simple calculations with fewer inputs may have a lower chance of error and therefore may lend themselves to a sampling approach. Additionally, the population of transactions subject to the control would ordinarily be expected to have a consistent risk profile such that they are initiated, authorized, processed and recorded in the same manner.

Example 5.16.10

Evaluating whether a control that operates on a sample basis is appropriate for an inventory count

Scenario

An entity has determined existence of inventory represents a low inherent risk of error and the nature of the population of inventory is homogenous. In addition, there are process control activities over the receipt and sale of inventory.

Analysis

Management has concluded a manual process control activity that operates over a sample of inventory items – a cycle count instead of a full year-end inventory count – sufficiently addresses the identified PRPs because:

- the cycle count process control activity is monitoring the effectiveness of the other process control activities; and
- the sample selection and results are representative of a full inventory count.

Question 5.16.30

What method is used to select the sample size to be used in a control?

Interpretive response: It depends on the facts and circumstances. However, in all cases, sampling should provide a basis for extrapolating results to the entire population from which the sample was selected.

Management should have a well-documented basis for their sampling methodology and strategy, including determination of the size of the sample to be used in a control's operation. Setting a sample size of a certain number of items with little to no documented basis is inappropriate.

Practical tip

When using a sampling method, management is responsible for understanding and establishing the parameters, assumptions and sampling method used to determine and select the sample.

Question 5.16.40

What other factors should management consider when designing a control that operates on a sample basis?

Interpretive response: Management should consider the following additional factors when designing controls that operate on a sample basis.

- **Whether the population to be sampled is complete.** For example, tying the population total back to the general ledger.

- **The characteristics of the population to be sampled.** The population's characteristics are important in determining whether it is suitable for sampling, and the characteristics may affect how the sample is designed. Management may consider the following questions to understand the population's characteristics:

  - Are there positive and negative or zero-value items present?
  - Is the population spread across multiple locations?
  - Are there groups or sub-populations within the population that have different risk characteristics?

  Consistency of risk profile is important in evaluating the population, which may be divided into multiple sub-populations or strata based on similar characteristics. It is critical that management assess the homogeneity within the separate sub-populations to conclude that one transaction is representative of the population subject to sampling.

- **Definition of an error.** A clear understanding of what constitutes an exception helps to focus on the relevant conditions. For example, management designs a control for warehouse personnel to compare a bill of lading to a pick list generated by the entity's sales system to verify customer name, SKU number and order quantity. The objective of the control is the existence and accuracy of the sale and shipping information. Discrepancies in payment terms or collectability would not be considered exceptions for this specific control and would be addressed by other controls in the sales and receivables process, as applicable.

- **Relationship between the objective of the control and the sample selected.** Using the bill of lading and pick list comparison example above, because the objective of the control is the existence and accuracy of the sale and shipping information, management would likely select samples from the population of sales invoices, because they presumably would have an associated pick list and bill of lading. Conversely, management would not select samples from a population of customer payments because they may not be directly associated with individual sales and shipments.

Question 5.16.50

Can a sampling control be used to address completeness?

Interpretive response: No. A control that operates on a sample basis is inappropriate to address a PRP regarding completeness. If a PRP regarding completeness is identified, additional process control activities would need to be designed and implemented to address this PRP.

.

5.17 Considerations when there are changes to controls

Question 5.17.10

What is considered a change in a control?

Interpretive response: A change in a control includes changes to:

- how the control attributes address the objective of the control;
- the nature or type of the control;
- the frequency of the control's performance;
- the precision with which the control operates;
- the investigation and resolution process for outliers identified in operating the control; and
- the information used in the performance of the control.

Question 5.17.20

What is the impact of a change in a control?

Interpretive response: When there have been changes to a control, including those listed in Question 5.17.10, they can affect the control's ability to address the objective(s) of the control (i.e. prevent or detect a material misstatement). This could result in a control deficiency and/or the need to identify other compensating controls.

Practical tip

When any of the changes listed in Question 5.17.10 occur, the control is considered a 'different control'. Therefore, as part of an ICFR assessment, management should consider testing both the old and new versions of the control separately in performing their assessment of the effectiveness of ICFR.

Question 5.17.30

What are the impacts of a change in the control operator?

Interpretive response: A change in the control operator may not directly affect the design of the control, but if the new control operator does not have the authority and competence to perform the control, the change could result in the control not being appropriately performed.

The following table provides common pitfalls and related best practices when there is a change in the control operator.

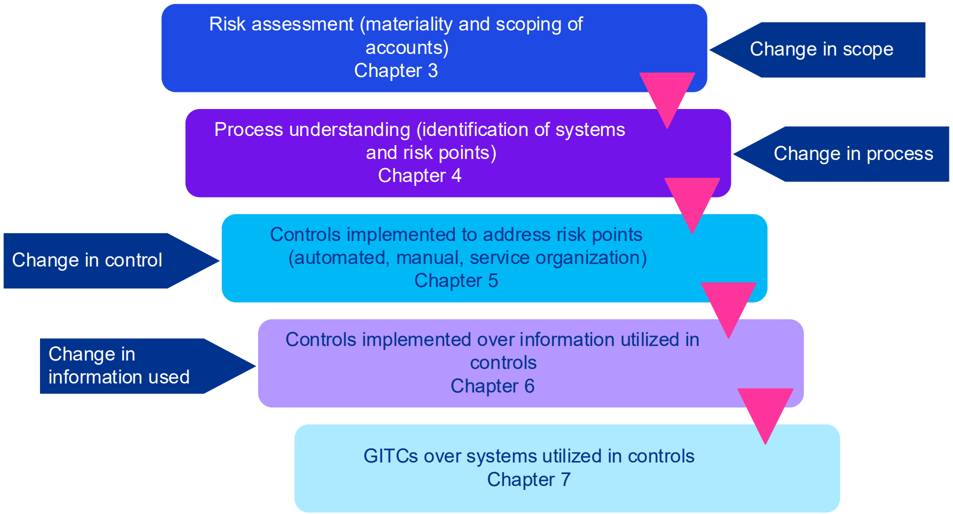
Common pitfalls	Best practices
• The new control operator changes the attributes or precision of the control such that they no longer address the risk.	• There is a process in place to transition the control to the new control operator before the former control operator stops performing the control. • Management maintains and makes available to the control operator documentation of how controls operate, including their precision, frequency, attributes, timing, and documentation.
• The new control operator forgets to perform the control (or is unaware of the control). • The new control operator uses a different report to perform the control without considering the relevance and reliability of the information (see chapter 6). • The new control operator does not maintain sufficient evidence of performance of the control. • The new control operator does not have the authority or competency to operate the control.	• There is a process in place where Internal Audit reviews the control's first performance after a change in the control operator to identify and remediate any issues identified on a timely basis.
• The new control operator has sufficient competence in the underlying subject matter of the control but lacks sufficient knowledge	• Management evaluates the nature of the information necessary for the control operator to perform the control and has procedures in place

Common pitfalls	Best practices
of the entity to be able to properly identify all expected outliers.	to share that information with the new control operator.

Question 5.17.40
Does a change in the PRP addressed by a process control activity require a change in the control?

Interpretive response: It depends. Controls are generally designed to address certain objectives. If the risk has changed to where the process control activity, as currently designed, no longer addresses the PRP, the control needs to be modified.

A change in the process or a change in the PRP could necessitate a change in the process control activity.


Risk assessment (materiality and scoping of accounts)
Chapter 3
Change in scope
Process understanding (identification of systems and risk points)
Chapter 4
Change in process
Change in control
Controls implemented to address risk points (automated, manual, service organization)
Chapter 5
Change in information used
Controls implemented over information utilized in controls
Chapter 6
GITCs over systems utilized in controls
Chapter 7

See section 3.7 for guidance on changes in risk assessment.

Practical tip

Failing to adequately respond to changes in the entity's ICFR is often a root cause of identified deficiencies. Open communication between upper management and control operators is important to identify and manage changes to the ICFR process to enable risks (and changes to those risks) to be properly identified and addressed by controls that would prevent or detect material misstatements.

5.18 Monitoring procedures over process control activities

Question 5.18.10
Is testing of process control activities performed as part of monitoring procedures?

Interpretive response: It depends. Management has several different ways they can obtain the evidence necessary to support their assessment of effectiveness of ICFR (see section 2.7).

However, if management has determined, as part of their monitoring strategy, to direct test controls, their testing may include entity-level controls (see chapter 2), process control activities (this chapter) and GITCs (see chapter 7). If the entity has an internal audit function, it typically assists in management's direct testing of internal controls.

Practical tip

Management is required to support its assessment of ICFR with direct evidence of the effectiveness of controls. A control's effectiveness cannot be inferred from the absence of misstatements detected by management or any related internal or external audit procedures. Accordingly, developing an appropriate testing plan to accumulate the evidence necessary to support management's assessment of ICFR is important.

Question 5.18.20
What is included in the direct testing of process control activities?

Interpretive response: Direct testing of process control activities includes testing their operating effectiveness. In performing this testing, management should evaluate all the factors discussed in Question 5.4.30, including whether the control is properly designed to address the PRP and operating at a level of precision to prevent or detect a material misstatement.

Question 5.18.30
What is the timing of direct testing of process control activities?

Interpretive response: SEC Regulation S-K Item 308(a) requires management of public companies to provide its report on ICFR containing its assessment of the effectiveness of ICFR as of the end of the most recent fiscal year in its annual report. Therefore, when direct testing process control activities for purposes of completing the annual assessment of ICFR, management's overall evaluation of the effectiveness of controls is as of year-end. Nevertheless, the testing of controls usually needs to begin before year-end for it to be completed in time to support the assessment included in the annual report.

In addition, given the cumulative nature of many balance sheet and income statement accounts, management may consider direct testing process control activities throughout the year to gain assurance that the controls are effective at preventing, or detecting and correcting, errors on a timely basis, including in connection with any interim financial reporting. Testing of process control activities before year-end also allows time for management to respond to any identified control deficiencies. For example, if management identifies a deficiency in the process control activity related to a cash reconciliation midway through the year, they have time to remediate the deficiency, operate the control activity appropriately for the remainder of the year, and not have a control deficiency as of their year-end assessment.

Practical tip

Communication with those charged with governance and external auditors is key when testing process control activities. When management requests that external auditors use a portion of testing performed by, for example, internal audit or others under the direction of management, alignment on timing of testing procedures, sample sizes and evidence required can reduce the burden on control operators and others by not requiring them to duplicate their efforts.

In addition, external auditors generally use the effective performance of controls to reduce the substantive procedures they perform as part of their audit. A control deficiency can result in increased substantive test work to be performed, including larger sample sizes and additional procedures. Therefore, the identification of deficient controls as of an interim date can provide sufficient time for the incremental testing to be completed.

Question 5.18.40

What is the extent of direct testing performed over a control activity?

Interpretive response: The extent of direct testing performed over a control activity depends on the frequency of the control's performance.

A process control activity over a balance sheet account or financial reporting performed at year-end may prevent, or detect and correct on a timely basis, a material misstatement as of year-end. In this instance, direct testing of the annual performance of the control at year-end may be sufficient. However, due to the cumulative nature of income statement accounts, process control activities affecting those accounts likely need to operate over the entire period to prevent or detect a material misstatement. The more frequently a process control activity is performed, the greater the extent of the direct testing performed (i.e. the number of instances of the control's operation to be tested).

Question 5.18.50
What evaluation strategies can be used in direct testing process control activities?

Interpretive response: To determine whether a process control activity is operating effectively through direct testing of control activities, one of the following evaluation strategies (or a combination of the strategies) may be applied.

Procedure	Manual	Automated
Inquiry – Whenever inquiry is used, it should not be used as the sole procedure.	May include asking the control operator to determine what they look for when performing the control and what actions they take to address exceptions. It may also include asking about the number and magnitude of outliers detected in the past and then obtaining evidence that those outliers were properly resolved in a timely manner.	May include asking the system owner to determine how the system is configured to operate the control.
Inspection	May include examining documents used by the operator in performing the control to obtain evidence to corroborate information obtained through inquiry (if performed) and evaluate the effectiveness of the control as implemented by the control operator.	May include examining the system configuration and/or code to obtain evidence to corroborate information obtained through inquiry (if performed) and evaluate the effectiveness of the control as implemented within the system.
Observation	Watching a control activity being performed by the control operator and others, such as observing key meetings or execution of inventory cycle counts.	Watching the system execute the control, such as observation of the system blocking a payment when a three-way-match fails.
Reperformance	This may include independently using the control operator's metrics, thresholds, or criteria to identify outliers or exceptions and then evaluating the control operator's follow-up on these items. When a control is reperformed, there should still be sufficient evidence showing that the control was, in fact, performed. In particular, this relates to the evidence of	This may include independently reperforming a calculation to verify the mathematical accuracy by using the information used by the control after understanding the business rules driving the calculation.

Procedure	Manual	Automated
	follow-up actions taken by the control operator, and their resolution of all identified outliers.	

Question 5.18.60

What evidence is maintained for the operation of process control activities to enable the performance of monitoring activities?

Interpretive response: Proper evidence is required to be available to enable the individual(s) performing the testing over controls to evaluate whether the process controls activities were operating effectively. This evidence should cover the operation of all the attributes of the control, including the identification, investigation, and resolution of outliers. Examples of this evidence may include notes written by control operators for each outlier, original and final copies of documents used in performance of the control, and communications or support used during the investigation process.

Practical tip

The 'example of one' is evidence of a completed instance of a control activity's operation during the current period. It includes supporting documentation showing how the control was performed, including any information used in the execution of the control such as queries, reports, or reconciliations. It may also include documentation of the related risk assessment and process, including a risk-and-control matrix. An annotated 'example of one' includes markups and references to the factors discussed in Question 5.4.30 that demonstrate how attributes, information, and precision of the control are evidenced in the performance of the control.

An 'example of one' is very beneficial to document and maintain annually to evidence the design and operation of a control for the use of management and external auditors as part of their testing procedures. Annotated 'examples of one' may also be beneficial to facilitate turnover in control operators, including the best practices described in Question 5.17.30. Other benefits of documenting and maintaining annotated 'examples of one' for control activities include:

- availability of documentation to evidence the consideration of the relevance and reliability of information used in the operation of control activities;
- availability of documentation to evidence how the control is performed and aligns with the control attributes;
- availability of documentation to evidence how process control activities operate at a level of precision to prevent, or detect and correct on a timely basis, a material misstatement;

- early issue identification and resolution of gaps in the design and implementation of control activities and related documentation; and
- ability to improve alignment of external auditors' control understanding and documentation with how management has designed and performs the control activity when provided to the external auditors.

Question 5.18.70

Is management required to test all control activities each year if using the direct testing approach?

Interpretive response: Not necessarily. For automated control activities, management could apply a benchmarking approach. Benchmarking automated controls uses a combination of:

- evidence obtained in prior monitoring periods (i.e. prior years), which establishes the baseline; and
- evidence obtained in the current year that the operation of the automated control has not changed.

Benchmarking may enable management to determine whether the automated control is implemented and operating effectively in the current period.

Practical tip

If management expects their external auditors to rely on management's direct testing of control activities, they should discuss with the auditors the possibility of using or changing to a benchmarking approach because there are limitations on an auditor's ability to rely on this approach.

Key takeaways

- A properly designed process control activity addresses the PRPs it is intended to address and operates at a level of precision that 'would' prevent, or detect and correct on a timely basis, a material misstatement.
- Control attributes need to be specific and sufficiently detailed for the control operator to understand what is expected of them in executing the control attributes and for the control to be performed consistently each time it is executed.
- Management should consider whether manual or automated controls are the most suitable in achieving a control objective, and use a mix of preventive and detective controls in their ICFR.
- The precision of a control increases when the frequency and consistency of its performance increases. Management considers if the control would prevent, or detect and correct, a material misstatement on a timely basis when determining the frequency.
- Control operators should have the authority within the organization to enforce the control's operation or correct its results, and the knowledge (including knowledge of the entity) and skills to effectively perform the control the way it was designed. As the level of judgment required by, and complexity of, a manual control increases, so does the necessary level of authority and competency of the control operator.
- Control activities involving judgment require more evidence and documentation to show how the control is designed and operated.
- The precision of a process control activity is the size of a potential misstatement the control activity would prevent, or detect and correct on a timely basis, when it operates effectively.
- Control operators should evidence the criteria for investigation used in the performance of the control, the outliers that were identified in performing the control, and how the outliers were resolved.
- If the performance of a control activity does not regularly identify outliers, careful consideration should be made of whether the control is designed to operate at a sufficiently precise level to address the control objective.
- Management should design control activities that address the risks associated with journal entries and other adjustments, including the completeness, existence and accuracy of recorded journal entries, and risks of management override of controls through manual journal entries and other adjustments.
- Management should design controls that would identify significant unusual transactions (SUTs) as well as related party transactions, even if no transactions occur in the period.
- Designing controls that operate on a sample basis requires careful consideration of whether the control achieves the control objective and

addresses the identified risk. Instances of controls that operate on a sample basis are expected to be rare.

- Changes to controls, or changes to the operator of a control, need to be identified timely and management should evaluate whether the change impacts the control's ability to address the objective of the control.

6. Information used in controls

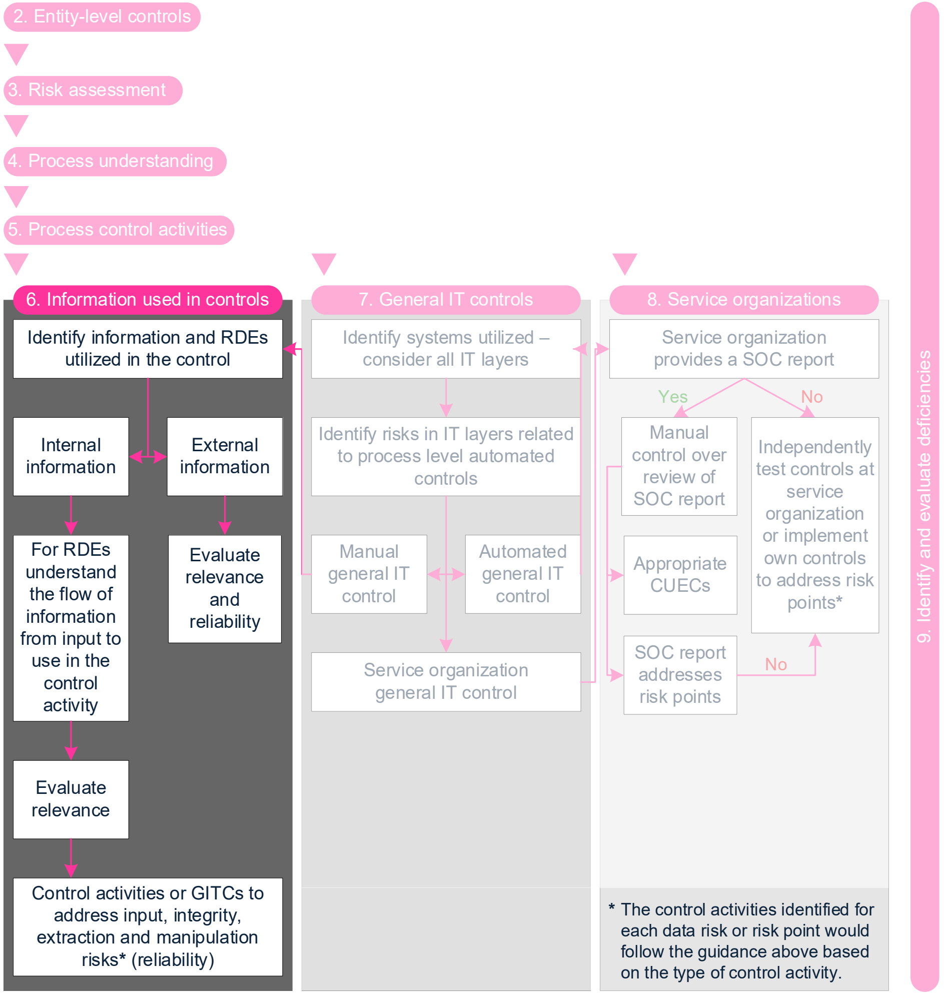
Detailed contents

Examples

Key takeaways

6.1 Management’s ICFR journey

As stated in the COSO Framework, “Information is necessary for the entity to carry out internal control responsibilities to support the achievement of objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of internal control.” Simply put, appropriately identifying and assessing the relevance and reliability of information used in controls is critically important to ICFR.


2. Entity-level controls
3. Risk assessment
4. Process understanding
5. Process control activities
6. Information used in controls
Identify information and RDEs utilized in the control
Internal information
External information
For RDEs understand the flow of information from input to use in the control activity
Evaluate relevance and reliability
Evaluate relevance
Control activities or GITCs to address input, integrity, extraction and manipulation risks* (reliability)
7. General IT controls
Identify systems utilized – consider all IT layers
Identify risks in IT layers related to process level automated controls
Manual general IT control
Automated general IT control
Service organization general IT control
8. Service organizations
Service organization provides a SOC report
Yes
No
Manual control over review of SOC report
Independently test controls at service organization or implement own controls to address risk points*
Appropriate CUECs
SOC report addresses risk points
No
* The control activities identified for each data risk or risk point would follow the guidance above based on the type of control activity.
9. Identify and evaluate deficiencies

This chapter starts by discussing information associated with a control and how it is identified (see section 6.2) and then delves further into assessing the relevance and reliability of external and internal information used in controls (see sections 6.3 and 6.4, respectively). An interactive PDF that summarizes the contents of this chapter and may be used in the day-to-day work on information used in controls is included in Appendix D.

The process of understanding and identifying controls and assessing the relevance and reliability of the related information involves management and others with ICFR responsibilities, such as control operators and IT personnel.

As part of this process, management identifies the data elements in the information, which are the units or types of data included in the information. One piece of information may have one or more data elements. Management's process also involves identifying information as external or internal. Doing so requires consideration of the information's source, as well as other factors that could result in information from an external source being treated as internal information.

Once information used in controls is identified and the source is determined, management assesses the information's relevance and reliability. To assess the relevance and reliability of a piece of information, management assesses the relevance and reliability of each relevant data element in the information.

Management's evaluation of the reliability of external information considers the information's nature and source. Management's evaluation of the reliability of internal information involves understanding the flow of information and whether the data risks associated with that information are addressed by:

- a control attribute of the control activity;
- a control attribute of another control activity that uses the same information; and/or
- a control activity specifically designed to address the completeness and accuracy of the information.

For the control attributes of a control activity to support the completeness and accuracy of internal information, those attributes must address the data risks present in that information. These risks relate to data input, data integrity, and data extraction and manipulation.

Throughout the process of identifying information used in controls and assessing its relevance and reliability, management considers whether it has identified **all** such information and clearly documented its assessment of the information's relevance and reliability. If information used in a control is not clearly identified and/or its relevance and reliability are not properly addressed, the control using the information is deficient.

Abbreviations

We use the following abbreviations in this chapter.

COSO	Committee of Sponsoring Organizations of the Treadway Commission
GITC	General IT control
ICFR	Internal control over financial reporting
RAFIT	Risk arising from IT
RDE	Relevant data element
SOC	System and Organization Controls

6.2 Identification of information in controls

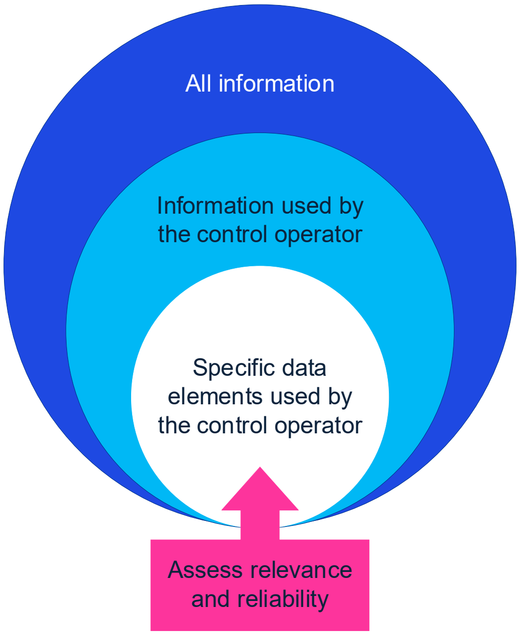
Question 6.2.10
What information is identified related to a control?

Interpretive response: Management identifies all information associated with the control. There are two types of information:

Information that is the subject of the control

Information used in the control

Most manual controls involve information – determining the type will guide management's response to the information. While it is important to identify all information associated with a control, it is critical for management to separately identify information used by the control operator, and specifically what individual data elements (see Question 6.2.40) are relied on, to determine what requires further attention from management. If information used by the control operator is not identified and/or controls over the relevance and reliability of information used do not exist or are not designed and/or operating effectively, the control will be deficient.


All information
Information used by the control operator
Specific data elements used by the control operator
Assess relevance and reliability

Question 6.2.20
What is information that is the subject of the control?

Interpretive response: Information is the subject of the control when the relevance and reliability of the information itself is directly addressed by the control objective and therefore no further assessment over the information is necessary by management.

For example, consider a process control activity where management reviews the bank reconciliation to determine if the reconciliation has been properly performed. The bank reconciliation directly addresses the accuracy of the cash recorded in the financial statements establishing its relevance, and management's review addresses the reliability of the bank reconciliation. Therefore, in this example, the information (the bank reconciliation and the related documents supporting the various reconciling items) is the subject of the control and therefore the reliability of the information is addressed through the performance of the control.

Question 6.2.30
What is information used by the control operator to perform the control?

Interpretive response: Information used by the control operator to perform the control includes any information that is relied on by the control operator to effectively execute the control.

For example, a credit limit exception report is used by the control operator to evaluate customers with outstanding balances greater than their approved credit limit. The process control activity will only be effective at identifying and following up on specific outliers if the credit limit exception report is complete and accurate. As such, the credit limit exception report is relied on by the control operator in performing the control.

Question 6.2.40
What are the specific data elements within information that are used in the control?

Interpretive response: A data element is a unit or type of data included within a piece of information. Data elements include both financial and nonfinancial data used in a calculation, selection or other manipulation of the information (e.g. to sort, filter or group data).

If the information used in the control has more than one data element, management identifies each of the specific data elements that are used in the control (RDEs) and evaluates whether those RDEs are sufficiently relevant and reliable. Data elements that are not used in the control do not need to be assessed for relevance and reliability.

For example, the control operator uses a report of all journal entries as part of the process control activity related to the review of all manual journal entries to verify that the entries were posted in the correct period, by an appropriate user, for the correct amount, and for a valid business purpose. The aging report has six data elements for each journal entry, and management identifies the four specific data elements used in the process control activity, i.e. the RDEs.

Data element	Used in the control
Journal entry number	No
Journal entry type code (e.g. manual or automated entry)	Yes
Journal entry date	Yes
Debit/credit amount	Yes
Username (i.e. user who posted the entry)	Yes
Description of the entry	No

Journal entry type code, date, debit/credit amount, and username are all used by the control operator as these data elements are relevant to the review of manual entries for the period.

Practical tip

In some cases, it is easier to identify RDEs by working backward from the final control product to the information source. This can assist in narrowing down the data elements used in the control.

Question 6.2.50

Why does management need to identify the specific data elements within information that is used in the control?

Interpretive response: Management identifies the specific data elements used in the control so that the consideration of the relevance and reliability of the information is targeted. The data elements targeted are those that affect the control operator's decision or support a key input or assumption; these are relevant data elements.

If information used by the control operator to perform the control is not relevant and reliable (i.e. accurate and complete), there is a deficiency in the design of the control (see Question 6.4.180).

Question 6.2.60

What does reliability of information mean?

Interpretive response: Reliability as it relates to internal information in a control equates to:

Reliability = Complete + Accurate

This means that such information contains:

- all the data that is necessary;
- only the data that is necessary; and
- data that is correct.

'Accuracy' in this context also relates to the way the data is manipulated and presented in a report, such as groupings, calculations based on the data, and totals in the report.

Reliability as it relates to external information in a control is a more qualitative analysis that considers factors related to the nature and source of the information. See Question 6.3.30 for more detailed information about these factors.

Question 6.2.70

What does relevance of information mean?

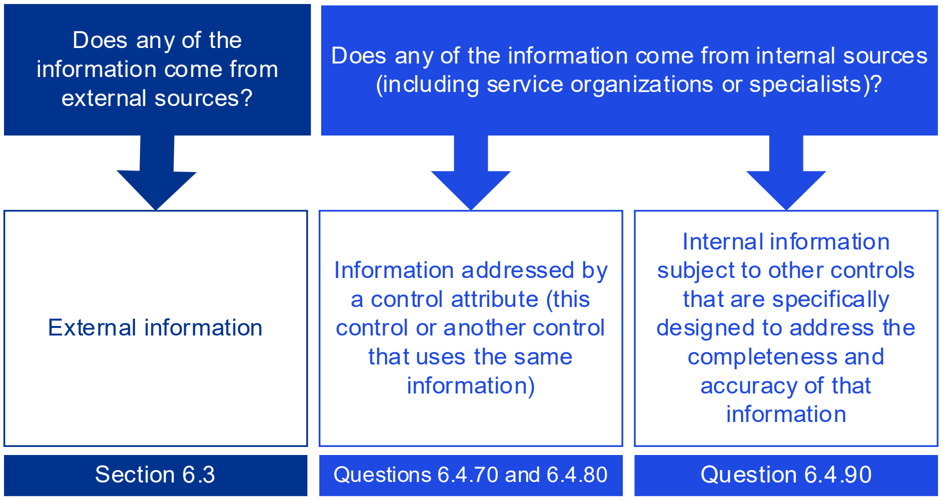
Interpretive response: Relevance is the relationship between the information and the objective of the control where the information is used. Information is sufficiently relevant when it has a logical connection or relationship with the objective of the planned control and is precise and detailed enough to meet the objective of the planned control.

Question 6.2.80

What are the different forms of information?

Interpretive response: Information used in the control may take various forms. Whether the information is from internal sources or external sources, it is important to identify the information (see Questions 6.3.10 and 6.4.10 for additional discussion of external and internal information, respectively).

Depending on the nature and source of the information, the relevance and reliability may be addressed differently. Each of these forms of information is discussed in upcoming sections of this chapter.



Does any of the information come from external sources?

Does any of the information come from internal sources (including service organizations or specialists)?

External information

Information addressed by a control attribute (this control or another control that uses the same information)

Internal information subject to other controls that are specifically designed to address the completeness and accuracy of that information

Section 6.3

Questions 6.4.70 and 6.4.80

Question 6.4.90

6.3 Relevance and reliability of external information

Question 6.3.10

What is external information?

Interpretive response: External information is information that is used by the entity that originates from a source (individual or organization) outside of the entity (i.e. an external source).

Examples of external information are listed below. Note that the list does not include information from service organizations or management's specialists, as these are typically considered internal information. Section 8.10 discusses information from service organizations. Question 4.5.230 discusses information from management's specialists.

- Contracts/Purchase orders
- Vendor invoices
- Insurance policies
- Mortgages
- Foreign exchange rates
- Periodic statements, such as bank statements
- Shipping documents
- Company share prices
- Loan agreements
- Royalty or usage reports
- Interest rates
- Market, industry or competitor information, including forecasts

- Rental agreements for both operating and finance leases
- Information received from licensees or collaborators
- Prices from a pricing service and pricing-related data, suitable for a broad range of users for a fee

Question 6.3.20

What does management consider when assessing the relevance of external information used in a control activity?

Interpretive response: Relevance of external information used in a control activity is often very simple to assess because it is often obvious. For example, relevance of bank statement information is clear from the objective of the control and the control attributes performed and documented in a bank reconciliation control. However, assessing the relevance of information is not always that obvious.

For example, consider a process control activity to evaluate whether the entity's discount rate is reasonable. The control operator obtains the discount rate from 10 publicly traded companies and assesses which of the 10 are relevant to the objective of the control. When evaluating the relevance of the discount rates, the control operator might consider the size, capital structure, industry, etc. of each of the 10 companies compared to the entity.

Specific to controls, the relevance of the information used depends on:

- the account balances, disclosures or assertions to which the information relates and the design of the control;
- whether there have been changes in the information or the account to which the information relates;
- the aggregation of the information;
- the period of time to which the information relates, and its age; and
- the timing of the control.

For example, when performing a process control activity over bank reconciliations monthly, the information used should be at a sufficiently detailed level and for the appropriate period (e.g. the bank statement for the month the control is performed over).

Practical tip

Control operators should maintain documentation of their assessment of relevance to evidence management’s ICFR environment. The control operator should consider if they need to reassess relevance with each control operation due to changes in circumstances. For example, if the entity begins operations in a new market or line of business, a control that uses information from comparable entities will need to be revisited to assess whether those entities are still comparable – i.e. relevant – given the change to the entity’s own business.

Question 6.3.30

What does management consider when assessing the reliability of external information used in a control activity?

Interpretive response: In assessing the reliability of external information, management considers the nature and source of that information. Management may consider the following factors when evaluating the reliability of information obtained from an external source.

Reliability factors	
Source	**Nature**
• The competence and reputation of the external source with respect to the information • Past experience with the reliability of the information provided by the external source • Extent of regulatory oversight of the external source • The ability of management to influence the information obtained through relationships with the external source	• Whether the external source accumulates overall market information or engages directly in 'setting' market transactions • Whether the information is suitable for use in the way it is being used and, if applicable, was developed using the applicable financial reporting framework • Whether the information has been subject to review or verification by the external source or another external party • Whether the information has been originated, aggregated, or adjusted by the external source

Sometimes it is helpful to think about the nature of the information in terms of where it falls on a spectrum of reliability. The following diagram includes factors that may indicate information is more or less reliable.

Less reliable	More reliable
• No evidence of general market acceptance of its reliability when used for a similar purpose	• Evidence of general market acceptance of its reliability when used for a similar purpose
• Lack of corroboration through other sources	• Corroboration through other sources
• Existence of contradictory alternative information	• Lack of contradictory alternative information
• Substantive disclaimers or restrictive language	• Limited or no disclaimers or restrictive language
• Obtained through a complex process	• Obtained through a straightforward process

Practical tip

Control operators should maintain documentation of their assessment of reliability to evidence management's ICFR environment. The control operator should consider if they need to reassess reliability with each control operation due to changes in circumstance. For example, if a control relies on information from an external party that has been historically reliable, but concerns have recently been raised as to their reputability, the assessment of reliability will need to be revisited to determine whether the external source is still reliable given the change in circumstances.

Question 6.3.40
What if external information is stored in the entity's IT systems?

Interpretive response: If management stores external information in the entity's IT systems, the relevance and reliability of the external information up to the point at which it is transferred onto the entity's IT systems should be addressed is in accordance with Questions 6.3.20 and 6.3.30 above. From the point of transfer, the relevance and reliability should be addressed in accordance with the guidance in section 6.4.

6.4 Relevance and reliability of internal information

Question 6.4.10
What is internal information?

Interpretive response: Generally, internal information originates from the entity, whereas external information originates from a source outside of the entity (i.e. an external information source) (see Question 6.3.10). Additionally, if information from third parties is developed specifically for use by the entity, it is considered internal information. External information that originates from a source outside of the entity that has been manipulated once received by the entity is considered internal information.

Examples of internal information

- Trial balances/subledgers
- Analyses of subledgers or balances
- Rollforward schedules
- Listings of transactions
- Spreadsheets, cost allocations, computations, and reconciliations
- Queries

Examples of internal information

- Budgets/forecasts
- Minutes of meetings
- Internal audit reports
- Information provided by a service organization (see section 8.10)
- Internal marketing information (e.g. information developed by the entity's sales function is an assumption in making an accounting estimate for a warranty provision)
- Prices from a pricing service for specific financial instruments not routinely priced for its subscribers

Question 6.4.20

What does management consider when assessing the relevance of internal information used in a control activity?

Interpretive response: Relevance of internal information used in a control activity is often very simple to assess because it is often obvious. For example, relevance of a listing of PP&E additions is clear from the objective of the control and the control attributes performed and documented in a roll forward of PP&E control. However, assessing the relevance of information is not always that straightforward. The assessment of relevance is the same for external and internal information. Accordingly, it is important to consider the factors listed in Question 6.3.20 and whether the information is precise and detailed enough to meet the objective of the planned control.

For example, when performing a process control activity over the recoverability of accounts receivable monthly, the information used should be at a sufficiently detailed level (e.g. the customer or transaction level) and for the appropriate period.

Question 6.4.30

What does management consider when designing control activities to address the reliability of internal information?

Interpretive response: To design control activities, management:

- understands the flow of information;
- identifies the risks related to the information (the data risks); and
- designs control activities to address the data risks.

Given the nature of entity level controls, the extent of procedures to evaluate the reliability of information used in entity level controls is different. See Question 2.3.70 for consideration of reliability of information used in entity-level controls.

Question 6.4.40

Why does management understand the flow of information?

Interpretive response: To identify the risks to internal information and data elements, it is important for management to understand the flow of information and data elements through the information system(s) back to the point of origin/data input. When determining the source of the information, management needs to consider all systems that the data passes through, from the originating control activity that verifies the data was correctly input into the system to the point of extraction.

For example, if information is entered into a sales or billing system that is then transferred to the general ledger system where the information is extracted, both systems need to be considered. However, if the data is entered directly into and extracted directly from the sales system, only one system needs to be considered.

Identification of the systems will assist management in identifying the related data risks and the necessary control activities that address the risks over the specific data elements.

Practical tip

When understanding the flow of information from the source, it can be beneficial to involve others in the discussion, including IT personnel (see Question 6.4.190). Flowcharts or other documentation created as part of process understanding (see chapter 4) may help in tracing information from the source to the extraction point.

Question 6.4.50

What are the data risks?

Interpretive response: There are three types of data risk – data input, data integrity, and data extraction and manipulation. Each data risk needs to be addressed by control activities to address the completeness and accuracy of internal information. The following table includes example risks for each type of data risk.

Data risk	Example risks
Input risks	• Data is incompletely or inaccurately entered into the IT system or not properly converted from its original source to electronic form. • Data arising from hard-copy source documents or electronic data interface (EDI) may be compromised before input.
Integrity risks	• Data is inappropriately altered during processing. • Data is inappropriately altered while in storage. • Data does not accurately transfer from one system to another. • Data is not valid.
Extraction and manipulation risks	• The information does not contain all data when extracted. • The information contains additional data when extracted. • The manipulation of data used to produce the information is incorrect or inaccurate.

Question 6.4.60

What forms of control activities address data risks?

Interpretive response: The reliability (or completeness and accuracy) of internal information and specific data risks could be addressed by:

- a control attribute of the control activity (see Question 6.4.70);
- a control attribute of another control activity that uses the same information (see Question 6.4.80); or
- separate control activities that are specifically designed to address the completeness and accuracy of the information (see Question 6.4.90).

Each data risk may be addressed through one or multiple forms of controls. See Example 6.4.10.

Question 6.4.70

When does a control attribute within the control activity address its completeness and accuracy?

Interpretive response: The completeness and accuracy of information is addressed by a control attribute within the control activity when the control operator performs a step that results in the verification of the completeness and/or accuracy of the information. This includes addressing the three types of data risk discussed in Question 6.4.50.

Often, for non-system generated information that is manually maintained (e.g. Excel spreadsheets), control operators address the completeness and accuracy of the information through control attributes within the control activity. For example, for the net income data element in an Excel spreadsheet used to track debt covenant compliance, the control operator agrees net income to the consolidating income statement to assess completeness. For another example, the data elements and related data risks in an Excel spreadsheet used to calculate interest expense are verified by the control operator performing the following control attributes.

Data element	Control attribute	Data risk and how addressed through attribute
Interest rate	Agrees to signed third-party loan agreement	• Input risk – addressed as agreed back to a signed third-party document • Integrity and extraction risk – N/A as agreeing to original so no risk of data being inappropriately modified after input and data is not extracted • Manipulation risk – addressed through the steps over interest expense
Loan amount		
Interest expense	Recalculates based on verified interest rate and loan amount	• Input, integrity and extraction risk – addressed through the steps over interest rate and loan amount • Manipulation risk – addressed through the recalculation of RDE

Question 6.4.80

When does a control attribute in another control activity address the completeness and accuracy of internal information?

Interpretive response: The completeness and accuracy of internal information can be addressed when a control attribute of a different control activity addresses the completeness and accuracy of the same information. This includes addressing the three types of data risk discussed in Question 6.4.50.

This approach can only work effectively if the two control activities use the same information for the same timeframe. Determining whether the information is the same can be tricky. For example, consider a scenario in which the information represents reports that are extracted, and the completeness and accuracy of those reports as extracted are addressed in another control activity. The reports are then manually manipulated as part of the current control activity (e.g. formulas are added to an extracted report to produce a total column). Therefore, in this scenario, the additional risks associated with the manual manipulation of the reports are not covered in the other control activity.

Practical tip

When designing new control activities or modifying control activities, management should consider the source of information used by the control operator and whether there is information that is already addressed by a separate control activity that can be relied on. This may be more efficient and effective than running a new report or using a separate source for the same information. Agreeing the information directly to the report used in the other control activity helps confirm that the information is the same in both control activities.

Example 6.4.10

Relying on another control activity to address the completeness and accuracy of internal information

A control operator reviews the equity rollforward on a quarterly basis. The control operator agrees the share repurchases on the equity rollforward to the repurchase schedule using the data elements of the repurchase date and repurchase value. The repurchase schedule is information that is used in the process control activity.

There is a separate quarterly process control activity where a control operator reconciles the same repurchase schedule, including the same data elements mentioned above, by:

- agreeing them to information from the registrar;
- agreeing them to the bank statement; and
- evaluating whether all transactions included in the information from the registrar are reflected in the repurchase schedule.

Therefore, the internal information (repurchase schedule) used in the process control activity over the equity rollforward, and the related specific data elements, are addressed by a control attribute in another process control activity that covers the completeness and accuracy of the same information.

The following table outlines the data elements, the control attributes that address them and how the data risks are addressed through those attributes.

Data element	Control attribute	Data risk and how addressed through attribute
Beginning balance Net income loss	Agree to the trial balance	• Input risk – addressed through agreeing back to the trial balance • Integrity and extraction risk – N/A as agreeing to trial balance so no risk of data being inappropriately modified after input and data is not extracted. • Manipulation risk – addressed through the recalculation of the period-end balance

Data element	Control attribute	Data risk and how addressed through attribute
Stock compensation expense	Agree to the stock compensation schedule (not included in the example)	• Addressed in the control over the stock compensation schedule
Share repurchase amount	Agree to the share repurchase schedule	• Addressed in the control over the repurchase schedule
Period-end balance	Recalculates based on other inputs	• Input, integrity and extraction risk – addressed through the steps over beginning balance, income, stock compensation expense and share repurchase amount • Manipulation risk – addressed through the recalculation of RDE

Share repurchase schedule control		
Data element	**Control attribute**	**Data risk and how addressed through attribute**
Amount of stock buyback	Agree to the bank statement and third-party repurchase notice	• Input risk – addressed through agreeing back to the third-party bank statement and information from the registrar • Integrity and extraction risk – N/A as agreeing to third-party bank statement and the registrar so no risk of data being inappropriately modified after input and data is not extracted • Manipulation risk – addressed through the recalculation of the total repurchase amount for the period
Date		
Total stock repurchase amount for period	Recalculates based on other inputs	• Input, integrity and extraction risk – addressed through the steps over amount of stock buyback • Manipulation risk – addressed through the recalculation of RDE

Consideration should be given to whether all data elements being relied on in the current control activity are addressed for completeness and accuracy through the other control activity. If the repurchase date's completeness and accuracy was not addressed in the process control activity to reconcile the repurchases, it could not be relied on in the equity rollforward process control activity.

Question 6.4.90

When is internal information subject to separate control activities that are specifically designed to address the completeness and accuracy of that information?

Interpretive response: If the completeness and accuracy of the information used by the control operator to perform the control is not addressed by an attribute of the control itself, or through an attribute of another existing control, separate control activities must be designed and implemented. When separate control activities are specifically designed to address the completeness and accuracy of information, especially around extraction risk, they are typically information controls. Information controls are generally used as the method to address the completeness and accuracy of internal information in:

- 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); and
- schedules created using end-user computing applications (i.e. end-user computing schedules).

Question 6.4.100

What is data input risk and how is it addressed through separate control activities?

Interpretive response: Data input risks are risks that the information being relied on is incomplete or inaccurate due to how the information was initially obtained and input into the system.

Example risks	Control consideration
• Data is incompletely or inaccurately entered into the IT system or not properly converted from its original source to electronic form. • Data arising from hard-copy source documents or EDI may be compromised before input.	The specific risk and related control activities differ depending on the source of the data and how the data gets into the IT system – EDI versus manual input of data from source documents.

Input risks may be addressed by process control activities over risk points when the information is first entered into an IT system, including consideration of proper authorization of transactions as specified by an entity's established policies and procedures (e.g. approval of a transaction by a person having the authority to do so).

Some entities design process control activities to address input risk in a system that is not the originating system. For example, procurement-related transactions may originate in a procurement system; however, process control activities over the input of the data (e.g. three-way match and expenditure review/approval controls) may occur in a downstream system.

Question 6.4.110

What is data integrity risk and how is it addressed through separate control activities?

Interpretive response: Data integrity risks are risks that the information being relied on is incomplete or inaccurate due to how the information is maintained within the system(s).

Example risks	Control consideration
• Data is inappropriately altered during processing. • Data is inappropriately altered while in storage. • Data does not accurately transfer from one system to another. • Data is not valid.	If data is changed/processed by an IT system(s) or is transferred electronically from one system to another, then control activities are identified related to: • the processing and/or transfer of the data; and • the GITCs that address risks that could affect the control activities' consistent operation. When data is stored in an IT system, evaluating and testing GITCs that address the applicable risks for the relevant IT system layer (e.g. database) may be sufficient to address the data integrity risk (see chapter 7 for discussion of GITCs). In more complex scenarios (e.g. when data is processed or transferred to another system), management may also identify risk points in the process and evaluate and test controls outside of GITCs including automated process control activities to address the data integrity risk.

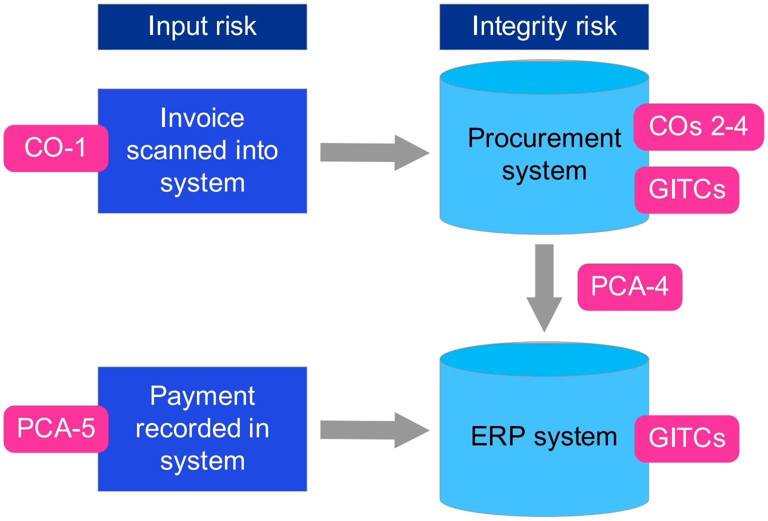
Integrity risk is generally addressed through GITCs over the systems identified by management used to generate the information used in the control. Situations in which data transfers between multiple systems tend to involve more control activities and risk points. At each point where information transfers to a new IT system, management considers whether there is data transfer risk that needs a process control activity to address the completeness and accuracy of the data transfer. This process control activity can be automated, manual or a combination of both.

The entity evaluates whether GITCs are designed and operating effectively in systems in which management is relying on automated process control activities (e.g. configuration controls related to extracted reports) to address processing and data transfer risks related to data integrity.

Question 6.4.120

How are data input and integrity risks considered if information originates in multiple systems?

Interpretive response: Data elements can originate in different systems, which can result in different risk points and control activities for different data elements from the same information/report. For example, consider an invoice payment report. The data elements identified are the invoice number, invoice amount, date, payment date and payment amount. While the invoice information originates in the procurement system (which resides at a service organization), the payment information is directly entered into the ERP system where the information is extracted. This results in different process control activities addressing data input risk for the data elements. In addition, more control activities are necessary to address data integrity risk for the procurement system and movement of data between systems. Using a diagram, the flow of information and the control activities that address the risks of input and integrity can be more easily visualized (CO – control objective in the SOC-1 report from the service organization; PCA – process control activity).



In this diagram, the risks are addressed by the following.

System	Input risk	Integrity risk
Procurement system	Control Objective 1 from the service organization report	Control Objectives 2, 3 and 4 from the service organization report GITCs that respond to Risks arising from IT (RAFIT) over integrity risk
Transfer between systems		Process control activity 4
ERP system	Process control activity 5	GITCs that respond to RAFITs over integrity risk

Question 6.4.130
What are data extraction and manipulation risks?

Interpretive response: Data extraction and manipulation risks are risks that the information being relied on is incomplete or inaccurate due to how the information is pulled from the system and/or subsequently altered.

Example risks	Control consideration
• The information does not contain all data when extracted. • The information contains additional data when extracted. • The manipulation of data used to produce the information is incorrect or inaccurate.	Data extraction and manipulation risks are present for all types of information obtained from IT systems – including system-generated reports, custom reports and end-user computing-schedules (including Excel, Alteryx, Power BI and other tools). An entity's use of custom reports and end-user computing schedules increases data extraction and manipulation risks.

The risk over data manipulation will vary based on where the data is extracted to and if there is intentional manipulation after extraction. Most information has some risk of manipulation after extraction. In many cases, information is extracted into Microsoft Excel, Microsoft Access, etc. and many entities are using additional tools such as Alteryx and Power BI where the data is intentionally manipulated or has a risk of being unintentionally manipulated.

Question 6.4.140
How is internal information extracted from its source?

Interpretive response: Generally, internal information is extracted from its source using the following methods.

- Configuration reports or 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 (sometimes referred to as canned reports) or custom-created by either the software vendor or management to meet the specific needs of the entity. Canned reports in many cases require the end user to select parameters before running the report, but management does not have access to the report code or ability to modify the report beyond the parameter selection.

- Query reports are custom reports that are written by management using query language (e.g. SQL queries).

- Report writer reports are custom reports that use a separate tool or report writer application to pull the report from the system (e.g. Crystal Reports, Essbase). The end user usually is required to select inputs to run the report.

- Service organization reports are those provided to the entity that involve no intervention by management as part of the extraction (e.g. the service organization emails management the report). If management extracts information from a service organization system, it would fall in one of the other sources.

Question 6.4.150

How is data extraction risk addressed through separate control activities?

Interpretive response: Management considers the nature of the report, including the method used to extract the data in the report from its source, to determine how the data extraction risk is addressed.

Nature of report	How to address data extraction risk	Additional considerations
Configuration	An automated process control activity over the configuration of the report or a manual process control activity(s) over the completeness and accuracy of the information.	
Query and report writer	A process control activity over the configuration of the custom report or the control operator reviews the query or extraction script.	When a report writer is used, the integrity of the data flowing to the tool and the integrity of the information while in the tool also needs to be considered and addressed.
Service organization	A process control activity or control objective within the SOC report that explicitly identifies the information and addresses the completeness and accuracy of the report.	See chapter 8 for guidance on use of SOC reports.

For all reports, if parameters are entered by the control operator to extract the report, there is an extraction risk that should be addressed through a manual process control activity (generally an attribute within the control using the information).

Tools and programs that use routines (e.g. macros in Excel, Alteryx) to process data or those that filter data (e.g. Power BI) are also subject to data manipulation and extraction risk. The entity should design and implement controls over the completeness and accuracy of the information in and out of the tools as well as over the configuration of the routine or filters used. This is similar to controls over information in a query or report writer.

Practical tip

Reports may be generated from off-the-shelf applications where management does not have access to make changes to the code. These reports are often called canned, standard or system reports, as they are developed by the vendor that provides the IT system and management cannot make changes to the reports that come from these applications. In contrast, custom reports (such as SQL reports) have parameters that are established by an IT developer. Custom reports are more prone to have information (e.g. data elements, records) inappropriately excluded or included. When designing new control activities that require information from a custom report developed specifically for that control activity, proper review of the development of the report should occur by the control operator upfront and whenever the report is modified.

Question 6.4.160

How is data manipulation risk addressed through separate control activities?

Interpretive response: Management considers where the data is extracted to and whether it is intentionally manipulated or has a risk of being unintentionally manipulated.

Control activities over manipulation risk can be a combination of:

- process control activities to check that the logic is functioning as intended (e.g. controls that reconcile the report to the data from which it was derived and compare the individual data from the report to the source and vice versa);
- use of validation software tools that systematically check formulas or macros (e.g. spreadsheet integrity tools); and
- use of access restrictions (e.g. password-protected server locations with restricted access and version controls).

Data manipulation risk generally occurs for each instance of the control activity's operation. For example, data manipulation risk occurs each time a report is moved into Excel and the data within it is sorted and filtered and/or calculations are added.

Practical tip

Embedding the control attribute to address data manipulation risk into the attributes for the control activity that is using the information will assist in ensuring the consistent operation and documentation of how the risk is addressed.

Example 6.4.20

Internal information subject to separate control activities that are specifically designed to address the completeness and accuracy of that information

Payroll information is uploaded from the HR system to the financial reporting system. On a monthly basis, a control operator reconciles the payroll register to the general ledger (GL) and investigates any variances. The control operator relies on the payroll register from the HR system to agree to the Interface summary and the GL. As the GL and the payroll summary reports are the subject of the control, the completeness and accuracy are addressed through the control. Therefore, the payroll register is identified as information. It is extracted from the HR system through a configuration report. Gross earnings, taxes, deductions and net earnings are identified as RDEs.

For purposes of this example we will assume all RDEs are addressed through the same controls.

Data risk	How data risk is addressed
Input	• Controls over input of payroll into the HR system (timesheet, salary rates, hiring controls, etc.) • Controls over calculation of taxes, deductions and net earnings • Monthly payroll variance control
Integrity	• GITCs over HR system database layer
Extraction	• Control over the extraction of the report including a test of one agreeing each RDE from the system to the report and agreeing the total
Manipulation	• As the report is exported into Excel, the control operator agrees the total of each RDE back to the system to confirm that no manipulation has occurred. No further changes are made to the Excel file for purposes of the control.

Question 6.4.170

Can management assume information received directly from a service organization is reliable?

Interpretive response: No. Even if information is received directly from a service organization with no intervention by management (e.g. the service organization emails management the report), management cannot assume the information is complete and accurate or that there are control activities addressing its completeness and accuracy. Generation of information by a service organization does not make the information complete and accurate unless the information is explicitly identified and subject to control activities captured in the SOC 1 report or if other procedures are performed to confirm with the service organization and the service auditor that controls have been performed over the completeness and accuracy of the information.

Many SOC 1 reports do not explicitly identify the information or reports provided to user entities. Therefore, management may need to perform additional procedures to determine whether a SOC 1 report addresses the risks over information produced by the service organization. These procedures may include:

- inquiring of the service organization and/or service auditor to understand how the control objectives and related controls included in the Type 2 SOC 1 report address the accuracy and completeness of the information, including the relevant data elements;
- reviewing the control objectives and tests of controls performed by the service auditor to determine if the accuracy and completeness of relevant data elements in the information used by management are addressed by the control objective and tests of controls;
- reviewing the control objectives to determine if the Type 2 SOC 1 report includes a control objective, control activities and tests of controls related to the accuracy and completeness of the output produced by the service organization;
- reviewing 'Management's Description' in the Type 2 SOC 1 report to determine if the information is specified as being produced for user entities; and
- inspecting the service level agreement between the service organization and the user entity to determine if the information is listed as part of the service organization's output delivered to the user entity.

If the information is not addressed in the SOC 1 report or though these additional procedures, management may need to implement additional control activities over the completeness and accuracy of the information.

If management is extracting information from a service organization’s system, they consider data extraction and manipulation risks similar to how they do so for information in configuration, query and report writer reports (see section 8.10 for further guidance).

Question 6.4.180

What are the repercussions of control activities that address risks over information being deficient?

Interpretive response: When there are separate control activities that address the completeness and accuracy (including data input risk, data integrity risk, and data extraction and manipulation risk) of the information, a deficiency in **any** of those control activities renders:

- the information unreliable; and
- the control activities where the information is used deficient.

Chapter 9 provides additional information about the evaluation of deficiencies.

Practical tip

It is important to understand and document which control activities rely on the effective operation of other control activities. This is critical to appropriately evaluating the effect of a control deficiency, especially when related to control activities that address information risks for multiple manual control activities.

Question 6.4.190

Who should be involved in the identification of risks and control activities over information used in control activities and how should they be documented?

Interpretive response: When management is designing a control, it is important to involve the appropriate parties to identify the related risks and control activities over the information that will be used in the control.

Involving other control operators who are involved in the broader business process or individuals who perform monitoring activities (e.g. Internal Audit) can be helpful in identifying:

- another control activity that addresses the completeness and accuracy of the information;
- manual process control activities to address the input risks, including the risk of appropriate approval to initiate the transaction; and
- manual process control activities to address integrity risks in the movement and/or transformation of information between systems.

Involving IT personnel with knowledge of the entity's systems and how data moves between each system can be helpful in identifying:

- automated process-level controls to address the input risks associated with EDIs;
- GITCs to address the integrity risks associated with information maintained in IT systems;
- automated process control activities to address integrity risks in the movement and/or transformation of information between systems; and
- automated process control activities to address the extraction risks related to the completeness and accuracy of system-generated reports.

Consistent with the documentation requirements of the COSO Framework, management is required to document their identification of risks and how those risks are addressed.

Practical tip

Due to the complexity of internal information that is subject to sperate control activities, management may consider using a consistent template to document:

- the data elements;
- the flow of information; and

- how data input, data integrity, and data extraction and manipulation risks are addressed.

This template can include the testing of data extraction risk. If management uses a benchmarking approach (see Question 5.18.70), this template can also be used to document and track the last change date for reports.

It’s beneficial to review any template with external auditors because use of an appropriately designed template can improve not only an entity’s ICFR documentation but also streamline the related external audit procedures.

Key takeaways

- Assume information is involved in every manual control, including manual GITCs.
- The relevance and reliability (i.e. completeness and accuracy) of all information used by the control operator should be addressed and documented.
- The risks related to internal information used in a control activity can be addressed in three ways:
  - a control attribute of the control activity;
  - a control attribute of another control activity that uses the same information; and/or
  - a control activity specifically designed to address the completeness and accuracy of the information.
- When using a control attribute of another control activity to address information, be careful of modifications made to information between control activities or the use of similar but not the same report(s).
- The control attributes need to address data input, data integrity, and data extraction and manipulation risks (data risks) present in information used in a control activity.
- A control activity is deficient if any of the control attributes that address data risks for information used in the control are deficient.
- See Appendix D for an interactive PDF that summarizes the contents of chapter 6 on information used in controls and its evaluation in a user-friendly format.

7. General IT controls

Detailed contents

Examples

Questions

Example

Questions

Example

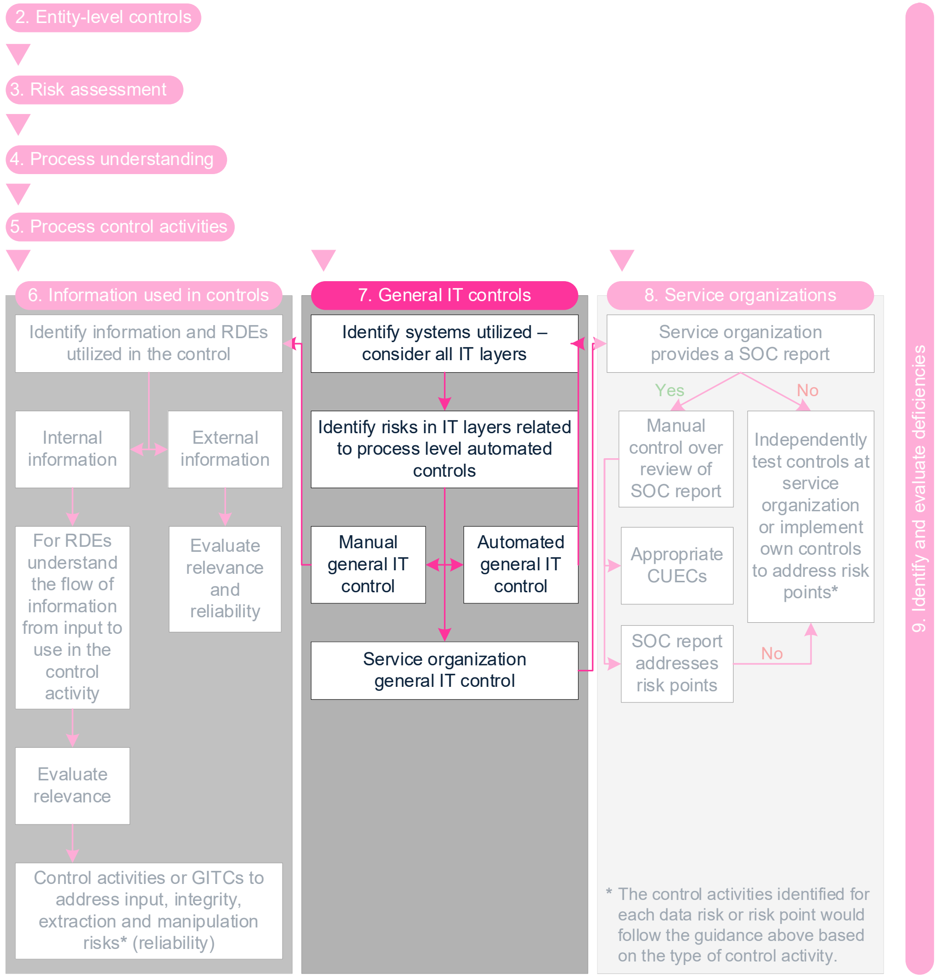
Questions

Example

Key takeaways

7.1 Management’s ICFR journey

GITCs are control activities over the entity’s IT processes that support the continued effective operation of the IT environment and the integrity of data and information within the entity’s IT system. Understanding GITCs is an important part of management’s ICFR journey because GITCs are critical to the effective operation of automated process control activities (see chapter 5) that have been identified to address risks of material misstatements (RMMs) (see chapter 3).


2. Entity-level controls
3. Risk assessment
4. Process understanding
5. Process control activities
6. Information used in controls
Identify information and RDEs utilized in the control
Internal information
External information
For RDEs understand the flow of information from input to use in the control activity
Evaluate relevance and reliability
Evaluate relevance
Control activities or GITCs to address input, integrity, extraction and manipulation risks* (reliability)
7. General IT controls
Identify systems utilized – consider all IT layers
Identify risks in IT layers related to process level automated controls
Manual general IT control
Automated general IT control
Service organization general IT control
8. Service organizations
Service organization provides a SOC report
Yes
No
Manual control over review of SOC report
Independently test controls at service organization or implement own controls to address risk points*
Appropriate CUECs
SOC report addresses risk points
No
* The control activities identified for each data risk or risk point would follow the guidance above based on the type of control activity.
9. Identify and evaluate deficiencies

Before GITCs are identified, management must first understand the IT layers within the entity’s IT system and then identify the relevant risks arising from IT (RAFITs) within each IT layer. Summary information about each is provided next, along with where additional information can be found in this chapter.

Relevant layers of IT and RAFITs (see section 7.2)	**GITCs** (see section 7.3)
- RAFITs represent the susceptibility of automated control activities to ineffective design or operation, or risks to the integrity of information in the entity’s IT systems, due to	- GITCs are not expected to directly prevent, or detect and correct, material misstatements. However, ineffective GITCs may lead to automated control activities that

Relevant layers of IT and RAFITs
(see section 7.2)

ineffective design or operation of GITCs. RAFITs may exist within the entity's processes to manage:

  - access to programs and data;
  - program changes;
  - program acquisition and development; and
  - computer operations.

- A relevant RAFIT is an IT risk where there is a 'reasonable possibility' that the risk could prevent the effective operation of the related automated control activity and/or affect the integrity of data within the IT system.
- The following four layers of technology comprise an IT system:
  - application;
  - database;
  - operating system; and
  - network.
- A layer of technology is relevant to ICFR when there is one or more RAFITs within that layer of technology that are relevant to the effective operation of automated control activities and/or the integrity of data and information within the IT system.

GITCs
(see section 7.3)

don't operate consistently and effectively, which may lead to the automated control activities not preventing, or detecting and correcting, a material misstatement on a timely basis.

- GITCs can be either manual or automated. A common example of a manual GITC is a periodic user access review. An example of an automated GITC is restricting access to make system changes to only authorized personnel in IT operations.
- Management considers a number of factors when designing and documenting a GITC, including its objective, nature, type and frequency of operation, as well as the judgment and information needed for its operation.
- Additional considerations exist when GITCs operate over multiple IT layers and when a service organization is responsible for performing control activities.
- Management is required to prepare and retain sufficient documentation to evidence the design, implementation and operation of the entity's GITCs.

Next, if management has determined to direct test controls as part of their monitoring strategy, management tests the effectiveness of the GITCs designed to address relevant RAFITs, which may result in the identification of GITC deficiencies. Additional information about both is provided next, along with where additional information about each can be found in this chapter.

Monitoring procedures over GITCs
(see section 7.4)

- GITCs are included in management's monitoring. If direct testing is performed as part of monitoring, the testing of operating effectiveness of GITCs should be performed throughout the period.
- As part of testing, management should evaluate all the factors considered when designing and documenting a GITC, including

GITC deficiencies
(see section 7.5)

- If GITCs are ineffective, management may not be able to rely on the automated control activities or the integrity of the information they support, which may impact management's conclusions on ICFR effectiveness.
- When a GITC deficiency is identified, management evaluates its severity and considers its effects

Monitoring procedures over GITCs (see section 7.4)	GITC deficiencies (see section 7.5)
whether the control is properly designed to address the RAFIT.	on the automated control activities that rely on the GITCs.

No discussion about IT-related risks is complete without discussion of cybersecurity. So, this chapter ends with discussion on the topic that emphasizes management's responsibility to:

- evaluate the risk of cybersecurity incidents and cyber-related frauds across all aspects of the entity's business operations;
- establish processes, structures and safeguards to mitigate those risks; and
- assess the effects of a cybersecurity incident on the amounts and disclosures in the financial statements and the entity's ICFR.

Section 7.6 provides additional information about cybersecurity.

Abbreviations

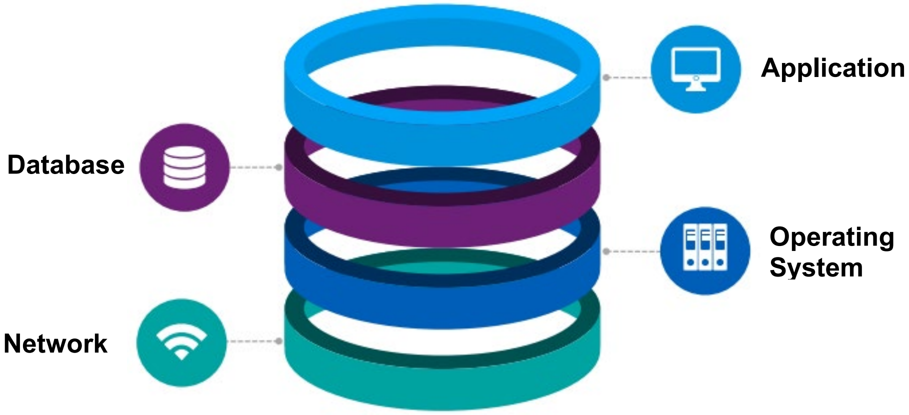
We use the following abbreviations in this chapter.

COSO	Committee of Sponsoring Organizations of the Treadway Commission
GITC	General IT control
ICFR	Internal control over financial reporting
ISD	IT System Diagram
PCAOB	Public Company Accounting Oversight Board
PRP	Process risk point
RAFIT	Risk arising from IT
RDE	Relevant data element
RMM	Risk of material misstatement
SEC	Securities and Exchange Commission

7.2 Relevant layers of IT and RAFITS

Question 7.2.10

What are the layers of technology that comprise an IT system?



Interpretive response: IT systems are comprised of four layers of technology (also referred to as IT system layers or IT layers) Application, Database, Network, and Operating System.

The database, operating system and network layers may be collectively referred to as IT infrastructure.

Each of the layers of technology may include RAFITs to be addressed by management so that:

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

The following table provides a description and examples of each layer of technology.

Description	Examples
Application	
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. For purposes of ICFR, 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.	• ERP systems, such as SAP and Oracle • Report writers (see Question 7.2.20) • Emerging technologies, such as robotic process automation and artificial intelligence • Transaction-processing systems, such as a customer relationship management or billing system

Description	Examples
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.	• SQL Server (this and similar technologies may be used by multiple IT application layers to store and retrieve information in its database) • Oracle Database • Stand-alone data repositories and data warehouses (see Question 7.2.30)
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 • MacOS
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. For example, user access to an IT application may be limited to a LAN or VPN.	• Wide Area Networks (WANs) • Local Area Networks (LANs) • Virtual Private Networks (VPNs)

Question 7.2.20

What are report writers and how are they relevant to ICFR?

Interpretive response: 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 applications 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).

Practical tip

Report writers are generally identified as a relevant application IT layer when they are used to extract information used in manual controls. The use of report writers in these controls may result in the identification of RAFITs in these IT application layers. Because of their nature, report writers are often more difficult to identify as part of the layers of technology. Question 6.4.150 provides additional considerations related to report writers.

Question 7.2.30

What is a data warehouse and how is it relevant to ICFR?

Interpretive response: Data warehouses are separate databases used as a central repository to accumulate and integrate data and information from a wide range of sources. These sources may be multiple databases or other IT systems used in financial reporting and business processes. Reports may be generated from data warehouses, or they 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.

Question 7.2.40

What are the risks arising from IT and how are they identified?

Interpretive response: RAFITs represent the susceptibility of automated control activities to ineffective design or operation, or risks to the integrity of information in the entity's IT systems, due to ineffective design or operation of GITCs. A RAFIT represents any condition that could impact the effective operation of automated control activities or the integrity of data and information within an entity's IT system.

RAFITs are identified within IT processes, which include the entity's processes to manage:

- access to programs and data;
- program changes;

- program acquisition and development; and
- computer operations.

Question 7.2.50
Is each IT process always relevant to ICFR?

Interpretive response: No. Not all IT processes affect the effective operation of automated control activities or the integrity of data and information within an IT system.

For example, program development may not affect the effective operation of automated control activities 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 risk in the computer operations process related to backup and recovery may not affect the effective operation of automated control activities or the integrity of data and information.

Example 7.2.10
Common RAFITs by IT process

The following table sets out a list of common examples of RAFITs for each IT process.

Access to programs and data
• Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data. • 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). • Logical access permissions are not revoked in a timely manner. • 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). • Physical access to facilities housing IT systems and/or electronic media is unauthorized or not commensurate with job responsibilities.
Program changes
• Changes to IT programs were inappropriate (i.e. unapproved or do not function as intended). • Changes to IT configurations were inappropriate (i.e. unapproved or do not function as intended). • Logical access to implement changes to IT system programs or configurations into the production environment is inappropriate (i.e. unauthorized or not commensurate with job responsibilities).

Program acquisition and development
• IT system developments (new components or significant changes) are unapproved or do not function as intended. • Incomplete, redundant, obsolete or inaccurate data is migrated to the production environment of acquired, newly developed or existing IT systems.
Computer operations
• System jobs, processes and/or programs do not function as intended, resulting in incomplete, inaccurate, untimely or unauthorized processing of data. • Logical access to make changes to system jobs, processes and/or programs is unauthorized or not commensurate with job responsibilities. • Financial data backups are not able to be recovered in a timely manner.

Question 7.2.60

What is a process risk point and how does it differ from a RAFIT?

Interpretive response: The following table sets out the difference between a process risk point and a RAFIT:

Process risk point (PRP)	Risk arising from IT (RAFIT)
Addressed by:	
Process control activities	General IT controls
Identified:	
• When obtaining an understanding of business processes and the financial reporting process.	• After identifying automated control activities that address PRPs; or • When evaluating the reliability of internal information through separate control activities that are specifically designed to address the completeness and accuracy of the information (see Question 6.4.90) and the data integrity risk is addressed 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. • The 'where' and 'how' in the entity's process that a misstatement could be introduced.	• The susceptibility of automated control activities to ineffective design or operation, or risks to the integrity of information in the entity's IT systems, due to ineffective design or operation of general IT controls. • Represents any condition that could affect the effective operation of automated control activities or the

Process risk point (PRP)	Risk arising from IT (RAFIT)
	integrity of data and information within an entity's IT system.

Question 7.2.70

What is a relevant RAFIT?

Interpretive response: A relevant RAFIT is an IT risk where there is a 'reasonable possibility' that the risk could prevent the effective operation of the related automated control activity and/or the integrity of data within the IT system. 'Reasonable possibility' means a more than remote possibility, which is a low threshold.

The following table sets out example factors, scenarios, RAFITs and things that may be considered when determining if a RAFIT is relevant.

Whether the entity has access to make code changes		
Example scenario	An entity has access to make code changes at the **operating system layer**. A coded automated process control activity where changes are migrated from the **operating system layer** quality assurance environment to the production environment.	
Example considerations		**Example RAFITs**
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 improper authentication in relation to the IT layer where the code can be changed. RAFITs are identified at the **operating system layer.**	Because generally only privileged users are able to make code changes, RAFITs related to privileged user access are identified.	Logical access to users and accounts that can perform privileged tasks and functions within IT systems is inappropriate.
	Identification and authentication mechanisms are then necessary to restrict access exclusively to privileged users.	Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data.
	In addition, as specific access is needed to promote such changes into the production environment, related RAFITs are identified.	Logical access to implement changes to IT system program or configurations into the production environment is inappropriate.
	Revoking access may also be likely, to the extent it relates to removal of privileged accounts.	Logical access permissions are not revoked in a timely manner.

Whether the entity has access to make configuration changes		
Example scenario	An entity has access to make configuration changes at the **application layer.** A configured automated process control activity where configuration changes are implemented directly in the **application layer**.	
Example considerations		**Example RAFITs**
When the entity has access to modify configurable settings for IT systems in which automated control activities reside, there is a risk that individuals or privileged users could make configuration changes in production without going through the appropriate configuration change management process. RAFITs are identified at the **application layer**.	Because generally only privileged users are able to make configuration changes, RAFITs related to privileged user access are identified.	Logical access to users and accounts that can perform privileged tasks and functions within IT systems is inappropriate.
	Identification and authentication mechanisms are then necessary to restrict access exclusively to privileged users.	Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data.
	In addition, as changes can be made directly in the application layer, related RAFITs regarding access to implement changes are applicable.	Logical access to implement changes to IT system program or configurations into the production environment is inappropriate.
	Revoking access may also be likely, to the extent it relates to removal of privileged accounts.	Logical access permissions are not revoked in a timely manner.

Process to approve and test source code changes to production		
Example scenario	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.	
Example considerations		**Example RAFITs**
This factor is relevant to situations in which code changes are made to IT systems where automated control activities 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	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.	Changes to IT programs were inappropriate.

Process to approve and test source code changes to production		
a vendor. RAFITs are identified at the **application layer**.		
Note that this factor is focused on risks related to the approval 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 in the production environment, listed above.		

Process to approve and test configuration changes to the production environment		
Example scenario	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.	
Example considerations		**Example RAFITs**
This factor is relevant to situations where configuration changes are made to IT systems where automated control activities 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. RAFITs are identified at the **application layer**.	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.	Changes to IT configurations were inappropriate.
Note that 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, listed above. 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 in the live environment.		

User type		
Example scenario	An entity grants regular business end users access to the **application layer** functionality that allows changes to the vendor master file.	
Example considerations		**Example RAFITs**
This factor is relevant when testing system	This means that risks related to inappropriate	Identification and authentication mechanisms

User type		
access controls. The type of user is considered at each layer of technology (see Question 7.2.80) that has access to the functionality or data subject to the automated control activity. Examples of user types include a regular business end user, system administrator, database administrator, system accounts and shared accounts. RAFITs are identified at the **application layer**.	end user access are likely relevant.	are not implemented to restrict logical access to IT systems and data.
		Logical access permissions are granted to users and accounts that are inappropriate.
		Logical access permissions are not revoked in a timely manner.
	In addition, the risks related to privileged user access are likely relevant.	Logical access to users and accounts that can perform privileged tasks and functions within IT systems is inappropriate.
Note that it is expected that this RAFIT factor is relevant to system access controls in all relevant layers of technology (see Question 7.2.80) in which the access is granted.		

How access to functions/transactions is restricted (does not include 'read only access')		
Example scenario	To manage access to functions/transactions, an entity uses security groups to assign user privileges/access rights at the **application layer.**	
Example considerations		**Example RAFITs**
This factor is relevant when testing system access controls. An entity considers 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. RAFITs are identified at the **application layer.**	The risks related to changing the security groups, roles or profiles are considered. Since security groups, roles or profiles are generally configured into the system and not hard coded, RAFITs for configuration changes are relevant.	Changes to IT configurations were inappropriate.
		Logical access to implement changes to IT system program or configurations into the production environment is inappropriate.
	In addition, risks related to inappropriate end user access are likely relevant.	Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data.
		Logical access permissions are granted to users and accounts that are inappropriate.
		Logical access permissions are not revoked in a timely manner.

How access to functions/transactions is restricted (does not include ‘read only access’)		
	The risks related to privileged user access are likely relevant as well.	Logical access to users and accounts that can perform privileged tasks and functions within IT systems is inappropriate.
Note that it is expected that this RAFIT factor is relevant to system access controls in all relevant layers of technology (see Question 7.2.80) in which the access is granted.		

Physical access		
Example scenario	An entity uses an open console where changes to the system can be made. In instances where physical security risks exist.	
Example considerations		**Example RAFITs**
An entity considers the risk that unauthorized changes can be made by individuals with access to the console.		Physical access to facilities housing IT systems and/or electronic media is unauthorized or not commensurate with job responsibilities.

Dependency on scheduled jobs		
Example scenario	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.	
Example considerations		**Example RAFITs**
An entity considers risks associated with inaccurate, incomplete and untimely processing of, or unauthorized changes to, system jobs, including batch jobs and interfaces (e.g. risk of unauthorized program execution, deviations from scheduled processing). RAFITs are identified at the **application layer**.	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	System jobs, processes, and/or programs do not function as intended, resulting in incomplete, inaccurate, untimely or unauthorized processing of data.
	Computer operations risks can themselves be caused by inappropriate access or inappropriate changes to the job scheduler, which then means that program change and access risks can also affect the control activity.	Logical access to make changes to system jobs, processes, and/or programs is unauthorized or not commensurate with job responsibilities.
	As the job scheduler is generally both coded and	Changes to IT programs were inappropriate.

Dependency on scheduled jobs		
	configured, RAFITs for configuration changes may be relevant, depending on how the schedule is set up.	Changes to IT configurations were inappropriate.
	Access to implement changes is likely relevant as it relates to the ability to implement any change in the scheduler.	Logical access to implement changes to IT system program or configurations into the production environment is inappropriate.
	In addition, the risks related to inappropriate privileged user access are likely relevant.	Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data.
		Logical access to users and accounts that can perform privileged tasks and functions within IT systems is inappropriate.

Dependency on backup and recovery of programs and data	
Example scenario	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.
Example considerations	**Example RAFITs**
This factor is relevant when an automated control activity relies on the backup and recovery of data. For example, when an interface runs automatically from one system to another and relies on backup and recovery of data to re-run the interface if there were issues with the transmission of data. RAFITs are identified at the **database layer**.	Financial data backups are not able to be recovered in a timely manner.

Occurrence of data migration	
Example scenario	An entity migrates data from their legacy system to a newly acquired system.
Example considerations	**Example RAFITs**
When data is migrated from one system to another during the period, this creates the risk that such data will be corrupted, lost or otherwise not migrated completely or accurately. Such migrations may occur	Incomplete, redundant, obsolete or inaccurate data is migrated to the production environment of acquired,

Occurrence of data migration	
when systems are upgraded, replaced or merged. RAFITs are identified at the **database layer**.	newly developed or existing IT systems.

Question 7.2.80

When is a layer of technology relevant to ICFR?

Interpretive response: A layer of technology is relevant when there is one or more RAFITs within that layer of technology that are relevant to the effective operation of automated control activities or the integrity of data and information within the IT system.

An entity identifies the relevant layers of technology and RAFITs by considering:

- the layer of technology where the automated control activity operates or where the data and information within an IT system exist;
- the layers of technology that are relevant to the effective operation of automated control activities 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 risk could prevent the effective operation of automated control activities or the integrity of data and information within an IT system.

The identification of relevant layers of technology and RAFITs is concurrent. Even though consideration over what layers of technology are applicable to the automated control activity or integrity of data within an IT system occurs first, they are not relevant unless a RAFIT has been identified within that layer.

When the application layer is relevant, the following are also typically relevant:

- the database(s) that stores the data processed by the automated control activity; and
- the operating system through which the IT applications and databases are accessed.

Generally, RAFITs on the network layer are related to network segmentation/remote access and are not relevant to automated control activities. The network layer may be identified as relevant when an IT system interacts with vendors or external parties through the internet. The network layer may also be relevant when an entity has web-facing applications used in financial reporting and there are cybersecurity risks that could result in risks of material misstatement to the financial statements. Management evaluates and manages cybersecurity risks across the entity at the network layer. Question 7.6.30 discusses management's responsibilities related to cybersecurity risks.

To determine if a layer of technology is relevant, it is important to think about the RAFITs and layers of technology in parallel. The entity should consider qualitative factors, such as where the automated control activity operates or where the data resides.

The following table sets out example factors that may be considered when determining whether a layer of technology is relevant and provides a scenario in which the factor may contribute to identifying an IT layer as relevant.

IT layer factors	Example scenario
Where the automated control activity 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 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 (i.e. stored procedures) is maintained	An automated control activity relies on stored procedures in a **database layer**, 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	An automated access process control activity restricts access to change the vendor master file. Users can access this 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 the IT layer in which the data 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.

Practical tip

Many times, there are patterns in the relevant RAFITs between similar control activities in a process. Therefore, creating a mapping document of automated control activities to their IT layers and the relevant RAFITs can be beneficial. For example, system configuration control activities would likely have consistent risks, whereas batch processing control activities potentially would have -

additional risks due to their possible dependency on scheduled jobs and/or backup of data.

In addition, mapping of the RAFITs to layers of technology will assist in consistent identification of risks. For example, due to their nature, operating systems have fewer individuals with access, as well as little or no changes. As a result, the identification of change management risks and/or some access risks may not be relevant for this layer.

Question 7.2.90
Can multiple layers of technology be relevant to a single automated control activity?

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

Question 7.2.100
How does an entity document relevant IT systems and layers?

Interpretive response: An understanding of the workings of IT systems used by the entity, including how information flows into, through, and out of the relevant IT systems, may be facilitated by using ISDs.

ISDs are not flowcharts; instead, they are diagrams that depict the different layers of an entity's IT environment. ISDs show relevant applications, databases, operating systems, and other network infrastructure. ISDs will often show how service organization systems interact with the entity's internal IT systems. The ISD is a diagram of the IT systems and a framework by which management and external auditors can gain an adequate understanding of IT when walking through a business process to identify relevant PRPs.

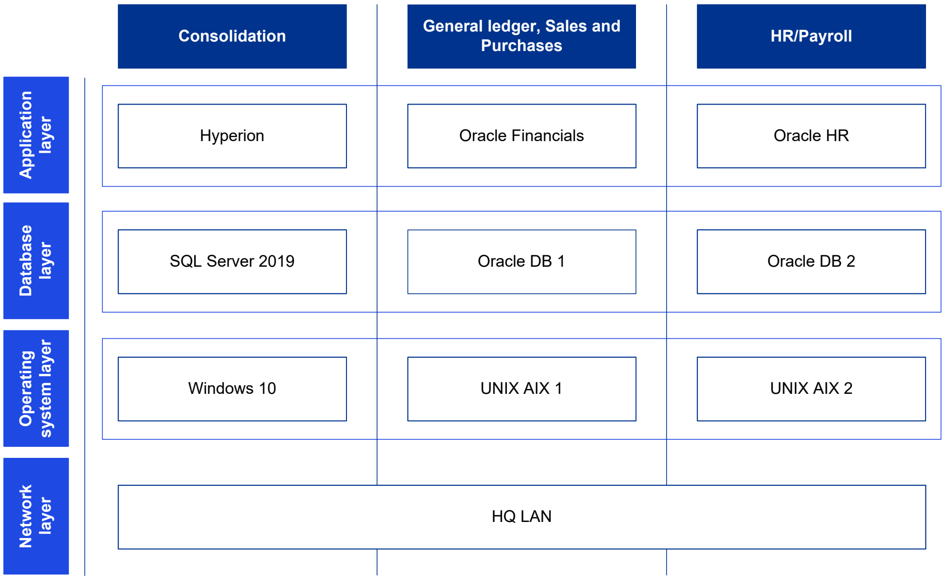
It is important to understand the overall IT environment to properly identify IT risks at the process level. This is because flowcharts or narratives that document the flow of information through a particular process are activity-based and often do not fully articulate the multiple layers of IT embedded in the process or the control activities management has in place to address the risks, including completeness and accuracy of relevant data elements flowing through the process.

Practical tip

Management should involve IT professionals in the risk assessment process as well as in reviewing the entity's process and control documentation to help identify applicable systems, related automated control activities and RAFITs.

Example 7.2.20
IT system overview diagram

The following is an example IT system overview diagram by process:



	Consolidation	General ledger, Sales and Purchases	HR/Payroll
Application layer	Hyperion	Oracle Financials	Oracle HR
Database layer	SQL Server 2019	Oracle DB 1	Oracle DB 2
Operating system layer	Windows 10	UNIX AIX 1	UNIX AIX 2
Network layer	HQ LAN		

Question 7.2.110
Why is it important to identify IT layers and RAFITs?

Interpretive response: Identifying the relevant layers of technology helps identify the relevant RAFITs within those layers, which in turn helps identify the GITCs that address those risk points.

Failure to identify the correct RAFITs and IT layers may result in not establishing appropriate GITCs to support the consistent operation of automated control activities. Lack of establishing appropriate GITCs renders those automated control activities ineffective. In addition, failure to establish proper linkage between automated control activities and GITCs may result in difficulties identifying the downstream impact of GITC deficiencies.

Practical tip

An entity should involve their IT professionals in the risk assessment and review of process and control documentation to help identify when data in a process is entered, stored, manipulated, exchanged or extracted. Once identified, these professionals can:

- design and implement automated control activities to address risk points;
- identify the IT system layers and related RAFITs where the automated control activities reside; and
- design and implement the related GITCs to mitigate those risks.

7.3 GITCs

Question 7.3.10
What are GITCs?

Interpretive response: GITCs are control activities over the entity's IT processes (see Question 7.2.50) that support the continued effective operation of the IT environment, including:

- the continued effective operation of automated control activities; and
- the integrity of data and information within the entity's IT system.

The IT environment encompasses the IT systems the entity uses as part of its financial reporting and business processes, including its layers of technology (see Question 7.2.10), the IT processes and the IT organization.

GITCs may be manual (see Question 7.3.40) or automated (see Question 7.3.50).

GITCs are not expected to directly prevent, or detect and correct, material misstatements on a timely basis. However, ineffective GITCs may lead to automated control activities that don't operate consistently and effectively, which may lead to the automated control activities not preventing, or detecting and correcting, a material misstatement on a timely basis.

Question 7.3.20
Where are GITCs in the COSO Framework?

Interpretive response: Principle 11 of the COSO Framework states: "The organization selects and develops general control activities over technology to support the achievement of objectives."

Once automated process control activities are identified to address process risk points, the relevant RAFITs that impact these automated control activities in the layers of technology in which they operate are identified. Under Principle 11, GITCs are established to address each relevant RAFIT within each relevant IT layer.

See Question 5.2.70 for discussion of the importance of principle 11.

Question 7.3.30

What is considered when designing and documenting GITCs?

Interpretive response: The table below sets out the items considered when designing a GITC. The considerations in the table should be present in the documentation for each GITC. Some considerations only apply to manual controls, where indicated.

Considerations	Description	Section/ Question
Control objective	The risk the control is intended to mitigate, i.e. the relevant RAFITs the GITC addresses. This is achieved using control attributes.	5.5
Nature and type of control	'Nature' refers to whether the GITC is manual or automated. 'Type' refers to whether the GITC is preventive or detective.	5.6; 7.3.40 and 7.3.50 for GITC specific considerations.
Frequency	The frequency with which a manual GITC is performed, which could be: • annually • quarterly • monthly • weekly • daily • recurring; or • ad hoc.	5.7
Authority and competence of the control operator (see Question 5.4.40)	The level of competence and authority necessary to operate a manual GITC (i.e. is the right person performing the control activity?).	5.8
Judgment involved	The subjectivity involved in determining whether something is an outlier and/or whether that outlier is correct/reasonable in operating a manual GITC.	5.9

Considerations	Description	Section/ Question
Investigation and resolution process	The documented steps performed by the control operator to investigate and resolve outliers identified in operation of a manual GITC.	5.11
Information used in the performance of the control activity	Information is usually used when performing a manual GITC (e.g. system reports, manually prepared spreadsheets, queries), including the relevant data elements (see Question 6.2.40).	Chapter 6 for discussion on information and 7.3.70 for GITC specific considerations.

Practical tip

Clear and concise documentation of the design of GITCs (addressing the considerations in the preceding table) provides evidence to support the achievement of Principle 11. Clear documentation of the design of the GITCs also enables management to perform separate evaluations necessary to monitor that the GITCs addressing the RAFITs are designed and operating effectively.

For example, if the design of a GITC is not clear in its documentation, the GITC may fail to function properly if the control operator leaves the entity and the GITC needs to be reassigned to a new person.

Question 7.3.40
What are manual GITCs?

Interpretive response: Like other manual control activities, the control attributes for manual GITCs are performed by people. See Question 5.5.20 for guidance regarding control attributes. The control operator in a manual GITC is a person.

A common example of a manual GITC is a periodic user access review. During this review, IT management considers each user's level of access in the system and makes changes as needed. In addition to this GITC, there are likely to be preventive controls in place to determine that:

- appropriate logical access permissions are granted to users and accounts; and
- access is revoked in a timely manner upon termination.

When these preventive controls exist, the user access review is a monitoring control that can also serve as a compensating control in case the preventive control(s) did not operate effectively.

Practical tip

User access review controls tend to be more difficult to operate effectively due to the manual nature of the control and the multiple steps that are needed to appropriately use them as a GITC. Common pitfalls in user access review controls that result in the improper operation (or design) of the controls include:

- incomplete listings of users with access;
- untimely review of the listing;
- insufficient evidence of review;
- individuals reviewing their own access;
- untimely removal of inappropriate access after identification by the control operator; and/or
- lack of consideration given to whether inappropriate access identified during the review was inappropriately used (e.g. no lookback of user activity is performed).

Example 7.3.10
RAFITs, GITCs and control attributes for manual GITCs

The following table shows RAFITS, example GITCs and control attributes that address those RAFITs (see Question 5.5.20):

RAFIT(s)	GITC	Control attributes
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 privileges for new and modified user access, including standard application profiles/roles and critical financial reporting transactions.	Control operator determines that requests for new system access, or modification to existing system access, are approved by an authorized individual 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 and roles by job function.
		Control operator determines that the access provisioned is consistent with access requested and approved.
Logical access permissions are not revoked in a timely manner.	Access for terminated/resigned users is removed within 7 days (the specified period) from the system.	Control operator revokes system access of the terminated/resigned user within X days (the specified period) of the user's termination/resignation date, in accordance with the Company Information Security policy or the policy in practice.
Logical access permissions (new or modified) are granted to users and accounts	Every month, business/functional managers review	User access reviews of the system are conducted periodically in accordance

RAFIT(s)	GITC	Control attributes
(including shared or generic accounts) that are inappropriate (i.e. unauthorized or not commensurate with job responsibilities). Logical access permissions are not revoked in a timely manner. 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).	user access to determine whether user access is authorized and commensurate with job responsibilities.	with Company Information Security policy or the policy in practice.
		Business/functional managers commensurate with the entity's IT delegation of authority perform user access reviews.
		Inappropriate access identified as a result of the user access review is investigated to determine if unauthorized tasks or functions were performed.
		Control operators modify user access in accordance with the instruction from the business/functional managers as a result of the user access review.

Question 7.3.50

What are automated GITCs?

Interpretive response: The control attributes for automated GITCs are performed by IT systems in the same way each time they operate. Therefore, the control operator of an automated GITC is an IT system.

There are many different types of automated GITCs. Different categories of common automated GITCs include:

- system access controls;
- system configuration controls; and
- interface controls.

Similar to automated process control activities, for each automated GITC that addresses a RAFIT, the entity identifies:

- IT layers where the automated GITC resides;
- RAFITs that impact the automated GITCs; and
- GITCs that mitigate those RAFITs.

Example 7.3.20
Automated GITCs

The following table provides examples of automated GITCs for three common categories of such controls.

System access controls

- Access to update workflow configurations in the ticketing system is restricted to the IT support team.
- Access to migrate changes to the production environment is restricted to authorized production support personnel and segregated from personnel responsible for system development activities.
- Access to add or update approval configurations in the identity access management system is restricted to the IT security management team.
- Accounts with privileged access rights, including super-user administrative and system accounts, are restricted to authorized personnel commensurate with job responsibilities.
- Access to make changes to system jobs is restricted to authorized personnel in IT operations.

System configuration controls

- The identity access management system routes access requests to the appropriate approver based on the type of access being requested.
- 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.
- Changes are automatically deployed by the change deployment application after all required approvals have been logged into the application.
- Dual authentication is enforced for users attempting to access operating system administrator functions.
- Application password configurations enforce the following password rules:
  - include minimum of eight characters;
  - include at least one number and one special character;
  - change every 90 days; and
  - restrict repeating 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.

Question 7.3.60
What are automated GITCs implemented in tools?

Interpretive response: An example of automated GITCs implemented in a tool is a ticketing system that is used to support an IT access provisioning control. In its most basic form, a ticketing system is a tool used by the entity to record and document IT access requests, approvals and the related actions taken.

In more complex environments, the ticketing system may include automated workflows to route the access requests to the team members responsible for approving and granting access as each step of the access provisioning process is completed. Some ticketing systems can even interface with other IT layers to automatically grant access once the required approvals are documented.

Regardless of how advanced the ticketing system is, the entity considers how this application supports management's access provisioning control. The entity also considers whether the control relies on automated GITCs in the ticketing system for which it is necessary to consider IT layers, RAFITs and GITCs that address those RAFITs.

The following table includes other examples of tools where automated GITCs may reside.

Identity access management (IAM) tools
• Perform tasks to identify the user, authenticate the user and/or authorize the user.
Privileged access management (PAM)
• Focused on back-office users who perform high risk activities. They enable a smaller user base to perform activities that are deemed to be high risk. • Combination of tools and processes used by an entity to securely store, manage and monitor the usage of privileged accounts and the users with access to those accounts. • Provide these capabilities as a centralized solution that includes secure password storage, automated password rotation and session brokering and recording.
Code repositories
• A central file location that provides a structured way for programmers to store development files. It is used by version control systems to store multiple versions of files. While a repository can be configured on a local machine for a single user, it is often stored on a server that can be accessed by multiple users. • Helpful for any type of software development, but it is especially important for large development projects. By committing changes to a repository, developers can quickly revert to a previous version of a program if a recent update causes bugs or other problems. Many version control systems even support side-by-side comparisons of different versions of files saved in the repository. These comparisons can be helpful for debugging source code. • When a repository is stored on a server, users can 'check out' files for editing. This prevents multiple users from editing a file at the same time.

Question 7.3.70

What additional considerations are relevant for information used in GITCs?

Interpretive response: Like other control activities, information can be used by the control operator to perform a GITC. For example, consider a GITC over the periodic review of user access rights. To perform this GITC, the control operator reviews a system-generated report of the current access rights to an IT system each period. The system-generated report is information used in the GITC, and the control operator needs to consider the relevance and reliability of that information.

The approach to assessing the relevance and reliability of information used in GITCs is not different from the approach used in other control activities. Relevance and reliability may be addressed by:

- a control attribute of the GITC;
- a control attribute of another GITC that uses the same information; or
- other controls that are specifically designed to address the completeness and accuracy of the information.

In addressing the reliability of the information, management considers data input, data integrity, and data extraction and manipulation risks for information used in the control. However, there may be circumstances where one or more of these risks are addressed by an attribute of the GITC. For example, when testing a GITC over the periodic review of user access rights, the control operator reviews a system-generated report of the current access rights to an IT system at a point in time. Data extraction and manipulation risks are applicable to the information used in the GITC and tested separately as the report may not be completely extracted or be improperly manipulated after extraction, which would not be identified through the performance of the control. The review, however, verifies that the information is correct. Therefore, data input and data integrity risks are inherently addressed by performing the GITC and separate procedures are not necessary.

Chapter 6 provides a comprehensive discussion of information used in controls.

Question 7.3.80

What additional considerations related to GITCs are relevant for third-party service organizations used by the entity?

Interpretive response: Using service organizations may result in unique risks because the entity has given up control, while retaining responsibility, of some or all of its IT systems. To address these risks, management:

- understands the system of internal control at the service organization;
- assesses the relevance of those controls;

- considers relevance of GITCs over each IT Process (system access, program changes, program development and computer operations); and
- implements complementary user entity controls, as appropriate.

Chapter 8 provides a comprehensive discussion about using a service organization in the entity's control environment.

Practical tip

When identifying RAFITs for a relevant layer of technology for a system that is supported by a service organization, management should consider both:

- the RAFITs that would be addressed by a GITC performed by management; and
- the RAFITs that would be addressed by a GITC performed by the service organization.

For example, there are potential risks related to the entity's management having access to the system, and separate potential risks related to the service organization's personnel having access to the system (e.g. access for system updates, IT helpdesk solutions, etc.). In this situation, there may need to be separate GITCs identified to address these separate risks.

Question 7.3.90

How does an entity evidence that GITCs are designed and operating?

Interpretive response: Management is required to prepare and retain sufficient documentation to evidence that the GITCs are:

- properly designed and implemented to address RAFITs individually and/or in combination with other GITCs; and
- operating as intended in an integrated manner.

The extent of evidence will vary based on the nature of the control. However, the documentation is expected to show the results of operating the control, including any further investigation required to conclude that the control is designed and operating.

7.4 Monitoring procedures over GITCs

Question 7.4.10
Is testing of GITCs performed as part of monitoring procedures?

Interpretive response: It depends. Management has several different ways they can obtain the evidence necessary to support their assessment of effectiveness of ICFR (see section 2.7).

However, if management has determined to direct test controls as part of their monitoring strategy, their testing may include entity-level controls (see chapter 2), process control activities (see chapter 5) and GITCs (this chapter). If the entity has an internal audit function, it typically assists in management's direct testing of internal controls.

Question 7.4.20
What is included in the direct testing of GITCs?

Interpretive response: Direct testing of GITCs includes testing their operating effectiveness. In performing this testing, management should evaluate all the factors discussed in Question 7.3.30, including whether the control is properly designed to address the RAFIT.

Question 7.4.30
What is the timing of direct testing of GITCs?

Interpretive response: SEC Regulation S-K Item 308(a) requires management of public companies to provide its report on ICFR containing its assessment of the effectiveness of ICFR as of the end of the most recent fiscal year in its annual report. Therefore, when direct testing GITCs for purposes of completing the annual assessment of ICFR, management's overall evaluation of the effectiveness of controls is as of year-end. Nevertheless, the testing of controls usually needs to begin before year-end for it to be completed in time to support the assessment included in the annual report.

GITCs support automated control activities that operate throughout the period. Any control deficiencies for relevant GITCs could result in a material misstatement to the financial statements. Therefore, direct testing should be performed over the entire period and not just as of year-end.

Testing of GITCs before year-end also allows time for management to respond to any identified control deficiencies. For example, if management identifies a deficiency in the GITC related to a logical access review mid-way through the year, they have time to remediate the deficiency and operate the control activity appropriately for the reminder of the year, and not have a control deficiency as of their year-end assessment.

Practical tip

Communication with those charged with governance and external auditors is key when testing GITCs. When management requests that external auditors use a portion of testing performed by, for example, internal audit or others under the direction of management, alignment on timing of testing procedures, sample sizes and evidence required can reduce the burden on control operators and others by not requiring them to duplicate their efforts.

In addition, external auditors generally use the effective performance of controls to reduce the substantive procedures they perform as part of their audit. A control deficiency can result in increased substantive test work to be performed, including larger sample sizes and additional procedures. Therefore, the identification of deficient controls as of an interim date can provide sufficient time for the incremental testing to be completed.

Question 7.4.40

What evaluation strategies can be used in direct testing GITCs?

Interpretive response: To determine whether a GITC is operating effectively through direct testing of control activities, one of the following evaluation strategies (or a combination of the strategies) may be applied, depending on if the control type is automated or manual.

Procedure	Manual	Automated
Inquiry – Whenever inquiry is used, it should not be used as the sole procedure.	May include asking the control operator to determine what they look for when performing the control and what actions they take to address exceptions. It may also include asking about the number and magnitude of errors detected in the past and then obtaining evidence that those errors were properly resolved in a timely manner.	May include asking the system owner to determine how the system is configured to operate the control.
Inspection	May include examining documents used by the operator in performing the control to obtain evidence to corroborate information	May include examining the system configuration and/or code to obtain evidence to corroborate information obtained through inquiry (if

Procedure	Manual	Automated
	obtained through inquiry (if performed) and evaluate the effectiveness of the control as implemented by the control operator.	performed) and evaluate the effectiveness of the control as implemented within the system.
Observation	Watching a control activity being performed by the control operator and others, such as observation of provision access or performance of user access review.	Watching the system execute the control, such as observation of the system blocking the access of a user when using an incorrect password.
Reperformance	This may include independently using the control operator's metrics, thresholds, or criteria to identify outliers or exceptions and then evaluating the control operator's follow-up on these items. When a control is reperformed, there should still be sufficient evidence showing that the control was, in fact, performed. In particular, this relates to the evidence of follow-up actions taken by the control operator, and their resolution of all identified outliers.	Not applicable.

Question 7.4.50
Can there be one GITC across multiple IT layers?

Interpretive response: Yes. When an entity uses one IT process across its IT environment or across certain layers of technology, it may identify consistent RAFITs and one manual GITC.

Question 7.4.60
What are the additional considerations when a GITC exists across multiple IT layers or IT systems?

Interpretive response: When a manual GITC exists across multiple IT layers or IT systems, an entity considers the shared characteristics of the IT layers or IT systems to determine whether the GITC is designed and implemented to operate consistently across those layers.

To test the operating effectiveness of the GITC when there is one manual GITC that operates across multiple IT layers or IT systems, management may either:

- test each IT layer or IT system separately; or
- test the one GITC across all IT layers or IT systems (see Question 7.4.70).

For example, management has one change control for approval of all changes. There are three relevant applications that follow the one change control. Management can test the change control by obtaining a sample for each of the three relevant applications separately or by combining the population of changes for all three applications and selecting a sample.

An entity considers the shared characteristics in the following table to determine whether the GITC is designed and implemented as one GITC across multiple IT layers or IT systems and therefore can be tested as one control.

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	The same type of information is used by the control operators in performing the GITCs (e.g. the relevant data elements are the same, the information is generated in the same manner).
Subject to the same monitoring activities	Monitoring activities are performed consistently across the GITCs.

Example 7.4.10
One GITC applicable to multiple IT systems/layers

The entity has three relevant IT systems. Automated process control activities were identified as relevant in each of the IT systems for the relevant business process. The following GITC was identified to address relevant RAFITs in each of the IT systems: Changes to IT system programs are tested and approved before implementation into the production environment.

Rationale for identification of one GITC to address all systems:

- The relevant IT systems include:
  - System 1: SAP application and SQL server database;
  - System 2: Oracle application and Oracle database; and
  - System 3: Hyperion Financial Management (HFM) application and SQL server database

- The IT department is comprised of three application development groups – one to support each of the IT applications. There is one group that supports all databases. All groups report to one leader.
- The IT department follows the same program change policies, practices and procedures for all applications and databases.
- The IT department uses the same change management ticketing tool to initiate change requests, evidence testing, track changes and obtain approvals.
- The GITC is designed and implemented to operate consistently across all three IT systems and layers of technology.

Question 7.4.70

What does management consider when testing the operating effectiveness of a manual GITC across multiple IT systems?

Interpretive response: The following table summarizes the main aspects of testing one GITC across multiple IT layers or IT systems to monitor the operating effectiveness of manual GITCs.

Applicability	Can be used when the IT process is designed to operate consistently across multiple IT layers, resulting in one manual GITC.
Population	Testing is applied to a single population across all relevant IT layers. The completeness of the population is important in supporting GITC conclusions. Relevant IT systems and/or layers should not be excluded from the tested population. Nonrelevant IT systems or layers should not be included in the tested population.
Deficiencies	Any deviations in GITCs are considered control deficiencies. The deficiencies apply to all IT systems and/or layers in the population. It is not appropriate to isolate deficiencies to only those layer(s) where the deviation occurred.
Conclusions	Conclusions about the operating effectiveness of GITCs apply to all relevant IT systems and/or layers included in the population.
Benefits	Testing as one control can reduce the level of testing and effort required by management.

While automated GITCs may also be designed to operate consistently across multiple IT systems and/or layers, the testing approach is the same for all automated GITCs whether they operate over one or more layers.

Question 7.4.80

What evidence is maintained for the operation of GITCs to enable the performance of monitoring activities?

Interpretive response: See Question 5.18.60.

7.5 GITC deficiencies

Question 7.5.10

How do ineffective GITCs affect management's ICFR?

Interpretive response: If GITCs are ineffective, management may not be able to rely on the automated control activities or the integrity of the information maintained in or extracted from the impacted systems. In turn, this may impact management's conclusions on the effectiveness of ICFR.

In addition, the significance of a GITC deficiency relates to its impact on the effectiveness of automated control activities or the integrity of information it supports, and whether that impact could result in a material misstatement to the financial statements. GITC deficiencies do not directly cause material misstatements to the financial statements on their own. But they may render an automated control activity or the integrity of information as ineffective, which could lead to material misstatements to the financial statements.

Question 7.5.20

How does management respond to ineffective GITCs?

Interpretive response: When a GITC deficiency is identified, it is important to step back and perform a critical analysis to confirm:

- the understanding of the GITC and its design;
- the nature of the deficiency; and
- the pervasiveness of the deficiency.

For example, the pervasiveness of the GITC deficiency may affect all the supported automated control activities and the integrity of information, or it may only affect a particular business function, location or IT application.

Remember that GITCs support the continued effective operation of the IT environment, including the effective operation of automated control activities and the integrity of data and information within the entity's relevant IT systems (see Question 7.3.10). It is important to determine how the automated control activities linked to the GITC through RAFITs are impacted by the deficiency, or whether the deficiency impacts the integrity of information that is used in a manual control activity.

Similar to other control deficiencies, management evaluates the severity of GITC deficiencies. Chapter 9 provides comprehensive discussion about how to evaluate the severity of GITC deficiencies and how to consider their effects on automated control activities that rely on the GITCs.

Management may also need to evaluate whether any compensating control activities sufficiently address the same RAFITs as the deficient GITC. Compensating controls may include:

- other formally established and regularly performed GITCs that address the same RAFITs and support the consistent operation of the same automated control activity as the deficient GITC; and/or
- process control activities (manual or automated) that do not rely on the deficient GITC but address the same risks as the automated control activities supported by the deficient GITC.

Alternatively, management may perform additional procedures to determine whether the deficient GITC actually impacted the automated control activities or integrity of information during the period under audit. These additional procedures performed by management may be considered as ad hoc compensating GITCs, if they are part of management’s ICFR, performed timely, documented as a control, have associated control attributes, and are not performed only in response to a deficiency identified by external auditors.

Ad hoc compensating GITCs may provide evidence that supports the consistent operation of the related automated control activities and/or integrity of the data within the IT system and may mitigate the severity of the deficiency. However, they do not eliminate the GITC deficiency.

Example 7.5.10
Deficient GITC and ad hoc compensating GITCs

A GITC related to application access is found to be deficient because application developers have inappropriate access to promote changes directly into the live environment. This is inconsistent with their job responsibilities.

Management’s response to this deficiency is to perform an ad hoc control with documented control attributes that would include obtaining evidence to determine whether the application developers:

- made any changes to the application; or
- used their inappropriate access to promote any changes that may impact the automated control activities.

To do so, management might inspect reliable (i.e. complete and accurate) application change logs for the period where the inappropriate access existed to determine whether any changes were made by the inappropriate users. If no changes were made, this ad hoc compensating control may support the consistent operation of the related automated control activities or the integrity of information. However, the GITC related to application access is still deemed to be deficient and would be evaluated as to its severity.

7.6 Cybersecurity

Question 7.6.10
What are cybersecurity risks and incidents?

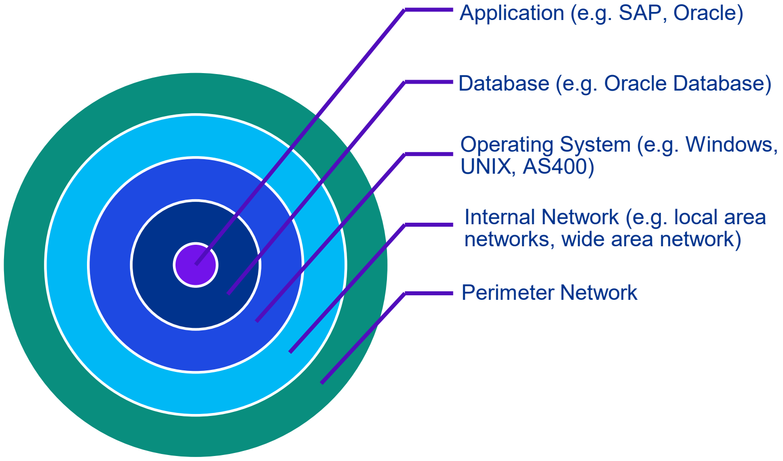
Interpretive response: A cybersecurity risk is the risk of loss or harm related to technical infrastructure, the use of technology within an entity or the potential for cybersecurity incidents that could impact the confidentiality, integrity or availability of information or IT systems. This includes risks associated with unauthorized access, data breaches and other cybersecurity threats that could disrupt operations, compromise data or cause financial and reputational damage.

A cybersecurity incident is an unauthorized occurrence or a series of related unauthorized occurrences on or conducted through an entity's IT system that jeopardizes the confidentiality, integrity or availability of an entity's IT systems or any information residing therein.

Cybersecurity incidents often have negative consequences for the entity, including:

- lost revenues;
- litigation costs and potential regulatory fines;
- incorrect/inaccurate financial reporting due to loss of data integrity;
- loss of availability to financial reporting systems, including impact to reliance on internal controls;
- remediation costs related to stolen information including privacy/personal 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.

The following diagram depicts the typical architecture of an on-premises IT system relevant to the evaluation of cybersecurity incidents.


Application (e.g. SAP, Oracle)
Database (e.g. Oracle Database)
Operating System (e.g. Windows, UNIX, AS400)
Internal Network (e.g. local area networks, wide area network)
Perimeter Network

Cybersecurity incidents usually first occur through the perimeter and internal networks. Depending on the entity's business environment, security around the internal and perimeter networks may not pose risks to financial and nonfinancial data relevant for financial reporting. However, network access may be relevant to financial reporting for entities that permit access to operating systems, databases and applications through single sign-on protocols. Unauthorized users can also move laterally within the network layer to attempt to gain access to the operating system, database or application layers, even if single sign-on protocols are not used.

An example of a cybersecurity incident at the internal or perimeter network is when a computer virus sent as an email attachment or download from a website infects systems in an entity's IT environment.

Question 7.6.20

Are cybersecurity risks also relevant for third-party service organizations used by the entity?

Interpretive response: Yes. When responding to cybersecurity risks at the entity, management also considers and responds to cybersecurity risks at third-party service organizations that they have determined are relevant to the entity's ICFR. Question 8.4.60 and Question 8.8.100 discuss service organizations and cybersecurity risks.

Question 7.6.30

What are management's responsibilities related to cybersecurity risks?

Interpretive response: Management is responsible for:

- evaluating the risk of cybersecurity incidents (e.g. ransomware attacks, phishing schemes, malware infections, insider threats, business email compromise scams and denial-of-service attacks) 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 assess and manage those risks.

Given the prevalence and potential impacts of cybersecurity risks in today's environment, public companies subject to periodic reporting under the Securities Exchange Act of 1934 are required, pursuant to Regulation S-K, to annually disclose the following information on Form 10-K:

- the entity's processes for identifying, assessing and managing material risks from cybersecurity threats;
- management's role in cybersecurity governance; and
- oversight of risks from cybersecurity threats by the board of directors.

See KPMG Defining Issues, SEC issues rules – Enhancing cybersecurity disclosures, for additional information.

Example 7.6.10

Processes and controls related to cybersecurity risk assessment and management

The following table includes examples of processes and controls that may be employed by an entity to assess and manage cybersecurity risks.

Process/control	Description
Govern	
Cyber governance	The entity incorporates cyber governance in its corporate governance regime, which includes those charged with governance regularly receiving reports on cybersecurity activities. Alternatively, on a quarterly basis, those charged with governance are briefed on findings and concerns relating to the entity's cyber intrusion protection program (CIPP) as well as other measures taken by management to mitigate cybersecurity risks.
Business continuity plan	If the entity does not have a separate cybersecurity incident response plan that is tested by the corporate cybersecurity incident response team (CIRT), the business continuity plan

Process/control	Description
	includes a documented and tested plan to deal with cybersecurity incidents.
Identify	
Resources	The entity identifies and evaluates the following that are relevant to its operations, assessing the potential cybersecurity risks these resources may pose to its financial statements and/or ICFR: • the entity's assets, including data, hardware, software, systems, facilities, services, and people; and • service organizations (including subservice organizations) and vendor-purchased software based on the nature of the services and software provided.
Protect	
Personnel training	New personnel are required to complete training upon hire that focuses on IT security and access. 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 training focused on IT security and access communications.
Corporate cybersecurity incident response team	As part of its CIPP, the entity sets up a CIRT, 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. Management often organizes their cybersecurity activities in a Security Operations Center.
Security evaluations	IT performs periodic network vulnerability assessments to: • 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.
Service organizations (including subservice organizations)	The entity has processes to assess cybersecurity risks related to service organizations (including subservice organizations), including processes to: • regularly review and update service for security compliance; • track and manage vulnerabilities associated with the services; and • handle cybersecurity incidents.
Verification controls	The entity has controls that verify changes to bank account information or vendor payment information (e.g. routing numbers, vendor names) to authenticate the validity of changes.

Process/control	Description
Detect	
Network monitoring	The entity uses various software tools across the organization to monitor systems. These may include one or more of the following: vulnerability scanners, packet sniffers, intrusion detection systems, vulnerability exploitation devices, packet crafting tools and firewall monitoring devices.

Question 7.6.40

What are management's responsibilities when a cybersecurity incident has been identified?

Interpretive response: Cybersecurity incidents could materially affect an entity's business (see Question 7.6.10). In accordance with Regulation S-K, public companies subject to periodic reporting under the Securities Exchange Act of 1934 are required to:

- disclose on Form 8-K specified information about a material cybersecurity incident within four business days of determining the incident was material; and

- provide information that was not determined or was unavailable about a previously disclosed material incident on an amended Form 8-K.

Therefore, it is management's responsibility to have sufficient disclosure controls and procedures to:

Step 1	Identify cybersecurity incidents on a timely basis.
Step 2	Assess and analyze the effect of the incidents on the entity's business (see Question 7.6.50).
Step 3	Evaluate the materiality of the incidents.
Step 4	Create open communications between technical experts and senior management responsible for disclosures.
Step 5	Make timely disclosures about the incidents.

In addition to satisfying the disclosure requirements discussed above, management also evaluates whether a known cybersecurity incident, whether or not material for purposes of reporting on Form 8-K, is relevant to the entity's financial reporting and/or ICFR and, if it is, whether:

- the cybersecurity incident indicates a significant deficiency or a material weakness in the entity's ICFR; and

- information about the range and magnitude of financial statement effects from the cybersecurity incident has been incorporated into the entity's financial statements on a timely basis.

Question 7.6.50

What does management consider when obtaining an understanding of a cybersecurity incident and its effects?

Interpretive response: Management considers the below matters when obtaining an understanding of a cybersecurity incident and its effects on the entity's business and financial reporting.

Nature

- Was the incident entity-specific or did it occur through a vendor-purchased software or service organization?

Magnitude

- How did the entity respond to the cybersecurity incident (e.g. activate the incident response plan, isolate affected IT systems or networks, inform relevant stakeholders, review audit logs, change IT security policies, training and/or instructions for employees not to open phishing emails)?
- What financial reporting-related IT systems were impacted by the cybersecurity incident?
- Was data stolen or modified by the perpetrators? If so, what was the type of data impacted (e.g. personal/sensitive customer and/or employee information, financial or transactional data)?
- Was there a loss of data?
- Was there a consultation with external resources to determine the extent and impact of the incident (e.g. forensic accountants, law enforcement, security forms, legal counsel)? If so, what were the results of these consultations?
- Were the audit committee or others charged with governance informed of the incident?
- Related to financial reporting IT systems:
  - Were IT systems taken offline? If so, how long were the IT systems or services offline and how did this impact the entity and its financial reporting?
  - Did any of the offline IT systems or services create a backlog of processing transactions/operations? If so, what impact did this have on the entity and its financial reporting? Were new controls created?

  - Was the root cause of the cybersecurity incident identified?
  - What steps were taken to confirm that the IT systems, services, and data were restored accurately and completely?
  - What changes or enhancements will be made because of the cybersecurity incident?

Duration

- For incidents that impacted IT systems relevant to financial reporting, what was the elapsed time between the cybersecurity incident occurrence and remediation?

Question 7.6.60

How does management determine whether a cybersecurity incident is relevant to ICFR?

Interpretive response: A cybersecurity incident is considered relevant to ICFR if it impacted, or could reasonably have impacted, the entity's IT systems that are relevant to financial reporting.

Whether a cybersecurity incident is considered relevant to ICFR is based on management obtaining an understanding of the cybersecurity incident (see Question 7.6.50) and determining:

- if any control deficiencies have been identified as a result of the cybersecurity incident; and
- the layer(s) of technology that may have been impacted by or exposed to any identified deficiency.

If an identified deficiency impacts one or more layers of technology relevant to financial reporting, it is evaluated for severity following the steps in chapter 9. This includes considering potential impacts to the GITCs that are relevant to the effective operation of automated controls or the integrity of information.

Question 7.6.70

If management determines that a cybersecurity incident is material for purposes of disclosure on Form 8-K, is there a presumption that the entity has a material weakness in ICFR?

Interpretive response: No. A cybersecurity incident could be deemed material and require public disclosure under the SEC rules due to its impact on the entity’s business and operations. Yet the incident may not be associated with, and may not indicate control deficiencies in, any layers of IT that are relevant to the entity’s financial reporting (e.g. when a cyber incident has only affected an operational system with no impact to the financial reporting process and internal controls). In this case, the incident may not indicate a deficiency in the entity’s ICFR. However, such conclusion requires careful evaluation of the incident by management, including its nature, magnitude and duration.

Question 7.6.80

If management determines a cybersecurity incident is not material for purposes of disclosure on Form 8-K, could there still be a material weakness in ICFR?

Interpretive response: Yes. A cybersecurity incident that management determines is not material for purposes of disclosure on Form 8-K may nevertheless indicate, based on management’s evaluation, that there is a deficiency in the entity’s ICFR. That deficiency would require a severity evaluation that may lead to a material weakness conclusion.

Evaluation of the severity of an identified control deficiency is separate and different from the materiality assessment of the related cybersecurity incident. In particular, the materiality assessment of a cybersecurity incident for purposes of disclosure on Form 8-K is based on what *‘has happened’* and applies the SEC’s traditional materiality standard, which is set out in the securities laws. Under that standard, information – including information about a cybersecurity incident – is material:

- if there is a substantial likelihood that a reasonable investor would consider the information important to their investment decision; or
- if it would have significantly altered the *‘total mix’* of information made available.

On the other hand, evaluation of the severity of a control deficiency revealed by a cybersecurity incident deals with what *‘could’* have happened as a result of the deficiency and focuses on potential impacts to the entity’s financial reporting. A material weakness can exist even in the absence of an actual misstatement or when the actual misstatement is not material (see section 9.5 for additional information regarding evaluation of severity of a control deficiency).

Question 7.6.90

What are the auditors’ responsibilities related to cybersecurity risks?

Interpretive response: The auditor is responsible for obtaining an understanding of management’s cybersecurity risk assessment process, which includes:

- understanding how management identifies and addresses cybersecurity risks, including the response to a cybersecurity incident when it occurs and whether the incident is relevant to the entity's financial statements and/or ICFR;

- evaluating the risks of material misstatement to the entity's financial statements resulting from, among other things, unauthorized access to financial reporting systems, including IT applications, databases and operating systems; and
- obtaining an understanding of the nature, magnitude and duration of the cybersecurity incident if one occurs and evaluating its effect on the audit approach.

The auditor also evaluates management's assessment of a cybersecurity incident's effect on the amounts and disclosures in the financial statements and the entity's ICFR.

The auditor is not responsible for:

- evaluating cybersecurity risks across an entity's entire IT environment;
- providing assurances on the adequacy of safeguards and controls established to address cybersecurity risks or the entity's ability to withstand a cybersecurity incident; or
- concluding on the appropriateness of the entity's actions in response to cybersecurity risks or to actual cybersecurity incidents.

Key takeaways

- Identifying the relevant layers of technology (application, database, operating system and network) helps to determine the relevant RAFITs within those layers, which in turn helps to identify GITCs that address those risks.
- GITCs are control activities over the entity's IT processes that support the continued effective operation of the IT environment, including automated control activities, and the integrity of data and information within the entity's IT system.
- Although ineffective GITCs do not directly cause financial statement misstatements, they do impact the effective operation of automated control activities or the integrity of information, which may lead to material misstatements.
- GITCs are included in management's monitoring. If management's monitoring includes performing direct testing of GITCs, the testing should be performed throughout the period.
- Management is responsible for establishing processes to identify, assess and manage material risks of cybersecurity incidents and cyber-related frauds across all aspects of the entity's business operations. Management also maintains effective disclosure controls and procedures to timely identify and evaluate cybersecurity incidents and consider them for disclosure in accordance with the rules of the SEC.
- When a cybersecurity incident occurs, management is also responsible for assessing its effect on the amounts and disclosures in the financial statements and the entity's ICFR.

8. Service organizations

Detailed contents

8.5 Management's monitoring of service organizations and subservice organizations

Questions

8.5.10 To what extent does management address each service organization and subservice organization when assessing the effectiveness of the entity's ICFR?

8.5.20 How does management monitor service organizations and subservice organizations?

8.6 Management's understanding and assessment of the service organization's ICFR

Questions

8.6.10 How does management obtain an understanding of the service organization and their ICFR?

8.6.20 How does management use a SOC report to assess the relevance of controls of a specific service provided to the user entity?

8.6.30 What does management consider when evaluating the 'nature' of the control testing performed by the service auditor?

8.6.40 How does management determine whether the nature of the tests of controls performed at the service organization is appropriate?

8.6.50 How does management evaluate whether the timing of relevant tests of controls provides sufficient appropriate evidence?

8.6.60 What does the 'extent of evidence' refer to in the context of a service organization's SOC report?

8.6.70 What does management consider when evaluating the 'extent' of the control testing performed by the service auditor?

8.7 Management's implementation of appropriate complementary user entity controls

Questions

8.7.10 What are CUECs?

8.7.20 How is it determined which CUECs are to be considered by the user entity?

8.7.30 What if certain CUECs linked to a relevant control objective are not relevant to the user entity?

8.7.40 How does the user entity design controls to address CUECs identified in the SOC report?

8.8 Management's review of SOC reports to evaluate effectiveness of controls

Questions

8.8.10 Should management have a control that requires review of SOC reports?

8.8.20 What is the first step performed by the control operator when reviewing the SOC report?

8.8.30 Who should perform the control to review the SOC report?

8.8.40 How often should the control to review a SOC report operate?

8.8.50 What should the control operator review and document for the SOC report review control?

8.8.60 How does the control operator evaluate the service auditor?

8.8.70 Does the control operator focus on control objectives or the individual controls when evaluating the SOC report?

8.8.80 How does a control operator address controls within a relevant control objective that are not relevant to the user entity?

8.8.90 What procedures does the control operator perform when the service auditor uses the carve-out method for a subservice organization?

8.8.100 What is management's responsibility when a cybersecurity incident is identified at a service organization?

8.8.110 What are management's responsibilities if the service auditor or other auditor issues an agreed-upon procedures or other attestation report?

8.8.120 What are management's responsibilities if the service auditor issues an agreed-upon procedures report to specified parties?

Example

8.8.10 Identifying control operators to perform the SOC report review control

8.9 Management's evaluation of deficiencies identified in SOC reports

Questions

8.9.10 What are management's responsibilities when a Type 2 SOC report identifies deviations or exceptions within a relevant control objective?

8.9.20 Can management rely on relevant controls without deviations or exceptions that are within a failed control objective?

8.9.30 Does an unqualified service auditor's report mean there are no deficiencies identified?

8.9.40 What are the implications when the service auditor's report has a qualification or other modification?

8.9.50 What kinds of qualifications can be noted in the service auditor’s opinion?

8.9.60 Can a user entity rely on an adverse opinion?

8.10 Use of relevant information in SOC 1 reports by management

Questions

8.10.10 When is information provided by service organizations identified in a business process?

8.10.20 How does the user entity obtain information from the service organization?

8.10.30 What are the different types of information related to a service organization?

8.10.40 When can a SOC 1 report be used to address the risks related to information used in controls or produced for an entity?

8.10.50 What are the implications of a Type 2 SOC 1 report not specifying that information used by management was tested for accuracy and completeness?

8.10.60 When the SOC 1 report does not provide evidence over the accuracy and completeness of information from the service organization, what other procedures may management perform to obtain this evidence?

8.11 Management’s evaluation of the period covered by the service auditor’s report and gap periods

Questions

8.11.10 How does management evaluate whether the period(s) covered by the service auditor’s report is appropriate for the entity?

8.11.20 What is a gap period?

8.11.30 What are management’s responsibilities when there is a gap period?

8.11.40 How are changes during the gap period identified and assessed?

8.11.50 What is a bridge letter?

8.11.60 What additional procedures may be performed to address changes during the gap period?

8.12 Management's response if no SOC report is available or 'controls gaps' are identified

Questions

8.12.10 What is a 'control gap'?

8.12.20 How does management address 'controls gaps'?

8.12.30 Can a user entity establish their own processes and controls over the activities performed by a service organization?

Key takeaways

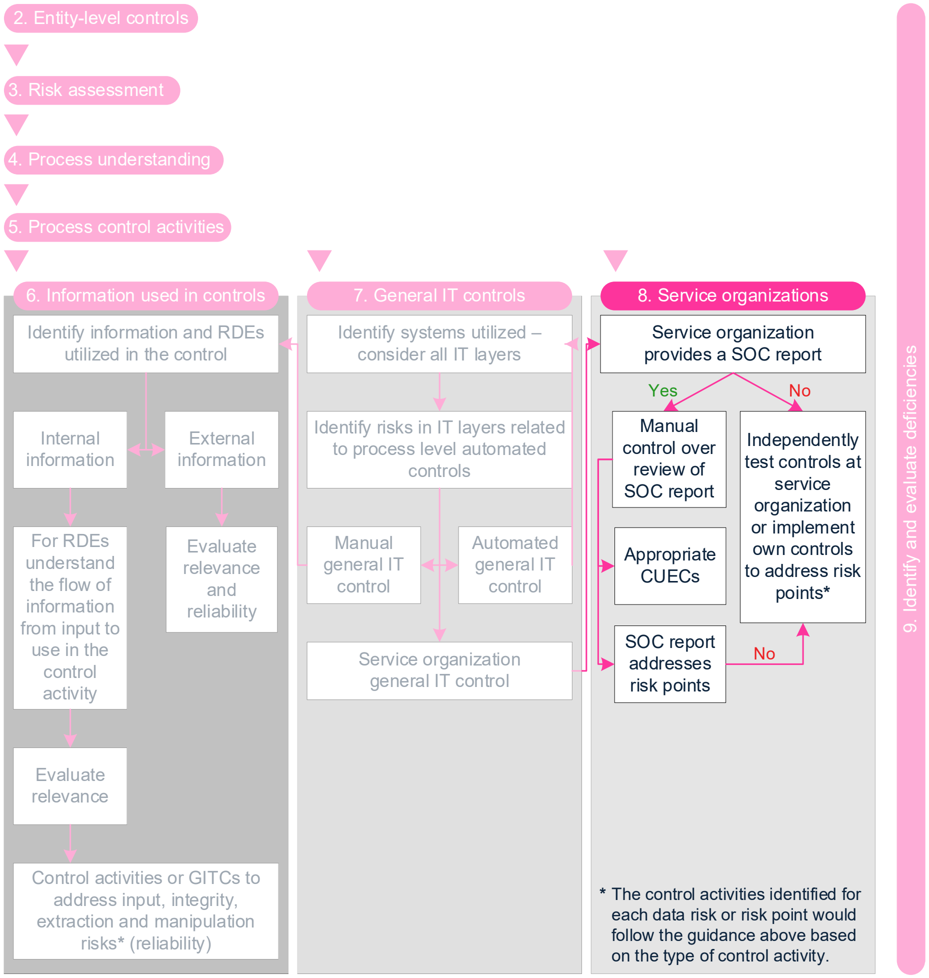
8.1 Management’s ICFR journey

One entity (user entity) may engage another entity (service organization) to provide services that become part of the user entity’s information systems. A common service provided by a service organization is payroll processing.

Depending on the nature of the services provided, a service organization is often considered part of the user entity’s control environment. When this is the case, management’s ICFR journey includes:

- understanding the service organization’s processes;
- evaluating the nature, timing and extent of the service organization’s controls and related testing; and
- assessing deficiencies at a service organization in management’s evaluation of ICFR deficiencies.

Key to performing these activities is whether the service organization provides a SOC report to management, and if so, the nature and contents of that report.


2. Entity-level controls
3. Risk assessment
4. Process understanding
5. Process control activities
6. Information used in controls
Identify information and RDEs utilized in the control
Internal information
External information
For RDEs understand the flow of information from input to use in the control activity
Evaluate relevance and reliability
Evaluate relevance
Control activities or GITCs to address input, integrity, extraction and manipulation risks* (reliability)
7. General IT controls
Identify systems utilized – consider all IT layers
Identify risks in IT layers related to process level automated controls
Manual general IT control
Automated general IT control
Service organization general IT control
8. Service organizations
Service organization provides a SOC report
Yes
No
Manual control over review of SOC report
Independently test controls at service organization or implement own controls to address risk points*
Appropriate CUECs
SOC report addresses risk points
No
* The control activities identified for each data risk or risk point would follow the guidance above based on the type of control activity.
9. Identify and evaluate deficiencies

This chapter starts by providing essential information related to:

- the role of service and subservice organizations in a user entity's ICFR and management's responsibilities related to those roles (see sections 8.2 and 8.3); and
- the nature of the SOC reports that may be issued by a service organization (see section 8.4).

Next, this chapter discusses the following specific management responsibilities related to a service organization's involvement in the user entity's ICFR.

Management responsibilities	Section
Monitoring service organizations and subservice organizations	8.5
Understanding ICFR at a service organization and assessing the relevance of controls to the specific service provided to the user entity	8.6
Implementing appropriate complementary user entity controls (CUECs)	8.7
Reviewing SOC reports to determine whether the reports provide the entity's management with sufficient evidence to address a risk point	8.8
Evaluating deficiencies in a SOC report	8.9
Identifying relevant information covered by a SOC report	8.10
Evaluating whether the period(s) covered by the SOC report is appropriate for the entity, including performing appropriate procedures over the period subsequent to the issuance of the report	8.11
Responding when no SOC report is available or identifying 'control gaps' when a SOC report does not achieve the desired objective of the entity's management	8.12

A common theme in many of these responsibilities is the importance of the user entity maintaining effective communication with the service organization so there are no surprises in the SOC report.

Abbreviations

We use the following abbreviations in this chapter.

AICPA	American Institute of Certified Public Accountants
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CUEC	Complementary user entity control
GITC	General IT control
ICFR	Internal control over financial reporting
PCAOB	Public Company Accounting Oversight Board
PRP	Process risk point
RAFIT	Risk arising from IT
RMM	Risk of material misstatement
SOC	System and Organization Controls

8.2 Management's responsibilities related to a service organization

Question 8.2.10
What is a service organization?

Interpretive response: A service organization provides services to a user entity (the entity that has engaged the service organization) that may become part of that user entity's information systems. However, all service providers are not service organizations.

For example, an entity might outsource actuarial services. In some cases, the nature of the actuarial services represents management's use of an expert, and the actuary is not a part of the entity's information system or control environment. An example of this is when management performs independent controls over all the process risk points (PRPs) over the development of the estimate. However, if the actuary uses IT software to perform their calculations, and/or performs controls over the completeness and accuracy of the data from input to extraction that are relied on by the user entity, it would be considered a service organization.

Question 8.2.20
What type of services can a service organization provide?

Interpretive response: A service organization can provide different types of day-to-day transactional processing services to a user entity, such as payroll processing, cloud computing, investment management or maintenance of accounting records. In performing these services, the service organization performs activities and related controls that the user entity would otherwise normally perform.

Although most controls at the service organization are likely to relate to financial reporting and control activities, there may be other controls that are also relevant to the user entity, such as controls over the safeguarding of assets.

For example, an entity may use a service organization to:

- Process payroll
- Provide shipping services
- Perform distribution services
- Provide inventory storage
- Perform the tax compliance function
- Service mortgages
- Provide custodian and trust services for pension plan assets

- Provide hosting services for applications, IT infrastructure components, or functions that the entity can access from external service providers

Question 8.2.30

Are all service organizations relevant to the user entity's ICFR?

Interpretive response: No. Not all service organizations or services performed by a service organization are relevant to the user entity's ICFR. However, careful evaluation of the nature of the services, and how they interact with the user entity's business processes, should be made if concluding the services are not relevant to the user entity's ICFR (i.e. if determined to not contain a potential risk of material misstatement (RMM) or a PRP).

Question 8.2.40

What is the difference between a service organization and a vendor?

Interpretive response: A service organization has controls necessary to cover and/or mitigate a risk point (PRP or Risk arising from IT (RAFIT)) within a financial reporting process. For example, a service provider that processes payroll is responsible for calculating payroll, taxes and deductions, and distributing payments. A vendor's controls are not necessary to cover and/or mitigate a risk point within a financial reporting process. For example, a vendor is responsible for picking up backup tapes and storing them at an off-site location.

Question 8.2.50

What is management's responsibility over a service organization?

Interpretive response: An entity's management is responsible for maintaining ICFR, which includes relevant service organizations. Management is responsible for the design, implementation and maintenance of internal controls. These responsibilities extend to internal controls at relevant service organizations.

The entity's management is responsible for:

- monitoring service organizations and subservice organizations (see section 8.5);
- understanding ICFR at a service organization and assessing the relevance of controls to the specific service provided to the user entity (see section 8.6);

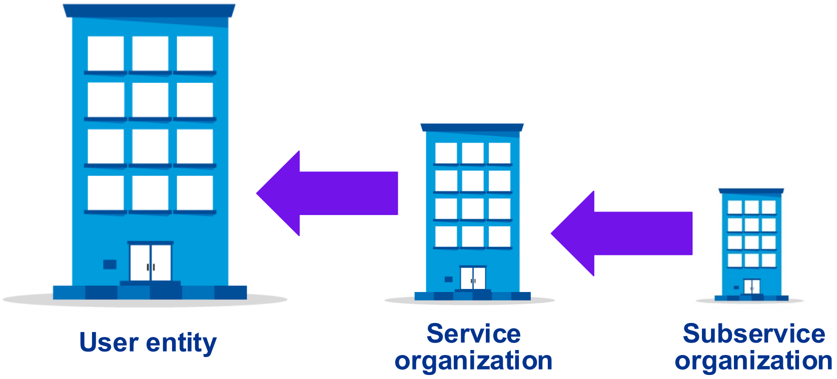
- implementing appropriate CUECs (see section 8.7);
- reviewing SOC reports (see section 8.4) to determine whether the reports provide the entity's management with sufficient evidence to address the risk point (see section 8.8);
- evaluating deficiencies in a SOC report (see section 8.9);
- identifying relevant information covered by a SOC report (see section 8.10);
- evaluating whether the period(s) covered by the SOC report is appropriate for the entity, including performing appropriate procedures over the period subsequent to the issuance of the report (see section 8.11); and
- identifying 'control gaps' when the SOC report does not achieve the desired objective of the entity's management (see section 8.12).

8.3 Management's responsibilities related to subservice organizations

Question 8.3.10
What is a subservice organization?

Interpretive response: A subservice organization is an organization that a service organization uses to perform some of the services provided to the user entity. These services may also be relevant to the user entity's ICFR. A subservice organization may be a separate entity from the service organization or may be related to the service organization.

Subservice organizations can also be thought of as the entities to which service organizations outsource some of their operations.



Question 8.3.20
How will management know if a subservice organization is used by a service organization?

Interpretive response: When a service organization uses a subservice organization, the service organization identifies the subservice organizations that may be relevant to achieving the control objectives included in the SOC report (see section 8.4). The service organization may use either the inclusive method or the carve-out method as it relates to the subservice organization.

Inclusive method	Carve-out method
When the service organization includes the subservice organization's relevant control objectives and related controls in the service organization's description of its system and the scope of the service auditor's engagement.	When the service organization excludes the subservice organization's relevant control objectives and related controls from the service organization's description of its system and the scope of the service auditor's engagement. Under this method, the service organization must identify complementary subservice organization controls (CSOCs) at the subservice organization (see Question 8.3.40).

Question 8.3.30
When is a subservice organization relevant to the user entity's ICFR?

Interpretive response: Just like a service organization, a subservice organization is relevant to the user entity's ICFR when its services, and the related controls, are part of the user entity's information system, including the IT environment relevant to financial reporting.

Practical tip

Many service organizations are using ‘cloud computing services,’ which are usually outsourced and, therefore, considered a subservice organization relied on by the service organization. Due to their prevalence, multiple SOC reports that are relevant to a user entity’s internal control system may rely on the same subservice organization.

Management should identify subservice organizations early and have open communication between the control operators reviewing SOC reports (see Question 8.8.10). Doing so will identify any overlap in the subservice organizations used and potentially provide an opportunity to eliminate duplicate efforts in reviewing SOC reports.

Question 8.3.40

What are the user entity’s responsibilities related to subservice organizations?

Interpretive response: When a service organization uses a subservice organization, the user entity treats these subservice organizations the same as other service organizations (see Question 8.2.50).

Consistent with its responsibilities related to a service organization, the user entity should:

- understand the processes and controls at the subservice organization; and
- obtain sufficient information about the types of transactions that the subservice organization processes, the materiality of those transactions and the ultimate effect on the user entity's financial statements arising from those transactions.

Understanding the activities performed by the subservice organization may identify additional risks and risk points in the process.

The user entity must also review the CSOCs listed in the SOC report of the original service organization and determine whether the controls at the subservice organization appropriately address the CSOCs. The evaluation of the relevant controls at the subservice organization is consistent with that of a service organization as discussed throughout the remainder of this chapter, including the evaluation of deficiencies.

For example, a service organization uses a subservice organization as a cloud hosting service. In their SOC report, the service organization indicates that the subservice organization needs to include:

- encryption of data during transmission; and
- change management and software development controls.

Therefore, the subservice organization SOC report would need to include controls that address the related risks.

8.4 Reports user entities can obtain for service organizations

Question 8.4.10

What is a SOC 1 report?

Interpretive response: A SOC 1 report addresses the controls at a service organization that are likely to be relevant to user entities' ICFR. The service auditor provides an opinion letter on the SOC 1 report, the “service auditor’s report". There are two types of service auditor reports (Type 1 and Type 2), and they are discussed in Questions 8.4.20 and 8.4.30.

Practical tip

Before signing an agreement with a service organization, management should understand if a SOC 1 report (or a SOC 2 report – see Question 8.4.80) is available, and if so, request to see it.

Management should understand the scope, nature, timing and extent of the procedures included in the SOC 1 report before entering into an agreement with a service organization. Having this understanding is necessary because the service organization will form part of the user entity's control environment.

Reviewing a SOC 1 report before selecting a service organization helps management verify that the report addresses the risk points, controls and information that will be relied on by the user entity. Management considers including a requirement in the contract or agreement with the service organization that an appropriate SOC report be provided on an annual basis.

Question 8.4.20

What is a Type 1 service auditor's report?

Interpretive response: A Type 1 service auditor's report provides an opinion about whether the controls at the service organization are appropriately designed and implemented to achieve the specified control objectives, and whether those controls are placed in operation as of a specific date. However, a Type 1 service auditor's report does not provide any evidence of the operating effectiveness of the relevant controls, and therefore does not provide much evidence to management for their ICFR considerations.

Question 8.4.30

What is a Type 2 service auditor's report?

Interpretive response: A Type 2 service auditor's report provides an opinion about whether the controls at the service organization are appropriately designed and implemented to achieve the specified control objectives, and whether those controls are operating effectively throughout a specified period of time.

Question 8.4.40
What are the different components of a SOC 1 report?

Interpretive response: A SOC report contains the following components:

- the Independent Service Auditor's report that includes:
  - an opinion on the fairness of presentation of the description of the service organization's system, the suitability of the design of the controls to achieve control objectives, and in a Type 2 report, the operating effectiveness of the controls to achieve control objectives;
  - the scope and period of the examination;
  - the service auditor's responsibilities; and
  - any inherent limitations of the report;
- management's assertion, which is a written assertion from management of the service organization on the fairness of presentation of their description of the system, the suitability of the design of controls to achieve control objectives and, in a Type 2 report, the operating effectiveness of the controls to achieve control objectives based on criteria specified in the assertion;
- description of systems and/or services provided, the processes and the control environment, including the related;
  - subservice organizations and CSOCs;
  - CUECs;
  - control objectives; and
- tests of controls for each control objective (only in a Type 2 report), which includes a description of the service auditor's tests of the controls and the results of the tests.

The report may also include other information that is not subjected to audit procedures by the service auditor.

Question 8.4.50
What are control objectives in a SOC report?

Interpretive response: Control objectives are the aim or purpose of specified controls at the service organization. Control objectives address the risks that controls are intended to mitigate. Controls are designed, implemented, and documented by the service organization to provide reasonable assurance about the achievement of the control objectives relevant to the services covered by the service auditor's report. Examples of control objectives include change management, incident management, logical security, invoice payment processing, pension administration processing controls, etc.

Question 8.4.60

Do SOC 1 reports address cybersecurity risks?

Interpretive response: SOC 1 reports have limited ability to address cybersecurity concerns related to service organizations. Management needs to understand where a service organization's cyber risk may significantly affect their ICFR environment. In addition, management may implement vendor management programs where they perform periodic security assessments at the service organization.

Practical tip

User entities can initiate a vendor review process requiring the service organization complete a cybersecurity checklist or survey on an annual basis.

Question 8.4.70

Can management rely on a service organization's SOC 1 report to address PRPs related to key calculations relevant to ICFR?

Interpretive response: Management may only rely on a SOC 1 report to address calculation risk if the description of the system and the control objectives and test procedures within the SOC 1 report describe risks and controls related to the specific calculation. Calculation risk can include inherent functionality in software used by the user entity (e.g. depreciation expense or price times quantity) or calculations of more complex items by service organizations (e.g. pension liability calculations).

Practical tip

In some cases, the management description section of the SOC 1 report, combined with the controls identified in the SOC 1 report, provide enough information to conclude that the SOC report addresses PRPs related to key calculations relevant to ICFR. Conversations with the service organization can also assist in clarifying whether and where they address calculations or inherent functionality.

Question 8.4.80

What is a SOC 2® report?

Interpretive response: A SOC 2 report, Reporting on an Examination of Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy, covers a service organization's controls relevant to one or more of the following trust categories as they pertain to the information processed by a system:

- security;
- availability;
- processing integrity;
- confidentiality; and
- privacy.

A SOC 2 report provides information about, and a service auditor's opinion on, whether controls were designed and operated effectively (the latter only in the case of a Type 2 report) to achieve the service organization's service commitments and system requirements in accordance with the AICPA trust services criteria for the selected trust categories. The trust services criteria have been aligned to the 17 criteria (known as principles) presented in the COSO framework (see chapters 2 and 5 for the COSO principles). In addition to the 17 principles, the trust services criteria include additional criteria supplementing COSO principle 12.

Like SOC 1 reports, there are two types of service auditor reports that may be included in a SOC 2 reports (Type 1 and Type 2), and they are discussed in Questions 8.4.20 and 8.4.30.

Question 8.4.90

Can Type 2 SOC 2 reports provide management with evidence on ICFR at a service organization?

Interpretive response: It depends. A Type 2 SOC 2 report may be used as evidence of the existence and operating effectiveness of controls included in the report if the system that is the subject matter of the report is relevant to the user entity's ICFR. Due to the nature of a SOC 2 report, careful consideration is needed to evaluate whether the SOC 2 report properly addresses ICFR-related risks. For example, if the report only covers security, the functionality of the system will not be covered.

Management should determine which trust services criteria specified in the report are relevant to the entity’s ICFR and may address the entity’s RAFITs for a specific technology layer(s) (see section 7.2). In doing so, management should consider the following:

- the nature of the services provided by the service organization to the user entity;

- the relevance of the system that is the subject matter of the report and the relevance of the trust services categories and related criteria to ICFR to address the user entity's RAFITs for relevant IT system layer(s);
- the boundaries and components (infrastructure, software, people, data, procedures) of the system that is the subject matter of the report and their relevance to the user entity's RAFITs for relevant IT system layer(s); and
- the service commitments and system requirements described in the report and their relevance to the user entity's RAFITs for relevant IT system layer(s).

8.5 Management's monitoring of service organizations and subservice organizations

Question 8.5.10

To what extent does management address each service organization and subservice organization when assessing the effectiveness of the entity's ICFR?

Interpretive response: Management must determine the extent to which they address each service organization and subservice organization in their assessment of the effectiveness of ICFR. A number of factors are considered by management when making this determination, including:

- the significance of the transactions or information processed by the service or subservice organization to the entity's financial statements;
- the risk of material misstatement due to error or fraud associated with the business activities processed by the service or subservice organization;
- the nature and complexity of the services provided by the service or subservice organization and whether they are unique to the entity or highly standardized and used extensively by many;
- the extent of the delegation of authority to the service or subservice organization;
- the extent to which the entity's processes and controls interact with those of the service or subservice organization and whether the entity has controls in place that can independently achieve the objectives of effective ICFR; and
- the extent to which the entity depends on the effective internal controls of the service or subservice organization.

Addressing a service organization or subservice organization includes obtaining an understanding of the business processes affected by the organization and identifying the relevant risks and controls.

Question 8.5.20

How does management monitor service organizations and subservice organizations?

Interpretive response: Management monitors service organizations and subservice organizations by establishing consistent and ongoing communication and by reviewing the organizations' SOC reports.

In many cases, service organizations issue SOC reports only on an annual basis (with some on a biannual basis). Management must consider the timing of when they will receive the SOC report, as it may be close to, or after their year-end and related reporting deadlines. An unexpected control deficiency, qualified or adverse opinion, or delay in issuance of the SOC report can result in management being unable to rely on the report for their ICFR.

Communication with the service organization on a regular basis can help diminish some of the risk of learning about an unexpected issue with little time to address it. Communication should also exist with subservice organizations deemed in scope, either directly or through the service organization.

Practical tip

While there can be changes year-over-year in a SOC report, when a service organization has a change in service auditor there can be more significant changes in the SOC report due to the new perspectives of a different service auditor. This includes modifications of control objectives or controls, and/or the nature, timing and extent of control testing performed. Maintaining open communication with the service organization can allow more timely knowledge of these changes and the ability to evaluate and respond to them on a timely basis.

8.6 Management's understanding and assessment of the service organization's ICFR

Question 8.6.10

How does management obtain an understanding of the service organization and their ICFR?

Interpretive response: Management may use a variety of information sources to help obtain a sufficient understanding of the service organization, including the scope of work, the services and processes provided by the service organization and their ICFR. These information sources may include:

- SOC reports (Type 1 or Type 2 SOC reports), if available;
- user manuals;
- system overviews;

- technical manuals;
- the contract or service level agreement between the user entity and the service organization that shows the services to be provided; and
- contact with the service organization or visits with the service organization to perform inquiries and other procedures.

Management may also be able to leverage the knowledge obtained through experience with the service organization, including prior year SOC reports, particularly if the services and controls at the service organization over those services are highly standardized.

Question 8.6.20

How does management use a SOC report to assess the relevance of controls of a specific service provided to the user entity?

Interpretive response: Management considers the following items when determining whether the tests of controls and results included in the SOC report are relevant to the specific service that are significant to the entity's financial statements:

- whether the control objective and the underlying controls are relevant to the user entity in that they address a risk point identified by the user entity's management; and

- whether the nature, timing and extent of relevant tests of controls provides sufficient appropriate evidence of the effective operation of the controls.

Generally, the user entity first identifies the relevant control objectives and then determines the relevant underlying controls. Not all controls within a control objective may be relevant to the user entity (see Question 8.8.80).

Question 8.6.30

What does management consider when evaluating the 'nature' of the control testing performed by the service auditor?

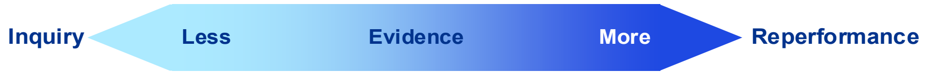
Interpretive response: When evaluating the ‘nature’ of the control testing performed by the service auditor, management considers the type of procedures applied by the service auditor. These procedures should include those akin to the procedures performed in the testing of controls (inquiry, observation, inspection, reperformance) (see Question 5.18.50).

Question 8.6.40

How does management determine whether the nature of the tests of controls performed at the service organization is appropriate?

Interpretive response: When determining whether the nature of tests of controls performed at the service organization is appropriate, management considers the level of risk (i.e. inherent risk) associated with the risks being addressed at the service organization. That level of risk informs management about the type, persuasiveness and quantity of evidence needed to conclude whether the nature of the tests of controls performed is appropriate.

Some types of tests of controls, by their nature, produce more evidence of the effectiveness of controls, while others produce less evidence.



Question 8.6.50

How does management evaluate whether the timing of relevant tests of controls provides sufficient appropriate evidence?

Interpretive response: Generally, within the service auditor report, the service auditor does not disclose the timing of each test of controls. Therefore, the user entity should rely on the service auditor to appropriately determine the timing in relation to the dates covered by their service auditor report.

Section 8.11 discusses considerations relevant to the timing of the service auditor report.

Question 8.6.60

What does the 'extent of evidence' refer to in the context of a service organization’s SOC report?

Interpretive response: The extent of evidence refers to the quantity of evidence obtained by the service auditor. While the Type 2 service auditor report does not necessarily disclose the number of sample items the service auditor tested unless there is a control exception noted, the report does disclose whether the items tested represent all or a selection of the items in the population. The responsibility of selecting the appropriate sample size resides with the service auditor.

Question 8.6.70
What does management consider when evaluating the 'extent' of the control testing performed by the service auditor?

Interpretive response: The responsibility of selecting the appropriate sample size resides with the service auditor and should be based on their methodology. Management considers if the extent of evidence obtained by the service auditor is sufficient based on the adequacy of:

- the controls selected for testing by the service auditor (e.g. whether the service auditor tested controls that appear to appropriately achieve the control objective); and
- the method used to test the control (e.g. whether the service auditor tested the full population or a sample of items).

8.7 Management's implementation of appropriate complementary user entity controls

Question 8.7.10
What are CUECs?

Interpretive response: CUECs are controls that the service organization assumes, in the design of its system, will be implemented by user entities to achieve the control objectives stated in the SOC report.

Question 8.7.20
How is it determined which CUECs are to be considered by the user entity?

Interpretive response: The SOC report links CUECs directly to control objectives within the report. Therefore, the CUECs linked to control objectives relevant to the user entity should be considered by the user entity. Management is responsible for implementing controls that address each CUEC deemed necessary by the service organization for control objectives relied on by the user entity. However, the way management does so may vary. For example, if one relevant control objective has four associated CUECs, management may implement one control activity to address all four CUECs.

In addition, management may determine that some CUEC's linked to control objectives are not relevant to the user entity. For example, for a SOC 1 the

CUEC is that user entities are responsible for complying with all laws and regulations.

Practical tip

Management may also identify controls that do not need to operate in the current year. For example, for a pension plan SOC 1 the CUEC is that user entities are responsible for reviewing and approving the Scope of Services and Plan Design document before implementation. For a plan that has been with the service provider for prior years and where there are no plan modifications in the current year, this is not a relevant risk in the current year.

Question 8.7.30

What if certain CUECs linked to a relevant control objective are not relevant to the user entity?

Interpretive response: When CUECs linked to a relevant control objective are not relevant to the user entity, management documents the rationale and the procedures performed to reach that conclusion.

Question 8.7.40

How does the user entity design controls to address CUECs identified in the SOC report?

Interpretive response: When developing controls to address the relevant CUECs identified in the SOC report, management should first look to existing controls to determine if controls already in place can address the CUECs. Where there is not a current control in place at the user entity, management should design one to respond to the CUEC identified in the SOC report.

If a CUEC has been identified as relevant, it is required to be addressed by a control and not a process for the user entity to rely on the control objective at the service organization.

8.8 Management's review of SOC reports to evaluate effectiveness of controls

Question 8.8.10
Should management have a control that requires review of SOC reports?

Interpretive response: Yes. Management should implement a formal control to review each SOC report to determine whether the reports provide sufficient evidence to support the effectiveness of the service organization's controls.

Question 8.8.20
What is the first step performed by the control operator when reviewing the SOC report?

Interpretive response: The first step the control operator performs is evaluating whether they have the appropriate SOC report and whether the report addresses the necessary systems and services that the user entity relies on.

For example, a payroll provider may have multiple SOC reports that cover different systems and services. The control operator should read the report to verify that the system used by the user entity is covered by that particular report. Specifically, the management description that includes background information and a description of the software, people, procedures and data. The control operator should also review this description closely to determine what the service organization may have chosen to exclude from the report.

Question 8.8.30
Who should perform the control to review the SOC report?

Interpretive response: It depends on the contents of the report. While some SOC reports only address GITCs related to the service organization, others address only process control activities, and some address both types of control activities.

When determining who should perform the control, management should consider who understands the entity's use of the service organization from both a process understanding perspective (see chapter 4) and an IT controls perspective (see chapter 7). In many cases, the individual with the process understanding may not be involved or have proper knowledge of what access the user entity has to the service organization's IT system and what controls they rely on at the service organization. Therefore, multiple control operators may need to perform the SOC report review control together.

In addition, training may be required to provide the control operator(s) with the knowledge needed to appropriately review all relevant pieces of the SOC report. The need for such training may be due to the infrequent nature of SOC report reviews and/or the specialized nature of the SOC report.

Example 8.8.10

Identifying control operators to perform the SOC report review control

The user entity has a SOC 1 report for a service organization that provides procurement invoicing services, including loading of invoices into the system and utilization of the service organization's software. There are process control objectives and GITC control objectives that the user entity would rely on.

The user entity's management determines that the Senior Manager of Procurement has the proper knowledge of the risks and controls relied on at a process level, specifically that the user entity uses and relies on the loading of invoices into the system and the related control objectives. However, management is aware that the Senior Manager does not have experience reviewing SOC 1 reports.

The user entity's management also determines that the Manager of Procurement Systems has the proper knowledge of the risks and controls relied on related to the service organization's software and IT system, specifically:

- what access the user entity has to the system;
- what GITCs are performed at the user entity; and
- what GITCs are performed by the service organization.

Based on the nature of the information in the SOC 1 report, the user entity's management decides that both the Senior Manager of Procurement and the Manager of Procurement Systems should perform the control to review the SOC 1 report. In addition, due to the Senior Manager of Procurement's lack of experience reviewing SOC 1 reports, Internal Audit provided a template for the control operators to fill out as part of their review and held a training session for the control operators before performing the review.

Question 8.8.40

How often should the control to review a SOC report operate?

Interpretive response: The control to review a SOC report should operate with each issuance of the SOC report. For example, if the SOC report is provided bi-annually, the control operator should perform the control biannually.

Practical tip

With a new service organization, management may wish to obtain a prior SOC report (if available) and perform an instance of the review control to evaluate whether the SOC report appropriately addresses the systems, processes and risks the entity has identified as part of their process walkthroughs. While the SOC report may have changes within the period, performing the review control on a prior SOC report would give management time to provide feedback to the service organization and implement CUECs and/or other controls to address risks that the SOC report does not appropriately address.

Question 8.8.50

What should the control operator review and document for the SOC report review control?

Interpretive response: The SOC report review control and related documentation should cover the following:

- the service auditor and their reputation and competence (see Question 8.8.60);
- the type of SOC report issued, whether it provides the necessary scope, nature, timing and extent of the procedure performed and whether there is a qualified or adverse opinion, an emphasis of matter in the opinion or a disclaimer of opinion (see section 8.4);
- the date of the SOC report (see section 8.11);
- the bridge letter (where applicable) (see Question 8.11.50);
- the relevant control objectives and control activities and whether the controls performed are relevant and sufficient to address the PRPs and/or RAFITs that are relevant to the user entity (see section 8.6);
- an evaluation of any exceptions or deficiencies identified in the SOC report and their effect on the user entity's ability to rely on the SOC report (see section 8.9);
- the CUECs addressed through the user entity's controls or the reasons why a CUEC is determined not to be relevant to the user entity (see section 8.7); and
- how the user entity's controls specifically address each applicable CUEC (see Question 8.7.40).

In addition, when there are relevant subservice organizations (see section 8.3), the procedures performed by the control operator depend on the method used by the service organization to report on the subservice organizations (see Question 8.3.20):

- When the carve out method is used, the control operator performs the same SOC report review control over each subservice organization SOC report.

- When the inclusive method is used, the control operator reviews the control objectives and control activities within the service organization's SOC report for relevance and sufficiency.

Practical tip

Given the fact that SOC 1 controls can be performed by different control operators and the nature and extent of the attributes to be performed, management should consider developing a template to document the SOC report review controls.

Question 8.8.60

How does the control operator evaluate the service auditor?

Interpretive response: The AICPA's standards indicate that only a CPA firm can issue a SOC report. As such, the control operator verifies that the service auditor is a CPA firm. In addition, the service auditor's professional reputation and competence may be evaluated by making inquiries or reviewing publicly available information from the following:

- PCAOB;
- AICPA;
- the applicable state society of certified public accountants and/or the local chapter, or in the case of a non-US auditor, their corresponding professional organization;
- other practitioners;
- bankers and other credit grantors;
- other appropriate regulatory agencies, if applicable; and
- other appropriate sources, including additional professional organizations.

The control operator may already have insights into the professional reputation and competence of the service auditor or other auditor based on the operator's previous experience or the service auditor's standing in the marketplace.

Question 8.8.70

Does the control operator focus on control objectives or the individual controls when evaluating the SOC report?

Interpretive response: Both. Ultimately, the control operator focuses on both control objectives and individual controls. However, control objectives provide a good starting point to identify the areas of the SOC report where the controls are likely to be relevant to the user entity's internal control environment.

Question 8.8.80

How does a control operator address controls within a relevant control objective that are not relevant to the user entity?

Interpretive response: When there are specific controls within a relevant control objective that are not relevant to the user entity, the control operator should identify those controls and document the rationale for why they are not relevant.

For example, a user entity may know that the service organization processes their transactions using only system ABC. But there is a control objective that includes controls over two different systems – systems ABC and XYZ – and the service auditor tests separate controls specified by the service organization that are unique to each system. In this situation, the control operator may conclude that the controls that address system XYZ are not relevant to the user entity.

Service auditors generally consider the suite of controls necessary to address each control objective in reaching their overall conclusions. Because the control operator is less informed of the controls at the service organization than the service auditor, the control operator should think carefully about the controls before concluding that one or more are not relevant. This is to avoid reaching that conclusion when the controls are a key part of addressing the ultimate control objective relevant to the ICFR environment.

There may be situations where the control operator is unable to determine whether a related control within a relevant control objective is relevant to the user entity based on the information provided by the Type 2 SOC report. In this situation, the control operator should assume the control is relevant and necessary to the effective operation of the other controls that are directly responsive to risks at the user entity or may ask the service organization for further information.

Question 8.8.90

What procedures does the control operator perform when the service auditor uses the carve-out method for a subservice organization?

Interpretive response: When a service organization uses the carve-out method to report on subservice organizations (see Question 8.3.20), the service organization identifies CSOCs that it assumes will be implemented by those subservice organizations and necessary to achieve the control objectives.

The control operator determines whether there is a SOC report covering the subservice organization that addresses the CSOCs. If there is no SOC report issued for the subservice organization, the control operator could:

- implement controls over the activities of the subservice organization;
- test the controls directly at the subservice organization; or

- use another auditor to test the subservice organization's controls, which may include obtaining an agreed-upon procedures or other relevant attestation report.

Practical tip

It is generally difficult to perform any of these alternative procedures if a relevant subservice organization is not included in a SOC 1 report. Therefore, timely communication with the service organization to confirm the availability of a subservice organization SOC report for management's use is critical.

Question 8.8.100

What is management's responsibility when a cybersecurity incident is identified at a service organization?

Interpretive response: For an identified cybersecurity incident at a service organization, management should discuss it with the service organization and determine:

- the incident's magnitude;
- the effects of the incident on the user entity's data; and
- the actions taken by the service organization to evaluate the extent of the incident's effects on the user entity.

Question 8.8.110

What are management's responsibilities if the service auditor or other auditor issues an agreed-upon procedures or other attestation report?

Interpretive response: If an agreed-upon procedures or other attestation report is issued by the service auditor or another auditor, instead of a Type 1 or Type 2 service auditor report, management must determine whether the procedures performed are sufficient for their purposes by considering the following questions.

- Do the controls tested by the service auditor address the right PRPs and relevant assertions for the RMMs?
- Did the service auditor use sufficient sample sizes for control tests performed?
- Is the nature, timing and extent of procedures performed by the service auditor sufficient for the control being tested?
- What is the effect of any identified control deficiencies on the control environment?
- What were the results of performing inquiries over the service auditor's or other auditor's professional reputation, competence and independence?

Question 8.8.120

What are management’s responsibilities if the service auditor issues an agreed-upon procedures report to specified parties?

Interpretive response: When using an agreed-upon procedures report, management must determine that the procedures are appropriate for the user entity’s purpose. When the report is restricted to specified parties, only those parties listed may use the report as evidence. Therefore, the user entity must be listed as one of the specified parties to rely on the report for ICFR purposes. When the report is not restricted to specified parties, the report may be used for ICFR when it is determined that the procedures are appropriate for the user entity’s purpose.

8.9 Management’s evaluation of deficiencies identified in SOC reports

Question 8.9.10

What are management’s responsibilities when a Type 2 SOC report identifies deviations or exceptions within a relevant control objective?

Interpretive response: Because service organization activities and controls form part of the user entity's processes and ICFR, management's ICFR considers internal controls at a service organization. This typically includes management:

- reviewing Type 2 SOC reports (see section 8.8);
- identifying deficiencies in relevant control objectives and related controls; and
- maintaining a process to mitigate the deficiencies, such as developing their own controls that respond to and address deficiencies noted in the Type 2 SOC report.

If a control within a relevant control objective has exceptions, user entity management accumulates and evaluates these exceptions like they do with other control deficiencies identified in the period. This is not necessary for those controls within a control objective previously determined not to be relevant to the user entity (see Question 8.8.80).

As management evaluates exceptions, it considers how they were mitigated and/or remediated and determines how they affect the user entity. It may be necessary to discuss remediation with the service organization directly and may also be necessary to include their service auditor in those discussions.

Chapter 9 provides further discussion of ICFR deficiencies and their evaluation.

Practical tip

At their discretion, service organization management may include an ‘other information’ section within the SOC report. Often, additional information will be provided in this section about exceptions and responses to exceptions, CUECs, or matters related to the scope of the report. For example, if management intends for a different SOC report to address a different set of risks not included in the SOC report being reviewed, it may be noted in the ‘other information’ section.

While the contents of the ‘other information’ section of the SOC report may help with understanding information included in other sections of the report, it is important to understand that it cannot be relied on by the user entity for ICFR purposes because:

- the ‘other information’ is not covered by the service auditor's opinion (i.e. the service auditor expresses no opinion on the ‘other information’); and
- the ‘other information’ has not been subject to procedures applied in the service auditor's examination.

Question 8.9.20

Can management rely on relevant controls without deviations or exceptions that are within a failed control objective?

Interpretive response: Given the interplay of related controls within a control objective, management generally would not rely on controls without deviations or exceptions that are within a failed control objective. This is because service auditors consider the suite of controls necessary to address each control objective in reaching their overall conclusions.

Because user entity management is less informed about the controls at the service organization than the service auditor, they generally don’t have enough information to determine whether controls without deviations or exceptions within a failed control objective can be relied on. The controls with deviations or exceptions within the failed control objective may be a key part of why the service auditor determined the control objective relevant to the user entity had failed.

Question 8.9.30

Does an unqualified service auditor’s report mean there are no deficiencies identified?

Interpretive response: No. An unqualified service auditor’s report does not mean that the service auditor did not identify any control exceptions or deficiencies.

Management should review the results of the service auditor's tests of controls described in the SOC report and evaluate control deficiencies and the effect those deficiencies may have on the user entity's ICFR. Because the service organization's deficiency is also a deficiency for the user entity, the evaluation follows the same process used to evaluate any other control deficiencies at the user entity (see chapter 9).

When there is an unqualified service auditor's report even though deficiencies are noted in the report, compensating controls may exist at the service organization, which are other controls within the relevant control objective that address the same risk as the deficient control. These compensating controls may have been the basis for the service auditor's conclusion that the control objective, as defined in the SOC report, was achieved despite the deficiencies noted.

Question 8.9.40

What are the implications when the service auditor's report has a qualification or other modification?

Interpretive response: When a service auditor's report is qualified, the service auditor concludes that a control deficiency or deficiencies exist and are of such a magnitude that one or more of the control objectives in the SOC report are not achieved.

If the service auditor's report has a qualification or other modification, management needs to understand the reason for the modification and then determine whether it affects the user entity.

For example, a service auditor's report may be qualified due to control deficiencies for controls related to a service that the user entity does not use. In this situation, management may still be able to rely on the other nondeficient controls relative to the control objective because the qualification does not relate to a system relevant to the user entity's ICFR.

Management considers the effects of any qualifications or other modifications to the service auditor's report that affect the user entity's ability to rely on relevant controls due to:

- certain controls are not included that are relevant to the entity; or
- controls relevant to the entity are not effective and, therefore, certain control objectives have not been achieved.

In limited cases, management may develop their own controls that respond to and address issues giving rise to a qualification or modification in a Type 2 SOC report (see Question 8.12.30).

Qualifications or other modifications can be identified by reading the service auditor's report and having discussions with management of the service organization and/or the service auditor.

Practical tip

In many cases, it is difficult to implement a compensating control at the user entity that addresses the risk point that the deficient control was supposed to address. Therefore, management should first discuss the deficiencies with the service organization to obtain further information about them before developing their response or considering the implementation of a compensating control.

Question 8.9.50

What kinds of qualifications can be noted in the service auditor's opinion?

Interpretive response: There are four possible opinions (and one modification to an opinion) a service auditor can express over a SOC report:

- **Unqualified –** The opinion expressed by the service auditor when the auditor concludes that:
  - management's description of the service organization's system fairly presents the service organization's system designed and implemented throughout the specified period (or in the case of a type 1 report, as of a specified date);
  - the controls related to the control objectives stated in management's description of the service organization's system were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the specified period (or in the case of a type 1 report, as of a specified date); and
  - the controls operated effectively to provide reasonable assurance that the control objectives stated in management's description of the service organization's system were achieved throughout the specified period.
- **Qualified –** The opinion expressed by the service auditor when the misstatements in management's description of the service organization's system or deficiencies in the suitability of the design or operating effectiveness of the controls are limited to one or more, but not all, aspects of the description of the service organization's system or control objectives and do not affect the service auditor's opinion on other aspects of the description of the service organization's system or other control objectives.
- **Adverse –** The opinion expressed by the service auditor if the misstatements in management's description of the service organization's system or deficiencies in the suitability of the design or operating effectiveness of the controls are material and pervasive throughout the description or across all or most of the control objectives.
- **Disclaimer –** The service auditor disclaims an opinion when it is unable to obtain sufficient appropriate audit evidence on which to base an opinion and the service auditor concludes that the possible effects on the subject

matters of undetected misstatements, if any, could be both material and pervasive.

- **Emphasis of matter or other matter paragraphs –** The paragraphs a service auditor includes in its report when the service auditor is required or otherwise considers it necessary to include additional communications with its opinion that are not modifications to the opinion itself. These most frequently occur when controls did not operate during the period under audit, and therefore auditors are unable to perform tests the controls to be able to opine on them.

Practical tip

The most important point to keep in mind is that the user entity wants an unqualified opinion in the SOC report. If any other type of opinion is provided, the report should include a description of the service auditor's basis for modifying the opinion. Management must understand this basis and evaluate the effect of the modification on the user entity's ICFR.

Question 8.9.60
Can a user entity rely on an adverse opinion?

Interpretive response: No. Due to the pervasiveness of the control deficiencies in an adverse opinion, the user entity cannot rely on the SOC report and may potentially develop their own controls over the risks at the service organization (see Question 8.12.30).

8.10 Use of relevant information in SOC 1 reports by management

Question 8.10.10
When is information provided by service organizations identified in a business process?

Interpretive response: Information that originates from a service organization can be identified at any point in a business process. Generally, information will be identified during process understanding (see chapter 4) or as part of control activities (see chapter 5).

When controls are implemented and/or tested, the control operator identifies where the information related to the control originates from and the flow of that information through to extraction. Some of this information may come from service organizations.

Question 8.10.20

How does the user entity obtain information from the service organization?

Interpretive response: Information from a service organization can include information that originates from the service organization and is sent out directly by them (e.g. pension reports that are emailed by the service organization to the user entity). Alternatively, the information from the service organization may be pulled by the user entity from, or automatically generated through a system interface with, the software and/or website of the service organization.

Chapter 6 provides further discussion of information used in controls.

Question 8.10.30

What are the different types of information related to a service organization?

Interpretive response: The following table lists the three types of information related to a service organization and provides one or more examples of each.

Type	Example(s)
Information provided by the service organization in response to ad hoc requests from the service auditor	A request by the user entity for a population list of application changes that the service auditor uses to select a sample of items for testing.
Information used in the execution of a control	A user access list used by service organization personnel in an access review control.
Information prepared for user entities	A reporting package, system-generated reports, an invoice or a payroll file reflecting the results of processing a payroll provided to user entities.

Question 8.10.40

When can a SOC 1 report be used to address the risks related to information used in controls or produced for an entity?

Interpretive response: If the Type 2 SOC 1 report only has a general statement that the service auditor has tested controls over the accuracy and completeness of information used in controls or produced for an entity, the user entity cannot simply rely on those controls to substantiate the reliability of the information.

Without knowing what information was included in the controls where completeness and accuracy are tested, the user entity is unable to determine if the reports they are relying on were included. In addition, without the ability to determine what controls were tested by the service auditor over the accuracy and completeness of the information and the relevant data elements, the user entity would be assuming that proper testing was performed without any information on the nature, timing and extent of the procedures. Such an assumption should not be made by the user entity.

However, if a Type 2 SOC 1 report specifies the information the service auditor tested for accuracy and completeness and the controls performed, then the user entity can rely on those controls for that specific information.

Question 8.10.50

What are the implications of a Type 2 SOC 1 report not specifying that information used by management was tested for accuracy and completeness?

Interpretive response: When the Type 2 SOC 1 report does not specify that information used by management was tested for accuracy and completeness, there may be other procedures management can perform, including a combination of:

- inquiring of the service organization and/or service auditor to understand how the control objectives and related controls included in the Type 2 SOC 1 report address the accuracy and completeness of the information, including the relevant data elements;
- reviewing the control objectives and tests of controls performed by the service auditor to assess the controls' operating effectiveness, to determine whether those objectives and tests address the accuracy and completeness of relevant data elements in the information used by management;
- reviewing the control objectives to determine if the Type 2 SOC 1 report includes a control objective, control activities and tests of controls related to the accuracy and completeness of the output produced by the service organization;
- reviewing 'Management's Description' in the Type 2 SOC 1 report to determine if the information is specified as being produced for user entities; and
- inspecting the service-level agreement between the service organization and the user entity to determine if the information is listed as part of the service organization's output delivered to the user entity.

By performing a combination of these and/or other appropriate procedures, management is determining whether:

- information provided by the service organization can be relied on by the user entity; and

- appropriate controls exist over the information and have been tested for operating effectiveness.

Practical tip

Communication with the service organization related to information is very important. User entities should work with their service organizations to request that SOC 1 reports include the appropriate language related to the completeness and accuracy of information such that management can rely on the reports used by the user entity. Management considers the timing of this request to allow an appropriate amount of time for the request to be discussed with and addressed by the service organization. User entities should make every effort to discuss the request with the service organization before signing an agreement.

Question 8.10.60

When the SOC 1 report does not provide evidence over the accuracy and completeness of information from the service organization, what other procedures may management perform to obtain this evidence?

Interpretive response: When a Type 2 SOC 1 report does not provide (or is not used to provide) evidence over the accuracy and completeness of information from the service organization, other procedures management can perform to obtain this evidence include:

- visiting the service organization and testing the relevant controls at the service organization;
- using the work of another auditor; or
- implementing controls over the accuracy and completeness of the information.

8.11 Management’s evaluation of the period covered by the service auditor’s report and gap periods

Question 8.11.10

How does management evaluate whether the period(s) covered by the service auditor’s report is appropriate for the entity?

Interpretive response: When determining whether the timing of test of controls at the service organization is appropriate, management looks to the period covered by the service auditor's report as compared to the period of the financial statements to identify whether there is a gap period (see Question 8.11.20).

The period covered by the service auditor's report should align with (or cover) the period reflected in the financial statements, and any period beyond the date of the service auditor report should be evaluated as the gap period.

Question 8.11.20

What is a gap period?

Interpretive response: A gap period is the time between the end of the period covered by the service auditor's report and the user entity's year-end (i.e. the portion of the entity's financial reporting period not covered by the service auditor's report).

For example, the service auditor's report for payroll processing performed by the service organization covers the period from October 1, 20X1 to September 30, 20X2; however, the entity's financial reporting period is from January 1, 20X2 to December 31, 20X2. There is a gap period from October 1, 20X2 to December 31, 20X2.

Question 8.11.30

What are management's responsibilities when there is a gap period?

Interpretive response: When there is a gap period, regardless of the length, management should understand whether there have been any significant changes to the controls during the gap period at the service or subservice organization.

Management should perform additional procedures to address the gap period (see Question 8.11.20), after considering:

- the significance of the service organization's and subservice organizations' activities to the user entity's ICFR;
- whether there are errors that have been identified in the service organization's or the subservice organizations' processing;
- the significance of the gap period;
- the nature and significance of any changes to the controls at the service organization and/or subservice organization during the gap period; and
- the effectiveness of the control environment and monitoring controls at the user entity.

Although a key factor, the length of the gap period is only one factor in determining its significance. A relatively short gap period could still be considered significant when the activities of the service organization are significant.

Question 8.11.40
How are changes during the gap period identified and assessed?

Interpretive response: Management should determine whether there have been any significant changes to the controls at the service or subservice organization during the gap period. The most common form of making this determination is through obtaining and reviewing a bridge letter from the service organization and subservice organization (as applicable) (see Question 8.11.50). Management may also be able to confirm that no changes occurred during the gap period through inquiries with management.

The following are indicators that there may be changes after the period covered by the SOC report:

- changes in personnel at the service organization with whom management interacts;
- changes in reports or other data received from the service organization;
- changes in contracts or service level agreements with the service organization; or
- errors identified in the service organization's processing.

For example, certain reports management receives from the service organization during the gap period are different from the ones received during the period covered by the service auditor’s report in the SOC report. This may indicate there have been changes to the systems and/or controls of the service organization after the end of the period covered by the service auditor's report.

Question 8.11.50
What is a bridge letter?

Interpretive response: A bridge letter, also known as a gap letter, is an unaudited letter the service organization and/or the subservice organization may make available to user entities to identify and address any material changes to the internal control environment that have occurred during the gap period covered by the letter.

The length of the gap in the period should be considered in determining if the bridge letter alone can address the gap period. If the gap period is deemed to be too long, the user entity’s management will need to perform procedures for that period as if they did not obtain a SOC report (see Question 8.12.30). Obtaining a bridge letter is equivalent with rolling forward a control based solely on inquiry, in that it provides minimal evidence.

Question 8.11.60
What additional procedures may be performed to address changes during the gap period?

Interpretive response: Additional procedures management may perform to address changes during the gap period include:

- implementing process control activities and/or monitoring controls to address changes during the gap period so as not to just rely on a bridge letter (this is the most effective manner to address the gap periods);
- visiting the service organization and testing the operating effectiveness of the controls in the gap period (this could involve management, internal auditors, external auditors or other auditors); or
- obtaining and evaluating any agreed upon procedures reports or other relevant attestation reports issued by the service auditor that address the gap period.

Each engagement is unique, and many factors can affect the procedures that management should perform to address a gap period.

8.12 Management's response if no SOC report is available or 'controls gaps' are identified

Question 8.12.10
What is a 'control gap'?

Interpretive response: A control gap exists in relation to a service organization's ICFR when management identified a risk point within the process provided by a service organization and:

- there is no SOC report available; or
- there is a SOC report available that does not include the proper controls to address the identified risk points of the user entity at the service organization.

Question 8.12.20
How does management address 'controls gaps'?

Interpretive response: Management may address the risks for which 'controls gaps' exist by:

- implementing controls over the activities of the service organization;
- testing the controls at the service organization (where management and/or an auditor performs the tests); or
- using another auditor to test the controls, which may include obtaining an agreed-upon procedures or other relevant attestation report that includes tests of the operating effectiveness of the relevant controls.

Question 8.12.30

Can a user entity establish their own processes and controls over the activities performed by a service organization?

Interpretive response: Yes.

Remember that a service organization is considered part of management's control environment. Therefore, with or without a SOC report, management is required to:

- obtain an understanding of the process performed by the service organization;
- identify risk points within the process; and
- either identify and test controls at the service organization or design controls to respond to the risk points.

In some cases, the user entity may establish their own processes and controls addressing risk points related to the activities of the service organization.

For example, if the entity uses a service organization to process its payroll transactions, the user entity may establish controls over the submission and receipt of payroll information that could prevent, or detect and correct, material misstatements that could occur at the service organization. These controls may include the following:

- comparing the data submitted to the service organization with reports of information received from the service organization after the data has been processed; or
- recalculating all or a sample of the payroll amounts for clerical accuracy and reviewing the total amount of the payroll for reasonableness.

Key takeaways

- Service organizations are considered part of the user entity’s control environment and should be treated that way. This includes:
  - understanding the service organization’s processes;
  - evaluating the nature, timing and extent of the service organization’s controls and related testing; and
  - assessing deficiencies at a service organization in management’s evaluation of ICFR deficiencies.
- Management should obtain prior SOC reports when a new service organization is used to get an early start on planning for its evaluation of the service organization.
- Communication with the service organization is important so the user entity is made aware timely of control deficiencies or other modifications to the service auditor’s report.
- Management should only rely on explicit statements or conclusions included in the SOC report and should not make assumptions about what is not explicitly stated in the SOC report.

9. Identifying and evaluating deficiencies

Detailed contents

Examples

9.3.10 Control deficiency related to implementation of new IT application

9.3.20 Control deficiency related to an error in a warranty accrual spreadsheet

9.3.30 Management's root cause analysis leads to sufficient description of control deficiency related to tax contingency accrual

9.4 Step 3: Determine whether the deficiency is indicative of other deficiencies

Question

9.4.10 What actions are taken to determine whether the control deficiency is indicative of other deficiencies?

Examples

9.4.10 Whether a control deficiency for lack of review precision for an estimate is indicative of other deficiencies

9.4.20 Whether a control deficiency for lack of review is indicative of other deficiencies

9.4.30 Whether a control deficiency for untimely reconciliation review is indicative of other deficiencies

9.5 Step 4: Evaluate the severity of the deficiency individually

Questions

9.5.10 What are the categories of control deficiencies based on severity?

9.5.20 What is a material weakness?

9.5.30 What determines whether a deficiency is a material weakness?

9.5.40 What is a significant deficiency?

9.5.50 What determines whether a deficiency is a significant deficiency?

9.5.60 How is materiality considered in the evaluation of deficiencies in ICFR?

9.5.70 How is the magnitude of a potential misstatement evaluated?

9.5.80 In evaluating the potential magnitude, can only the current period activity be considered?

9.5.90 Can various potential misstatements offset each other to determine the severity of the deficiency?

9.5.100 Are indirect effects of the potential misstatement considered in evaluating the severity of the deficiency?

Examples

Questions

Examples

Questions

Examples

Questions

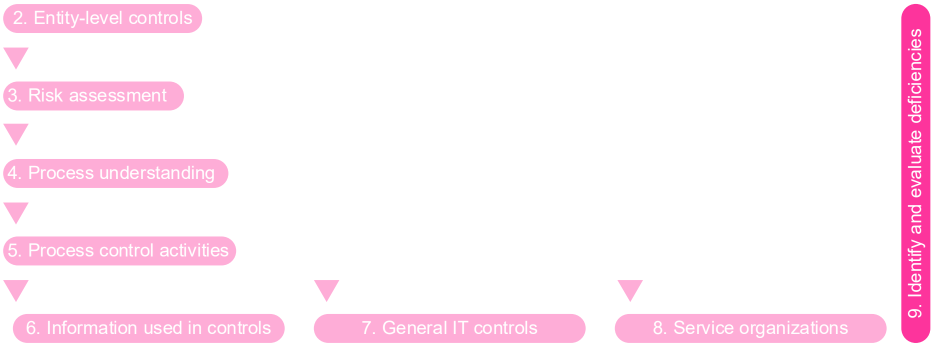
Example

9.1 Management's ICFR journey

Control deficiencies may be discovered during any point of an entity's ICFR. 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. The existence of a control deficiency means that there is an opportunity for a misstatement to occur, even though a misstatement may not have actually occurred.

When a control deficiency is discovered, management is responsible for its identification and evaluation.



Identifying and evaluating control deficiencies may seem straightforward, but challenges may, and often do, arise. This chapter walks through the following six-step process that may help management properly identify and evaluate the severity of control deficiencies, while avoiding or properly navigating common challenges.

Identifying the internal control deficiency	
Step 1	Determine whether a deficiency exists and identify the deficient or missing control (see section 9.2)
Step 2	Understand the cause of the deficiency (see section 9.3)
Step 3	Determine whether the deficiency is indicative of other deficiencies (see section 9.4)
Evaluating the internal control deficiency	
Step 4	Evaluate the severity of the deficiency individually (see section 9.5)
Step 5	Evaluate the effect of compensating controls and conclude on the severity of the individual control deficiency (see section 9.6)
Step 6	Evaluate the severity of similar deficiencies in the aggregate (see section 9.7)

See Appendix C for a template that can be used to document the evaluation of internal control deficiencies under the six-step process outlined above, examples of completed evaluations and a flowchart with key questions and decision points underlying the six-step process.

Also discussed in this chapter are incremental considerations applicable to SEC registrants related to control deficiencies (see section 9.8).

Abbreviations

We use the following abbreviations in this chapter.

COSO	Committee of Sponsoring Organizations of the Treadway Commission
GAAP	Generally accepted accounting principles
GITC	General IT control
ICFR	Internal control over financial reporting
PRP	Process risk point
RAFIT	Risk arising from IT
SEC	Securities and Exchange Commission
SOC	System and Organization Controls

9.2 Step 1: Determine whether a deficiency exists and identify the deficient or missing control

Question 9.2.10
What is a control deficiency?

Interpretive response: 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. The existence of a control deficiency means that there is an opportunity for a misstatement to occur, even though a misstatement may not actually have occurred.

Question 9.2.20
How is a control deficiency identified?

Interpretive response: Deficiencies in internal control can come to management's attention in several ways, including but not limited to the following.

- Management's assessment of ICFR
- External auditor's work
- Service organization reports
- Restatements
- Management's risk assessment or monitoring process
- Operational or compliance deficiencies
- Internal Audit's work (whether or not related directly to ICFR) or other internal sources
- External sources, such as regulatory reports or SEC staff comment letters
- Prior period immaterial error corrections

Some deficiencies, such as those identified by testing internal controls, may be obvious deficiencies in ICFR. Deficiencies found in other ways, such as by reading regulatory reports, might be related to operations or compliance objectives – but may also be indicative of an ICFR deficiency and should be evaluated for any ICFR effect.

Question 9.2.30

If a misstatement in the financial statements is identified, does that mean there is a control deficiency?

Interpretive response: Generally, a misstatement in the financial statements would not exist without a control deficiency that permitted the misstatement to occur. But whether a control deficiency exists depends in part on whether the misstatement was discovered by the external auditor or as a result of the entity's normal operation of its ICFR.

Misstatements identified by the external auditor are usually the result of an underlying control deficiency. However, when misstatements are identified by the external auditor during management's period-end financial statement reporting process before all the entity's controls have operated, judgment is necessary in determining whether there is an underlying control deficiency.

Example 9.2.10

Misstatement in preliminary financial statements identified by management vs external auditor

Overall scenario

Management provides preliminary financial statements to the auditor to expedite the audit with a caveat that they have not completed their financial reporting process and performed the related control activities.

Scenario A

Management identifies and corrects a misstatement in the preliminary financial statements while completing the financial reporting process and related control activities.

Analysis

The identification and correction of the misstatement by management likely indicates that the internal controls are effective, not deficient.

Scenario B

The external auditor detects a misstatement in the preliminary financial statements, knowing management has not fully executed relevant controls.

Analysis

Management uses judgment to determine whether the misstatement is indicative of a control deficiency. Management should be able to identify controls that have not yet operated and are of sufficient precision that they would have detected the misstatement.

Example 9.2.20
Increase in products returned under warranty

Scenario

An internal audit finds that an unusually high number of products are being returned for issues covered by the warranty. This may mean the entity's quality assurance process needs improving (an operational matter).

Analysis

If the entity has controls over the process to accurately estimate the warranty reserve considering the level of returns for issues covered by the warranty, a need for improved quality assurance may not be indicative of an ICFR deficiency. If the entity's controls over the assumptions and/or data used in the warranty reserve did not appropriately consider the increase in the number of products being returned, that may be indicative of an ICFR deficiency.

Example 9.2.30
Completeness of inventory cycle count program

Scenario

An internal audit finds that the entity's inventory cycle count program excludes certain categories of inventory from the counts and needs to be revised.

Analysis

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

Example 9.2.40
ICFR over fair values recognized for a business combination occurring shortly before year-end

Scenario

A calendar year-end entity acquires a business in early December.

Management of the entity 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 (PRPs). However, given the proximity of the acquisition to the fiscal year-end, management and its external expert are in the preliminary stages of determining the fair value measurements. Management's controls over those measurements cannot operate at a level of precision greater than the related process to estimate and record the initial purchase price allocation. As of the reporting date, this process may have significant estimation uncertainty if provisional fair value measurements are used, with that uncertainty to be reduced as management finalizes those fair values within the measurement period.

Analysis

It would not be reasonable to expect that management's controls over the provisional fair value measurements are designed and operating at a higher level of precision than the relevant accounting framework requires of the measurements themselves. Therefore, the controls around the final purchase price allocation (and final fair value measurements) should be more precise than the controls around the initial purchase price allocation (and provisional fair value measurements). This is consistent with the increased precision of the underlying accounting for the final fair values required by the end of the measurement period.

If management's controls are not at the appropriate level of precision in the initial or final purchase price allocation, a control deficiency would exist.

Question 9.2.40

If there is no misstatement, does that mean there is no control deficiency?

Interpretive response: No. A deficiency represents the potential for misstatement. Therefore, a deficiency can exist in the absence of a misstatement.

Question 9.2.50

Are control deficiencies at a service organization considered a control deficiency at the user entity?

Interpretive response: Yes. Deficiencies in controls at a service organization represent a deficiency in the user entity's ICFR when management relies on these controls for the entity's ICFR. Chapter 8 discusses the use of a service organization in the user entity's control environment.

An unqualified service auditor's report does not mean that the service auditor did not identify any control exceptions or deficiencies at the service organization. Control deficiencies identified by the service auditor are included in the detail of the report (see section 8.9). Management considers the control deficiencies identified at the service organization that are relevant to the user entity's ICFR just like any other control deficiencies originating within the entity itself.

Question 9.2.60
What is included when describing a control deficiency?

Interpretive response: The entity correctly describes a control deficiency by identifying:

- the situation where the deficiency was identified;
- the deficient control, including the type of control;
- the type of deficiency (e.g. the control is missing, not designed correctly, or not operating effectively);
- the accounts or disclosures affected;
- the relevant assertion affected;
- the component(s) of internal control affected (and principle(s) of the component affected); and
- the components of the entity affected.

Example 9.2.50
Insufficient description of a control deficiency related to an error in a tax calculation

Scenario

The external auditors find an error in the entity's tax calculation and determine there was a breakdown in the controls related to a management review. Management concludes that, due to the error, the entity has a deficiency in the controls related to the review of the tax calculation.

Analysis

Management's conclusion does not specify which control was missing, designed inappropriately, or operating ineffectively, nor does it address the other items noted in Question 9.2.60. The conclusion is simply saying that the control deficiency is the result of the error in the entity's tax calculation.

It is common, but inappropriate, to describe the control deficiency in terms of the error rather than specifically identifying which controls within the process failed. Using the error to describe the control deficiency will lead to difficulty in determining:

- the true scope of the deficiency;
- whether the deficiency indicates that other deficiencies may exist;
- how to evaluate the severity of the deficiency, including its potential magnitude; and
- whether the deficiency has been remediated.

Example 9.2.60

Use of management's remediation plan as the starting point to describe a control deficiency related to an error in the tax provision

Scenario

The external auditor identifies an error in an entity's tax provision. The entity has a control requiring review of the entity's tax provision by the tax manager. Management's remediation plan is to assign the tax director to perform the same review.

Analysis

The results of the remedial action (tax director's review of the tax provision) may indicate the review control was designed appropriately but not performed correctly – in which case a personnel issue may exist because the Tax Manager had insufficient training or knowledge to effectively perform the control. This result would indicate that Principle 4 of the COSO Framework was likely not met (see Question 2.4.140).

Although management and the external auditor would still need to determine if the remedial action is sufficient and appropriate to address the control deficiency, understanding the nature and extent of the remediation plan helped them identify an appropriate starting point for describing the control deficiency.

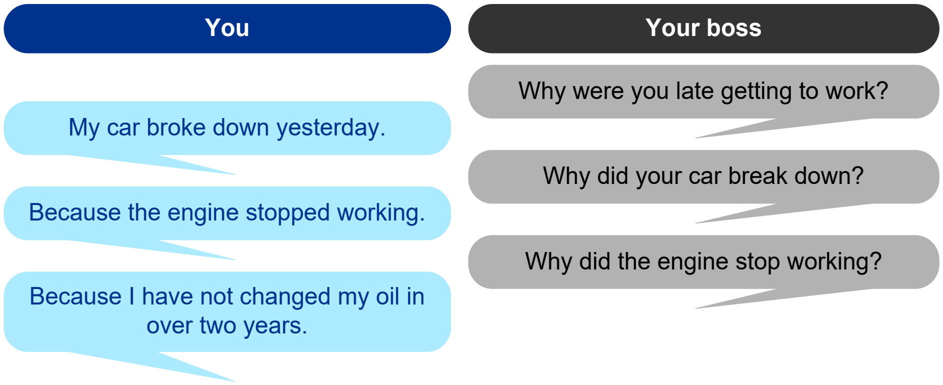
9.3 Step 2: Understand the cause of the deficiency

Question 9.3.10

Why is it important to understand the cause of the control deficiency?

Interpretive response: Understanding why a deficiency occurred helps prevent assumptions from being made on where the control breakdown occurred. Understanding what caused the control deficiency involves asking probing questions containing the interrogatives who, what, where, when, how – and most importantly, why.

For example, say you were late getting to work, which led to the following conversation:



You | **Your boss**

Your boss: Why were you late getting to work?

You: My car broke down yesterday.

Your boss: Why did your car break down?

You: Because the engine stopped working.

Your boss: Why did the engine stop working?

You: Because I have not changed my oil in over two years.

Through this conversation, the true 'cause' for you being late to work comes to light – you not maintaining your car.

The same thought process applies in control deficiency evaluation. The deficiency identified may be due to any number of reasons. So asking the ‘why’ questions peels back the layers to get to what really caused the deficiency. This is considered a ‘root cause analysis’. This approach helps to:

- better describe the deficiency;
- identify interrelated controls that are also deficient and/or expose more pervasive deficiencies; and
- gather all the information that is key to appropriately evaluating the severity of the deficiency, both individually and in the aggregate.

Question 9.3.20

What probing questions can help in understanding what caused a control deficiency?

Interpretive response: In understanding what caused a control deficiency, the first question considered is – why did the control not operate effectively? Was it deficient due to:

- insufficient technical competence of those involved in the control;
- incomplete or inaccurate information used in performance of the control;
- discrepancies in the operation of the control;
- insufficient time to perform or review the control; and/or
- lack of timeliness in performing or reviewing the control?

Management may need to ask ‘why’ several times to peel back the layers to understand what really caused the control deficiency. For example, if the control deficiency was due to incomplete or inaccurate information used in performance of the control, management might next ask why the information was incomplete or inaccurate. Probing questions that might be asked in peeling back the layers include:

- Who was involved in the control? Were the right people involved? Did they have the right level of expertise and knowledge? Did the control operator perform other controls that might also be deficient?

- When did the control operate? Was the control deficiency due to untimely review or performance?
- At what level of detail was the control performed? Was it performed at a sufficient level of precision to be effective?
- What are management's remedial actions? How does management intend to remediate the deficiency?

Practical tip

When assessing the cause of a deficiency, if it is not clear which principle(s) of the COSO Framework is/are not met, more probing questions are needed.

Example 9.3.10

Control deficiency related to implementation of new IT application

Scenario

During the year, the entity implemented a new application control that automatically transfers information via an automated interface between the entity's sub-systems and the general ledger. This automated interface is configured to generate an exception report when the data transfer is not complete and accurate. No exception reports were generated so far in the current year.

When testing the configuration of the automated interface and related exception report, it was determined that the feature to generate the exception report could be turned on and off at any time. When the feature to generate the exception report was turned off, no system alert was generated to notify anyone in the IT department. Thus, incomplete or inaccurate data transfers may not have been detected.

Root cause analysis

Management asked probing questions to understand what caused the potential for incomplete or inaccurate data transfers to go undetected, and determined the following:

- The IT team who implemented the new application was not aware that there was a feature to turn off/on the generation of the exception report.
- Had the IT team read the manual on how the application works, it would have been clear that the on/off feature existed. There was also information in the manual that an alert could be configured to notify someone if this feature was turned off.
- When the new application was implemented, the IT team did not perform any testing to verify whether an exception report would be generated.
- The IT team did not configure the application to generate an audit trail on who makes changes to the application and what those changes are, which

would have identified that the exception report functionality had been turned off, by whom and when.

- There was no training or resources for the IT team to understand features of the new application due to an inadequate risk assessment related to the implementation of the new application.

Based on its root cause analysis, management determined that Principle 4 of the COSO Framework was not met (see Question 2.4.140). This principle requires the organization to demonstrate a commitment to attract, develop and retain competent individuals in alignment with objectives. Management also determined Principle 7 of the COSO Framework was not met (see Question 2.5.100). This principle requires the organization to identify risks to the achievement of its objectives across the entity and analyze risks as a basis for determining how those risks should be managed.

Example 9.3.20
Control deficiency related to an error in a warranty accrual spreadsheet

Scenario

Internal Audit discovered an error in a spreadsheet used by management to determine the warranty accrual. It was determined that management did not have an adequately designed control around completeness and accuracy of information input in the spreadsheet. Management was relying on the control operator's review of the warranty accrual to also address the completeness and accuracy of the information, rather than designing a control specifically for that purpose.

Root cause analysis

As management performed the root cause analysis, they determined the following.

- The control operator was assuming the information in the spreadsheet was complete and accurate.
- The control operator's review would have been difficult to design in such a way that would allow them to ascertain completeness and accuracy of the information.
- Management did not understand the importance of having separate controls over the completeness and accuracy of information being used in the operation of a control.
- Management's risk assessment process never contemplated risks such as completeness and accuracy of information, even though their process should be designed to identify such risks.

The root cause analysis shows that the control deficiency is more than just a design deficiency in one control related to the warranty accrual. Instead, the deficiency is related to management not having sufficient knowledge of what is required by the COSO Framework, which would indicate Principal 4 of the COSO Framework was not met (see Question 2.4.140) as it relates to information used in ICFR. This further led to an insufficient risk assessment, which would indicate Principle 7 of the COSO Framework was not met (see Question 2.5.100).

Importantly, management should consider whether other controls that rely on information produced by the entity might have a similar deficiency. If so, all deficiencies eventually would be aggregated in the risk assessment ICFR component, by principle, to determine whether a material weakness exists. Without a proper root cause analysis, management may never have associated this deficiency with the risk assessment component and related principles.

Example 9.3.30

Management's root cause analysis leads to sufficient description of control deficiency related to tax contingency accrual

Scenario

The external auditor finds an error in the entity's tax calculation and determines that the deficiency relates to a control designed to identify misstatements in the tax contingency accrual. Specifically, the control that a tax director reviews the quarterly tax contingency calculation.

Analysis

Management's root cause analysis and description of control deficiency

Management determined that the error was caused by the tax director being unaware of a decision senior management made that affected the tax contingency accrual. While the review was operating as designed, it was not designed in such a way that the reviewer had access to critical internal information that may have affected the effectiveness of the review. To remediate the deficiency, management plans to include the tax director in certain quarterly meetings where senior management discusses significant events that may affect key accruals.

As management performed its root cause analysis, it was determined that had the tax director attended the quarterly meeting with senior management in the past, he would have had, and would appear to have in the future, sufficient information to effectively perform his review of the tax contingency accrual.

Other factors were also carefully considered by management in its root cause analysis, including:

- the technical competence of the tax director; and
- the precision of the tax director's review.

Management concluded that the tax director has the technical competence to perform an effective review and that the control was otherwise designed appropriately, had the tax director had the information needed in performing the control.

Management evaluated the design of the controls related to all other significant accruals and estimates and determined that other employees responsible for reviewing significant accruals or estimates already attend the quarterly meeting with senior management. Therefore, management concluded that the design deficiency appeared to be limited to:

- the tax contingency accrual review, because the tax reviewer, by design, did not receive information necessary for his review; and
- the risk assessment process because it did not identify this design deficiency.

Additional root cause analysis is necessary to understand why the risk assessment process did not identify the design flaw in the tax contingency accrual review. The additional root cause analysis should also investigate:

- whether there is a broader deficiency within the risk assessment process, and therefore the risk assessment component of ICFR, because of that process not functioning properly in similar instances; and
- whether there are control deficiencies in the information and communication and/or control environment components of ICFR because of the reviewer not having access to the critical internal information.

Evaluation of control deficiency description

Management provided an appropriate description of the control deficiency because it identifies the control and explains both how it was inappropriately designed and why it did not properly function. In addition, the description provides related information to help management determine whether any other deficiencies should be identified.

Note the difference in the analysis required to determine the root cause of the control deficiency compared to Example 9.2.50. In this example, the evaluator asked probing questions, such as the following, to determine the control that failed, the deficiency related to the control, and the related COSO component:

- Who was involved in the review of the tax provision? Were the right people involved?
- When did the review take place? Was it timely?
- What went wrong with the review?
- Why did it go wrong? Was it technical incompetence, a lack of information, a lack of sufficient time, or something else?
- How detailed was the review? Was it performed at a sufficient level of precision to be effective?
- What are management’s remedial actions?
- How likely it is that similar weaknesses exist in similar controls?

Question 9.3.30

Is it necessary to understand what caused control deficiencies at a service organization upon which the entity relies for its ICFR?

Interpretive response: Yes. Deficiencies in controls at a service organization can still represent a deficiency in the user entity's ICFR. Management considers the control deficiencies identified that are relevant to the entity's ICFR, just like any other control deficiencies originating within the entity itself.

9.4 Step 3: Determine whether the deficiency is indicative of other deficiencies

Question 9.4.10

What actions are taken to determine whether the control deficiency is indicative of other deficiencies?

Interpretive response: To determine whether a control deficiency is indicative of other deficiencies, the following actions can be taken.

Action 1	Consider the information gathered from understanding what caused the deficiency (see section 9.3 for additional information about the information gathered).
Action 2	• Determine whether there are similar or interrelated controls with the same type of deficiency (i.e. commonalities); and/or
	For example: – If the deficiency occurred because of the control operator's lack of knowledge, management considers the effect on other controls for which the same person is responsible. – If there is a breakdown in the process, management considers whether there might be other deficiencies in other process control activities within the same process. – If the deficiencies occurred because of a specific factor (e.g. the timing of the control), management considers the effect on other controls that operated at that time.
Action 3	• Determine whether the control deficiency represents a more pervasive issue in other internal control components (e.g. entity-level).
	– For example, there may be a relationship between a deficiency in the control activity component and the risk assessment component of ICFR. – If the deficiencies occurred because of a change in a process and management did not perform sufficient risk assessment to identify the change and related effect on

	controls, management considers whether there are deficiencies in the entity's risk assessment controls.

Example 9.4.10

Whether a control deficiency for lack of review precision for an estimate is indicative of other deficiencies

Scenario

Internal Audit's control testing indicates that a control over a

key estimate was not designed at a sufficient level of precision. This resulted in a conclusion that there was a deficiency related to the design of the control.

Analysis

Management considers whether similar issues may be present or have been identified in other review controls related to estimates.

Management may also reconsider whether it needs to perform additional testing of the design of similar controls to have sufficient evidence of their operating effectiveness now that a deficiency has been identified in this control.

Example 9.4.20

Whether a control deficiency for lack of review is indicative of other deficiencies

Scenario

A deficiency in the design of internal control is identified because certain key transactions are not required to be reviewed by the appropriate level of management, which may indicate that the risk assessment process was inadequate.

Analysis

Management considers why the risk assessment process did not identify the deficiency in the design of the control and whether there are other ways management's risk assessment process is deficient.

Example 9.4.30
Whether a control deficiency for untimely reconciliation review is indicative of other deficiencies

Scenario

A deficiency in the operating effectiveness of internal control is identified because a control to review certain reconciliations was not performed timely, which may mean that the reviewer did not have the time to perform the review. It may also mean the monitoring process was not sufficient to detect that the control was operating incorrectly.

Analysis

Management considers whether there is a sufficient complement of qualified personnel to perform controls timely, why the monitoring process did not identify the deficiency, and if there are other signs of weakness in either the control environment or monitoring components of ICFR.

9.5 Step 4: Evaluate the severity of the deficiency individually

Question 9.5.10
What are the categories of control deficiencies based on severity?

Interpretive response: A deficiency can be a material weakness, a significant deficiency, or a deficiency. The severity of a control deficiency is a factor of both its potential magnitude and likelihood of resulting in a material misstatement.

Question 9.5.20
What is a material weakness?

Interpretive response: A material weakness is a deficiency, or a combination of deficiencies, in ICFR such that there is a reasonable possibility that a material misstatement of the entity's annual or interim financial statements will not be prevented or detected on a timely basis.

Question 9.5.30

What determines whether a deficiency is a material weakness?

Interpretive response: When evaluating the severity of a deficiency, the deficiency is determined to be a material weakness when:

	Severity: material weakness
Likelihood of potential material misstatement	There is a reasonable possibility (more than a remote possibility) that a misstatement could occur.
Magnitude of the potential misstatement	The potential misstatement[1] is material.

Note:

1. The potential misstatement is considered, not the actual misstatement. In fact, material weaknesses can exist even in the absence of an actual misstatement or when the actual misstatement is not material.

Additionally, there are specific indicators of material weaknesses. If a deficiency is the result of one of these indicators, the deficiency is ordinarily a material weakness. However, the absence of these indicators does not mean the deficiency is not a material weakness.

One indicator of a material weakness per Accounting Standard (AS) 2201.70 is when a deficiency, or combination of deficiencies, 'might prevent prudent officials in the conduct of their own affairs from concluding that they have reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in conformity with US GAAP. When this indicator is present, the deficiency, or combination of deficiencies, is ordinarily a material weakness.

In addition, the SEC staff has provided the following specific indicators of material weaknesses:

- identification of fraud, whether or not material, on the part of senior management;
- restatement of previously issued financial statements for a material misstatement due to fraud or error;
- identification by the auditor of a material misstatement in circumstances that indicate management's ICFR would not have detected the error; or
- ineffective oversight of the entity's financial reporting and ICFR by those charged with governance.

If a deficiency consistent with one of these four indicators is identified, ordinarily the deficiency is a material weakness.

Question 9.5.40

What is a significant deficiency?

Interpretive response: Per AS 2201.A11, 'A significant deficiency is a deficiency, or a combination of deficiencies, in ICFR that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of the entity's financial reporting.'

Question 9.5.50

What determines whether a deficiency is a significant deficiency?

Interpretive response: When evaluating the severity of a deficiency, a significant deficiency exists when:

	Severity: significant deficiency
Likelihood of potential misstatement	There is a reasonable possibility (more than a remote possibility) that a misstatement will occur.
Magnitude of the potential misstatement	The potential misstatement[1] is not material, but significant enough to merit the attention of those charged with governance.

Note:

1. The potential misstatement, not the actual misstatement, is considered. A significant deficiency can exist even in the absence of an actual misstatement.

The following factors may be additional indicators of significant deficiencies, even if the above factors of likelihood and magnitude are not present:

- multiple deficiencies within a COSO principle related to the entity-level controls component of ICFR (see chapter 2);
- an ineffective controls response in areas in which management has identified increased risks of material misstatement (e.g. absence of control activities over such a risk); or
- misstatements detected by the external auditor's procedures that were not prevented, or detected and corrected, by the entity's ICFR.

In addition to these indicators, other matters may be considered when determining whether the deficiency is significant. Those considerations include:

- the importance of the deficiency to the entity's business (e.g. in a key revenue stream, in a metric to the users of the financial statements, related to a recurring issue, etc.);
- the personnel involved in the deficient control;
- if management was aware of the deficiency in ICFR, its actions in response to the issue (e.g. whether the deficiency has been remediated);

- the likelihood that the deficiency may become a material weakness in the future; and
- the nature of the accounting system and the financial statement amounts or transactions exposed to the deficiency, or combination of deficiencies.

Finally, consideration of if the deficiency merits attention of those charged with governance based on the following:

- whether those charged with governance wish to be informed of certain potential misstatements above a specific magnitude (where the magnitude may be lower for certain significant accounts and disclosures and relevant assertions, and/or certain components in a group);
- whether those charged with governance wish to be informed of deficiencies in a specific area; and
- whether those charged with governance wish to be informed if any process has a cumulative number of deficiencies over a certain threshold (e.g. those charged with governance wish to be informed if a process has more than five deficiencies).

The term significant deficiency often leads individuals to believe that a potential error must be very significant to reach this level of deficiency. In fact, a significant deficiency is one that may be just greater than a deficiency, as even though the magnitude of the potential error may be relatively inconsequential, it has characteristics that indicate it is of interest to those charged with governance. Conversely, it may be very close to a material weakness, although determined to not meet such criteria.

Question 9.5.60

How is materiality considered in the evaluation of deficiencies in ICFR?

Interpretive response: The materiality applied to the evaluation of deficiencies in ICFR is the same materiality that is determined and applied during risk assessment procedures (see section 3.3). Materiality includes consideration of both quantitative and qualitative factors.

- Quantitative factors relate to whether misstatements or potential misstatements that would be missed by ICFR, individually or collectively, have a quantitatively material effect on the financial statements.
- Qualitative factors relate to the perceived needs of reasonable persons who will rely on the information.

Question 9.5.70
How is the magnitude of a potential misstatement evaluated?

Interpretive response: In evaluating the magnitude of a potential misstatement, the maximum amount by which an account balance or total of transactions can be overstated is generally the recorded amount, while understatements could be larger.

The minimum amount of the potential misstatement is the misstatement that has occurred, if any. However, in many cases, the magnitude of the potential misstatement can be greater than the amount of any misstatement that actually occurred.

It is the potential misstatement, not the actual misstatement, that drives the severity of a control deficiency. Moreover, a control deficiency can exist even when a misstatement has not occurred.

To evaluate the magnitude of the potential misstatement, management keeps the following in mind.

- Properly identifying the deficiency is key to appropriately evaluating its severity.
- Material weaknesses may exist in the absence of a misstatement.
- Immaterial misstatements can result in a material weakness.
- The actual misstatement is the minimum misstatement that could occur (i.e. the actual error is the ’floor’ for the magnitude of the potential misstatement).
- The maximum amount that an account balance or total of transactions can be understated may be larger than the recorded amount.
- Factors to consider when assessing potential magnitude include:
  - financial statement amounts, or the total of transactions exposed to the deficiency; and
  - volume of activity in the account balance or class of transactions exposed to the deficiency in the current period or that is expected in future periods (see Question 9.5.80).
- The potential magnitude of a misstatement is not limited by the assertion that ‘management has learned its lesson’, ‘reviews are more thoroughly performed when the stakes are higher’, or other such assertions.
- Remedial actions taken in response to the control deficiency after the assessment date do not have an effect on potential magnitude.

Question 9.5.80

In evaluating the potential magnitude, can only the current period activity be considered?

Interpretive response: No. Management needs to evaluate the volume of activity in both the current period and future periods because the potential misstatement may not be material in the current period, but it may become material in the future.

The severity of a deficiency that has the potential of becoming a bigger issue in the future is greater than that of another deficiency whose potential misstatement will never be material. Therefore, assessing the magnitude of the potential misstatement involves projecting what could happen in the future, such as in the following examples.

- If an account balance exposed to a deficient control has gradually increased each period as the entity grew in size, management considers the projected continued growth in that account balance.
- A deficiency has been identified related to insufficient knowledge of international tax accounting at a pharmaceutical entity. In considering the severity of the deficiency, it may be prudent for management to take into consideration their near-term plans for expanding internationally when evaluating the magnitude of the potential misstatement.

In making assessments about a deficiency's magnitude, more weight may be put on past experience with an account that is objective and verifiable, and less weight may be put on considering future projections that are inherently more subjective.

Question 9.5.90

Can various potential misstatements offset each other to determine the severity of the deficiency?

Interpretive response: It depends. When evaluating the magnitude of the potential misstatement, the various potential misstatements may net only in those instances in which the internal control design dictates that failure of a specific process control activity will result in offsetting (in total or in part) potential misstatements in:

- the same financial statement account or disclosure; or
- closely related financial statement accounts or disclosures.

For example, a deficiency in placing construction-in-progress (CIP) fixed assets in service may result in offsetting errors to CIP and other fixed asset types, as well as errors to depreciation expense. When evaluating the severity of this deficiency, it may be appropriate to offset the CIP and fixed asset errors (if it is concluded that the individual fixed asset line-item disclosures are not relevant to users of the financial statements), but not to offset those errors with depreciation expense.

Although revenue and expense 'offset' in the statement of income, it is not appropriate to offset revenue and expenses when evaluating the severity of a deficiency if users of the financial statements consider revenue or any of the other effected financial statement line items to be individually relevant.

Question 9.5.100

Are indirect effects of the potential misstatement considered in evaluating the severity of the deficiency?

Interpretive response: Yes. Indirect effects of a potential misstatement may be relevant when evaluating the magnitude of such potential misstatement.

For example, the level of revenues may affect:

- complying with debt covenants;
- calculating an earn-out on a business combination; or
- attaining a performance-based stock award or bonus program.

Each of these indirect effects could affect the evaluation of the severity of a deficiency involving revenue.

Question 9.5.110

How is the likelihood of a material misstatement considered in evaluating a deficiency?

Interpretive response: The severity of a deficiency depends on both its magnitude and the likelihood (i.e. whether there is at least a reasonable possibility) that the entity's controls will fail to prevent or detect a misstatement of an account balance or disclosure. It does not depend on whether a misstatement actually occurred.

A reasonable possibility exists when the likelihood of an event occurring is either reasonably possible or probable.

Reasonably possible	Probable
The chance of the future event or events occurring is more than remote but less than likely.	The future event or events are likely to occur.

Reasonable possibility is a low threshold.

Risk factors affect whether there is a reasonable possibility that a deficiency, or a combination of deficiencies, will result in a material misstatement of an account balance or disclosure. Risk factors include, but are not limited to:

- the nature of the financial statement accounts, disclosures and assertions involved;
- the susceptibility of the related asset or liability to loss or fraud;

- the subjectivity, complexity or extent of judgment required to determine the amount involved;
- the interaction or relationship of the control with other controls, including whether they are interdependent or redundant;
- the possible future consequences of the deficiency; and
- the cause and frequency of exceptions detected as a result of the deficiencies.

Example 9.5.10

Evaluating the severity of a deficiency related to legal accruals

Scenario

An entity overstates a legal accrual by $2 million. The control deficiency identified relates to control design – specifically, the control was not designed to have the legal department inform the finance department of all developments surrounding legal matters.

The legal department has a practice of immediately communicating negative developments and discussing the ramifications of those developments on the legal accrual. In this case, because the development was positive (the case was dismissed), the legal department thought it was being 'conservative'.

The entity has several legal matters outstanding with a total legal accrual of $15 million.

Analysis

The 'floor' of the potential magnitude is the actual $2 million overstatement. For illustration purposes only, the potential magnitude, or 'ceiling', for overstatements will be evaluated. In practice, both the possibilities of overstatements and understatements is considered.

Evaluating the severity of the deficiency likely would include the potential for overstatement of the legal accrual related to all legal matters, not just the legal matter that led to the error. Judgment is used to determine whether there is sufficient evidence to suggest that the likely potential magnitude is less than the absolute maximum error – in this case, the overstatement of all legal accruals.

An overstatement of the entire legal accrual would be $15 million. But of the $15 million accrued, $11 million relates to legal matters that are close to settlement and, in fact, the entity has made offers to the plaintiffs equal to the $11 million. The entity has a demonstrable history that, once making a settlement offer to the plaintiff, the payouts approximate the settlement offers. The ratio of matters close to settlement ($11 million) compared to those not close to settlement ($4 million) is typical for the entity. The $4 million accrual for those matters not close to settlement, which includes $2 million of the actual misstatement, is management's best estimate of probable loss, but the matters are not close to being resolved and no settlement offers have been made.

Based on the evaluation of this scenario, the likely potential magnitude may be closer to $4 million than $15 million.

Example 9.5.20
Evaluating the severity of a deficiency related to a warranty accrual

Scenario

An entity understates its warranty accrual by $1 million. The error was a result of inaccurate underlying warranty claim data used by management in its calculation and review of the warranty accrual balance.

An accounting clerk generated a report of underlying warranty claim data from the entity's ERP system into an editable spreadsheet and recorded manual adjustments to present the claim data in the format necessary to calculate the required warranty accrual. The accounting clerk made an error in his manual adjustments to the spreadsheet, which resulted in the understatement of the warranty accrual.

The controller reviews the warranty accrual for appropriateness and relies on the same underlying warranty claim data in the spreadsheet prepared by the accounting clerk to perform the review. As a result of the error in the spreadsheet, the controller's review did not detect the understatement in the accrual.

Management performed a root cause analysis and determined that the deficiency was related to a missing control over end-user computing in the editable spreadsheet. Management concluded that the review control over the warranty accrual would have operated appropriately if the controller had been provided accurate underlying claim data. Management also determined that:

- no other judgmental accruals rely on underlying data that is manually modified after being extracted from the ERP system; and
- controls over the ERP underlying warranty claim data report and relevant GITCs were designed and operating effectively.

The warranty accrual, after correction for the $1 million understatement, was $20 million at period end. The warranty accrual has fluctuated between $15 million and $20 million over the last three years but has gradually increased as the entity has grown and sales have increased and is expected to continue with similar growth prospectively.

Analysis

The 'floor' of the deficiency's potential magnitude is the actual misstatement of $1 million. The potential magnitude, or 'ceiling', is more difficult to evaluate in this circumstance because of:

- the understatement risk associated with the warranty accrual; and
- the nature of the deficiency potentially resulting in either an overstatement or understatement of the balance.

Because of the understatement risk, the potential magnitude is not necessarily limited by the balance of the warranty accrual. Determining the potential magnitude will require judgment but is almost certainly an amount greater than the $1 million actual misstatement in this case.

Assessing the potential magnitude should also consider the fact that the warranty accrual has increased in recent years and is expected to continue that trend in the future. As a result, the potential magnitude of the deficiency may be higher due to that expected growth than if it was assessed strictly based on the current account balance.

Assessing likelihood in this scenario also requires judgment. The controller's review over the warranty accrual was otherwise designed and operating effectively, apart from the completeness and accuracy of the underlying data. Because of this, it is reasonable to expect that as the size of the misstatement increases, the controller would have eventually detected the error irrespective of the issues in the underlying claim data.

Consideration is given to the dollar threshold (magnitude of the error) at which it becomes remote that an error would not be identified through the controller's review, despite the deficient controls over the underlying data. For example, it may be unreasonable that the balance would ever be below $15 million, since business is growing and there may be a reasonable ceiling that could be determined based on the level of growth.

Example 9.5.30

Evaluating a deficiency involving insufficient resources in the accounting and financial reporting departments

Scenario

A mid-size entity executes on its strategic initiative to grow rapidly through targeted acquisitions of companies in its direct and related industries. Over a period of three years, the entity triples in size as measured by revenues, while expanding into new geographic markets and product lines.

The rapid growth in the business places significant stress on the entity's accounting and financial reporting departments, which were not staffed with sufficient resources, both in terms of quantity and relevant expertise. The pressure on the entity's accounting and financial reporting departments resulted in delays in the monthly close process and other indicators of deficiencies in the entity's ICFR.

The entity's CEO and CFO, while aware of the stress put on the accounting and financial reporting departments, determined that the deficiency – due to its lack of sufficient and appropriate resources – did not rise to the level of a material weakness when performing the annual assessment of ICFR. This conclusion was reached, in part, based on the absence of any actual identified misstatements in the entity's financial statements during this period.

Subsequently, material errors in the entity's financial statements were identified related to more complex and judgmental areas of the financial statements. Upon completion of its root cause analysis, management determined the errors resulted from a lack of sufficient, qualified personnel to design and manage an effective control environment. The entity restated its prior year financial statements because of the errors.

Analysis

In the situation above, management assessed the severity of the deficiency related to its lack of sufficient and qualified personnel as of its assessment date and concluded that it did not represent a material weakness. In doing so, management considered the lack of identified misstatements in the financial statements as evidence supporting the potential magnitude of the deficiency not being material.

However, the absence of a misstatement to the financial statements doesn't prevent the deficiency from being a material weakness. Assessing potential magnitude involves projecting what *could* happen in the future if a control deficiency results in a misstatement remaining undetected.

In this scenario, management did not appropriately apply the deficiency evaluation guidance contained in the SEC's 2007 Management Guidance[7] because it evaluated the magnitude of the control deficiency based primarily on the absence of a misstatement to the financial statements. As a result, management failed to fulfill its obligations under SEC Rule 13a-15(c).

Example 9.5.40

Evaluating the severity of a deficiency with cumulative effects involving the calculation of amortization

Scenario

An entity makes an error in its calculation of amortization resulting in an error of $1 million each year over 20 years. On a cumulative basis, the largest the error will be on the balance sheet is $10 million in year ten ($1 million a year over ten years that then begins to reverse in the following years).

The control to review the calculation of the amortization is not designed effectively as it relies on the original setup of the asset, which was done incorrectly. It was determined that $1 million is not material to the entity's income statement, but $10 million is over calculated materiality.

[7] 17 CFR Part 241 (Release No. 33-8810), Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934.

Analysis

Initially this deficiency would appear to be a material weakness, as the cumulative error that could occur is material if discovered and corrected in year ten. However, other than the actual correction of the error in year ten, there is no period that is materially misstated, and there is not a reasonable possibility of material misstatement in any given year. Based on a quantitative and qualitative analysis, the entity may be able to conclude the error is not material and avail itself of an immaterial error correction. In evaluating the related ICFR effect, the entity may also be able to conclude that the control deficiency is not a material weakness. Both qualitative and quantitative considerations are of increased importance in situations such as this one.

Question 9.5.120

Are there incremental considerations when evaluating GITC deficiencies?

Interpretive response: Yes. Evaluation of the severity of GITC deficiencies is similar to the evaluation of the severity of other control deficiencies. However, with GITC deficiencies management also needs to think about:

- how the deficiency effects the related automated or manual control activities that rely on information from the affected systems (see Question 9.5.130); and
- several additional factors that could affect whether there is a reasonable possibility that the GITC deficiency will lead to a material misstatement (see Question 9.5.140).

Question 9.5.130

How does management consider control activities that rely on a deficient GITC?

Interpretive response: In identifying GITC deficiencies, management considers the control activities that rely on the deficient GITCs. This helps to identify:

- whether there are potential automated control activity deficiencies; and/or
- whether the GITC deficiencies effect the integrity of any manual control activities that use information from the effected systems.

As GITCs support the operating effectiveness of automated controls and information used in manual controls that come from the effected system, management needs to identify the automated and manual control activities effected by the GITC deficiency. Although a control dependent on a deficient GITC would not be operating effectively, management would still test the design and implementation of any effected controls. If the design and implementation are not determined to be appropriate, that would be considered a separate deficiency.

When there are no compensating GITCs, including ad-hoc controls that address the same risk arising from IT (RAFIT) as the deficient GITC, the control activities are also considered deficient.

The severity of a GITC deficiency is consistent with the evaluation of the combined severity of the associated process control activity deficiencies that are adversely affected by the GITC deficiency. For example, when the associated process control activity deficiencies are determined to be a significant deficiency, the GITC deficiency is likely also a significant deficiency.

Question 9.5.140

What other factors are considered in evaluating whether there is a reasonable possibility that a GITC deficiency will lead to a misstatement?

Interpretive response: Management thinks about the following additional factors to help evaluate whether there is a reasonable possibility that the GITC deficiency will lead to a material misstatement. These factors are considered because purely quantitative methods are not necessarily helpful in evaluating GITC deficiencies in all circumstances.

Factor	Guidance and helpful questions
Nature and significance of the deficiency	• What is the nature of the deficiency and how significant could it be? • For example, does the deficiency relate to a single area in the program change process, or is the entire process inadequately controlled?
Pervasiveness of the deficiency to control activities and underlying data	• The more pervasive the GITC is, the more likely it is that the GITC deficiency will contribute to a misstatement in the financial statements that could be material. • How many automated control activities rely on the GITC that is deficient? • How many automated control activities are deficient that are related to or caused by the GITC deficiency? • Does the GITC deficiency affect integrity of information used in manual controls?
Possible future consequences of the deficiency	• Do not only consider the severity of the current period deficiencies in the automated control activities and control activities related to integrity of information that are related to or caused by the GITC deficiency but also consider the automated control activities linked to the GITC. By doing this, management determines the possible future implications of the GITC deficiency, including the possibility that the automated control activities and control activities related to the integrity of

Factor	Guidance and helpful questions
	information linked to the GITC will not operate effectively because of that deficiency.
Complexity	• How complex are the entity's systems and how does the complexity affect the likelihood that the GITC deficiency could adversely affect control activities?
Proximity of the GITC to control activities and data	• How close is the deficient GITC to relevant control activities and data? • From the four IT layers – application, database, operating system and network – the application layer is the 'closest' in proximity to the control activities and data. The network layer is the 'furthest' from the control activities and data. • Deficiencies in the operating system layer are less likely to have a direct effect on control activities because there may be other compensating controls at the application and database layers. However, deficiencies in the application and database layers are more likely to have a direct effect on the control activities, which will increase the likelihood that a material misstatement could occur.
Susceptibility to loss or fraud	• Does the GITC deficiency relate to control activities or data associated with significant accounts or disclosures that are susceptible to loss or fraud?

Question 9.5.150

Are there incremental considerations when evaluating entity-level control deficiencies?

Interpretive response: Yes. The severity of deficiencies in entity-level controls is determined by evaluating the likelihood and magnitude of the potential misstatement, as with any other deficiency. However, the magnitude of a potential misstatement usually cannot be evaluated directly because deficiencies in entity-level controls usually do not prevent or detect assertion-level risks of material misstatements.

Purely quantitative methods to determine the magnitude of the potential misstatements are not necessarily helpful in evaluating deficiencies in entity-level controls because of their pervasiveness. As such, management needs to evaluate likelihood and magnitude by thinking about other factors. The following table includes factors designed to determine whether there is a reasonable possibility (likelihood) that a deficiency in an entity-level control would contribute to circumstances that could result in a misstatement and, if so, the magnitude of the potential misstatement (magnitude).

Factor	Guidance and helpful questions
Pervasiveness of the deficiency across the entity	• How pervasive is the deficiency across the entity? • The more pervasive the entity-level control, the more likely it is that the deficiency will contribute to a misstatement in the financial statements that could be material.
Relative significance	• What is the nature of the deficiency and how significant is it? • What is the relative significance of the deficient control to the COSO principle? • Why is the control important to the entity's ICFR?
Specific control activities affected	• Are there specific control activities affected by the deficiency in the entity-level control? • How many control activities affected by the entity-level control are deficient?
Potential impact and severity of control activities affected by the deficient entity-level control, in the aggregate	• If there are specific control activities affected by the deficient entity-level control, evaluate the reasonable possibility that those control activities will fail to prevent or detect a misstatement of an account balance or disclosure and, if so, the likelihood and magnitude of potential misstatements. • Depending on the pervasiveness of the entity-level control deficiency, a quantitative analysis may not be possible.
Possible future consequences of the deficiency	• What would be the effect if all control activities affected by the entity-level control deficiency fail? • Do not only consider the severity of the current period deficiencies in the control activities affected by the deficient entity-level control, but also consider all control activities affected by the entity-level control. By doing this, management determines the possible future implications of the entity-level control deficiency, including the possibility that all the control activities affected by the entity-level control will not operate effectively because of that deficiency.
Cause and frequency of known or detected deviations in the entity-level control	• What is the cause and frequency of known deviations in the operating effectiveness of the entity-level control?
Susceptibility to loss or fraud (including management override of controls)	• Does the deficiency in the entity-level control affect control activities associated with significant accounts or disclosures that are susceptible to loss or fraud (including management override of controls)?

Example 9.5.50
Entity-level control deficiencies

The scenarios in the following table illustrate management's consideration of the pervasiveness of entity-level control deficiencies and whether a material weakness may exist (i.e. whether there is a reasonable possibility that the entity's control activities will fail to prevent or detect a material misstatement).

Scenario	Analysis
A deficiency is identified in Principle 1 of COSO, which is: The organization demonstrates a commitment to integrity and ethical values (see Question 2.4.60). Specifically, management does not routinely enforce consequences for deviating from the entity's code of conduct. This control is important to ICFR because, without consequences, personnel may not have an incentive to act ethically while performing their duties.	Because of the pervasive nature of this control across the entire entity, management may conclude this entity-level control deficiency is a material weakness.
A deficiency is identified in Principle 4 of COSO, which is: The organization demonstrates a commitment to attract, develop and retain competent individuals in alignment with objectives (see Question 2.4.140). Specifically, the entity has a specific pre-screening process where the HR director assesses the competence of potential new hire candidates. During the year, the HR director left the entity, and the entity hired a new controller without following the pre-screening processes and related controls.	The potential effect of this deficiency is pervasive because the controller has oversight and influence over many control activities. Therefore, management may conclude this entity-level control deficiency is a material weakness.
This scenario is a continuation of the previous scenario. The CFO performed the following additional steps as part of hiring the new controller: • reviewed resumes to determine whether the candidate's background was consistent with the job description; • interviewed candidates and assessed competence through questions targeted to the candidate's experience; and • confirmed references before approving the hire.	In this scenario, the additional steps performed by the CFO may reduce the severity of the control deficiency created by the HR director's departure and lack of pre-screening performed on candidates. After considering all relevant facts and circumstances, management may conclude that this deficiency is not a material weakness.

Question 9.5.160
Are deficiencies at service organizations evaluated differently from other deficiencies?

Interpretive response: No. If the deficient control at a service organization is a control the entity relies upon for its ICFR, its severity is assessed by evaluating the likelihood and magnitude of the potential misstatement, as with any other deficiency. It is generally more significant if a control objective has not been achieved versus a deficiency in an individual control that supports a control objective (see Question 8.9.20).

Service organizations often process large volumes of transactions, such as payroll, and use automated control activities to mitigate related risks. In situations where deficiencies relate to GITCs, it is important to consider the pervasive nature of those controls and which control activities the entity relies on.

Often the service organization's SOC 1 report will provide information to help management understand the effect of deficiencies at the service organization. Because an entity may only rely on the service organization for some, but not all, services offered by the service organization, the lack of a material weakness at the service organization may not be conclusive for management's purposes. Management needs to evaluate how the deficiency at the service organization effects the service organization's controls that the entity is relying on for its ICFR.

See section 8.9 for further information on deficiencies at service organizations.

9.6 Step 5: Evaluate the effect of compensating controls and conclude on the severity of the individual control deficiency

Question 9.6.10
What are compensating controls?

Interpretive response: Compensating controls are controls that address:

- the same objective (e.g. PRP(s), RAFIT(s)) as a deficient control at the appropriate level of precision; and
- the same period of time that the control is deficient, which does not end until the deficient control is remediated.

Compensating controls may be:

- different controls that were already in place and operating throughout the period and cover the same objective as the deficient control (i.e. redundant or duplicative controls); or
- 'ad hoc' controls management put in place on a timely basis to respond to the identified deficiency and determine whether the deficiency caused a material misstatement during the period.

For example, management identifies a deficiency in the access termination control (e.g. an untimely removal of access at the time of termination) during the monthly access review by the CIO. Immediately after identification of the inappropriate system access, the access was removed and management performed their own procedures ('ad hoc') and determined that the person(s) who had inappropriate access did not, in fact, use that access. The monthly review control, and additional 'ad hoc' procedures to determine that no access occurred, serve as a compensating control for the deficient access termination control.

An 'ad hoc' control should be part of management's control process to be considered a compensating control and not a control designed at the external auditor's request or to support the external audit.

Question 9.6.20

How are compensating controls identified?

Interpretive response: Management may identify compensating controls by looking to other controls at the entity that are capable of achieving the same objective as the deficient control. In addition, for process control activities, the control looked to by management must be capable of achieving the appropriate level of precision.

Question 9.6.30

When can compensating controls be used to mitigate a deficiency in a process control activity?

Interpretive response: For a compensating control to effectively mitigate a deficiency in a process control activity, the compensating control must be designed to operate at a level of precision that would prevent, or detect and correct on a timely basis, a material misstatement. Effective compensating controls address the same PRP(s) as the deficient control(s) and cover the period of time the control(s) was deficient.

To limit the severity of a deficiency, it is not necessary for a compensating control to be as precise as the deficient process control activity, if it:

- achieves the same control objective as the deficient control; and
- operates at a level of precision that would prevent, or detect and correct on a timely basis, a material misstatement.

Compensating controls cannot lower the potential misstatement below the actual known misstatement, or the 'floor', for purposes of evaluating the severity of a deficiency.

Example 9.6.10

Whether final review of the financial statements by the CFO and others may be a compensating control

Scenario

The following controls are evaluated to determine whether they adequately compensate for a deficient control:

- a final review of the financial statements by the CFO; and
- a final review of the financial statements by the CEO and Audit Committee.

Analysis

The evaluator considered whether the CFO's review was performed at a level sufficiently precise to be able to detect a material misstatement at the 'would' level (see Question 5.3.20). The CFO's review of the financial statements was a control identified and tested by management. However, testing the control showed the CFO's review lacked the precision necessary to detect material misstatements to the account affected by the identified deficiency because the review was not performed:

- at a disaggregated level; or
- with an expectation of what the account balance should be.

The CFO review control functioned as a monitoring control, or as more of an operational review for purposes of evaluating the propriety of management discussion and analysis (MD&A), rather than a control activity designed to detect material misstatements.

The evaluator then considered if the final reviews by the CEO and the Audit Committee might be considered appropriate compensating controls. However, these controls also were not operating at a sufficient level of precision for similar reasons.

Therefore, neither the final reviews performed by the CFO, nor the CEO and Audit Committee are compensating controls that can reduce the severity of the identified deficiency.

Example 9.6.20

Evaluating the existence of compensating controls for deficient GITCs over a revenue application

Scenario

A deficiency in GITCs over the revenue application is identified such that reliance on any of the application controls related to the existence, completeness and accuracy of revenue is not appropriate. The only manual controls the entity has over revenue include:

- a revenue subledger to general ledger reconciliation;
- a reconciliation of cash receipts to the Accounts Receivable (A/R) subledger; and
- a management review control where the CFO reviews the financial statements for existence, completeness and accuracy of revenue.

Analysis

Neither the subledger to general ledger reconciliation or the reconciliation of cash receipts to the A/R subledger provide any evidence over the existence, completeness and accuracy of revenue recorded in the subledger. Therefore, these controls do not meet the same objectives as the deficient revenue application controls.

The CFO's review of the financial statements may meet some of the same objectives as the deficient revenue application controls, but it is unlikely this review control provides sufficient evidence at an appropriate level of precision. Further, the CFO's review may not be designed to meet all the same objectives as the revenue application controls, including fraud risks.

Because the manual controls are not sufficient compensating controls, it would be necessary for management to evaluate the severity of the GITC deficiencies by considering the potential magnitude of all controls affected by the GITC deficiencies in the aggregate.

Example 9.6.30

Compensating control related to provisioning of access

Scenario

Management identifies a few exceptions in the control over provisioning of access. However, management also has a detective access control that involves a quarterly review of access. Part of this quarterly review includes determining whether anyone who had inappropriate access inappropriately used that access.

Analysis

Management determines the detective access control addresses the same RAFIT for the same period as the control over provisioning of access. As a result, the detective access control is likely to be an effective compensating control.

Example 9.6.40
Compensating control related to bank reconciliations

Scenario

Small errors are identified in the bank reconciliation control, and it is determined that the control is deficient. However, management also has a review control that involves management reviewing the bank reconciliations using specified metrics and thresholds.

Analysis

All the errors discovered in the bank reconciliation control were either less than the specified metrics of management's review control or identified in management's review. In addition, management determines that its design, including the precision with which it operates, is appropriate to detect or prevent a material misstatement. As a result, the review control is likely to be an effective compensating control.

Question 9.6.40
Can a compensating control eliminate a control deficiency?

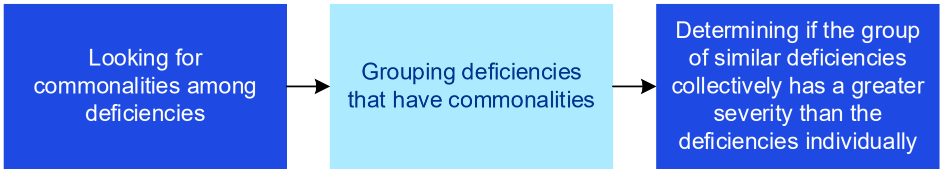
Interpretive response: No. A compensating control might limit the severity of a deficiency and prevent it from being a significant deficiency or material weakness but does not eliminate the deficiency. The presence of a compensating control does not change the fact that a deficiency exists in the original control.

9.7 Step 6: Evaluate the severity of similar deficiencies in the aggregate

Question 9.7.10
When are individual deficiencies aggregated?

Interpretive response: After individual deficiencies are evaluated for severity, management considers whether individual deficiencies with certain commonalities (see Question 9.7.20), in combination, result in a material weakness or significant deficiency. The requirement to aggregate deficiencies was established to evaluate the 'big picture' as it relates to deficiencies.

The severity of similar deficiencies can be evaluated in the aggregate by:



Looking for commonalities among deficiencies → Grouping deficiencies that have commonalities → Determining if the group of similar deficiencies collectively has a greater severity than the deficiencies individually

As part of this process, consideration should be given to any compensating controls (see Question 9.6.10) that operate at a level of precision that would prevent or detect a misstatement that could be material.

Question 9.7.20

What are commonalities among deficiencies?

Interpretive response: Management aggregates deficiencies if they have a characteristic in common that could lead to similar or larger types of misstatements. The typical commonalities evaluated for aggregation include those involving the same:

- account/disclosure;
- relevant assertion; and
- ICFR component and principle(s).

Other relevant commonalities evaluated for aggregation include those involving the same:

- control type;
- anti-fraud controls;
- IT layer/RAFIT addressed by GITC controls;
- locations; and
- control operators or roles.

As noted in Step 2 (see section 9.3), it is important to perform a sufficient root cause analysis in determining exactly what caused a deficiency. An appropriate root cause analysis and description of the deficiency assists in performing an appropriate aggregation assessment.

The aggregation exercise is only as good as the root cause analysis, and only as good as the ability to analyze the 'big picture' of all related deficiencies.

Example 9.7.10

Aggregating deficiencies related to management's risk assessment process

Scenario

This example is a continuation of Example 9.3.20, which involved a scenario where errors were discovered in a spreadsheet. The root cause analysis concludes that management's risk assessment process, specifically Principle 7 of the COSO Framework (see Question 2.5.100), was deficient.

To the extent that the deficiency identified in Example 9.3.20 was the only deficiency noted related to Principle 7 and management's risk assessment process, the effect of that deficiency would be limited to that one control. However, management identifies other deficiencies that also have a root cause in a deficient risk assessment process, albeit a different principle.

Analysis

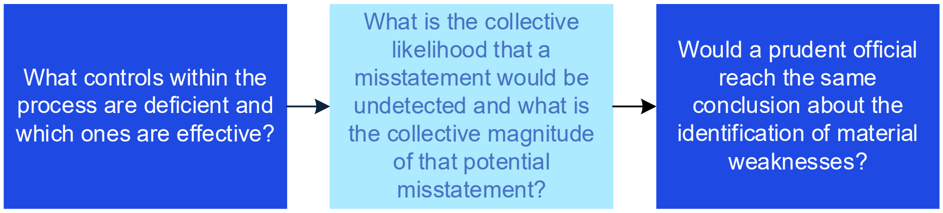
Management would likely aggregate the effect of the individual risk assessment process deficiencies to determine if the lack of an appropriate risk assessment process could have caused a material misstatement. This is the case even though all the deficiencies do not involve the same principle.

After aggregating the potential magnitude of each individual risk assessment process deficiency, management determines whether there is a reasonable possibility that they could have caused a material misstatement in the aggregate.

Question 9.7.30

How is a group of similar deficiencies evaluated to determine if they have greater severity in the aggregate?

Interpretive response: When evaluating the severity of a group of deficiencies in the aggregate, management should consider the following 'big picture' questions.



What controls within the process are deficient and which ones are effective? → What is the collective likelihood that a misstatement would be undetected and what is the collective magnitude of that potential misstatement? → Would a prudent official reach the same conclusion about the identification of material weaknesses?

Considering these questions helps management to 'not lose the forest for the trees' – not to be so focused on the details of a situation that they miss the big picture. When many individually insignificant deficiencies are identified that relate to the same account, assertion, location, person or other commonality, it may mean that there is a bigger problem – an aggregated deficiency with greater severity than the individual deficiencies.

Example 9.7.20

Evaluating the potential magnitude of a group of individual deficiency/es in the aggregate

Scenario

A root cause analysis reveals three deficiencies with the potential to affect the income tax account, plus two additional deficiencies that relate to the information and communications component of the COSO Framework, specifically Principle 13 (see Question 2.6.40). None of the deficiencies were individually considered a material weakness. Also, no compensating controls were identified for any of the deficiencies.

Analysis

Management evaluates the potential magnitude of the aggregated effect of the three income tax deficiencies.

- Each one was determined to be approximately half of what management considers a material error.
- None of the deficiencies would qualify to offset the others – all three deficiencies could happen in the same quarter, and all could be a debit or a credit to the income tax account.

When the three deficiencies are aggregated, the potential magnitude exceeds materiality. Therefore, management concludes a material weakness exists.

Next, management evaluates the potential magnitude of the two deficiencies related to the information and communication component of the COSO Framework. The potential magnitude of each deficiency was determined to be approximately 25% of what management would consider to be material. Management concludes that aggregating the deficiencies within the information and communication component does not rise to the level of a material weakness, and that a prudent official would reach the same conclusion. However, management also concludes that those responsible for oversight of the entity's financial reporting process should be informed about the aggregated deficiencies, resulting in their categorization as a significant deficiency in the aggregate.

9.8 Other considerations

Question 9.8.10
What is management's responsibility in communicating deficiencies?

Interpretive response: For SEC registrants, management has an obligation pursuant to Section 302 of the Sarbanes-Oxley Act to communicate to the external auditor and the audit committee significant deficiencies and material weaknesses on a quarterly basis.

In addition, management should communicate all deficiencies in ICFR identified as part of management's evaluation process over the course of that process to the external auditors. This communication can be made in several different forms. In most circumstances, management's documentation of its assessment would be sufficient for communicating all deficiencies to external auditors and a separate documentation package is not necessary.

Question 9.8.20
What must be included in management's annual report on ICFR?

Interpretive response: Management's annual report on ICFR must state or disclose the following in item 9A, Disclosure Controls and Procedures (DCP).

- Management's responsibility for establishing and maintaining adequate ICFR for the entity.
- Management's criteria for evaluating the effectiveness of ICFR.
- Management's assessment of the effectiveness of the entity's ICFR at year end, including a statement saying whether or not ICFR is effective (see Question 9.8.30).
- Any material weaknesses in the entity's ICFR identified by management, with consideration given to describing:
  - the nature of the material weakness;
  - the effect of the material weakness on the entity's financial reporting and ICFR, if any; and
  - the current plans, or actions already undertaken, if any, to remediate the material weakness.
- The fact that the entity's independent public accountant, who audited the financial statements included in the annual report, has issued an attestation report on the entity's ICFR (if applicable).

See Example 9.8.10 for Item 9A disclosure considerations regarding material weakness.

Question 9.8.30

What should management consider in deciding whether its ICFR is effective or not effective?

Interpretive response: Management must decide if its ICFR is effective or not effective. The following should be considered in making this decision:

- Management cannot conclude that its ICFR is effective if there are one or more material weaknesses.
- Management cannot qualify its conclusion by stating that its ICFR is effective with certain qualifications or exceptions.
- Management may state that its controls are ineffective for specific reasons.

Question 9.8.40

Does ineffective ICFR lead to a conclusion that an entity's DCP are ineffective?

Interpretive response: Yes. Per the SEC Division of Corporate Finance Financial Reporting Manual Section 4310.9, 'Because of the substantial overlap between ICFR and DCP, if management concludes that ICFR is ineffective, it must also consider the effect of the material weakness on its conclusions related to DCP.' This has been interpreted to mean that DCP is also ineffective when ICFR is ineffective.

This would be included in the company's 9A disclosure. See the following example:

Example 9.8.10
Item 9A material weakness disclosure considerations

The following table includes example paragraphs for Item 9A material weakness disclosures within a company's annual 10-K report, the source of the requirements and additional implementation guidance. This example is structured to walk through the following components of the disclosure:

- Evaluation of Disclosure Controls and Procedures
- Management's Report on Internal Control Over Financial Reporting
- Management's Remediation Plan

Item 9A Example paragraph	Source of requirements	Tips and guidance
EVALUATION OF DISCLOSURE CONTROLS AND PROCEDURES		
Our Chief Executive Officer, Chief Financial Officer and Chief Accounting Officer (certifying officers) have conducted an evaluation of the effectiveness of the design and operation of our disclosure controls and procedures (as defined in Rules 13a-15(e) and 15d-15(e) under the Securities Exchange Act of 1934, as amended (the Exchange Act)) as of December 31, 20XX. Our certifying officers concluded that, as a result of the material weakness in internal control over financial reporting as described below, our disclosure controls and procedures were not effective as of December 31, 20XX.	**S-K 307** – Disclose the conclusions of the registrant's principal executive and principal financial officers, or persons performing similar functions, regarding the effectiveness of the registrant's disclosure controls and procedures (as defined in § 240.13a-15(e) or § 240.15d-15(e) of this chapter) as of the end of the period covered by the report, based on the evaluation of these controls and procedures required by paragraph (b) of § 240.13a-15 or § 240.15d-15 of this chapter. **SEC Financial Reporting Manual (FRM) 4310.9** – Because of the substantial overlap between ICFR and DCP, if management concludes that ICFR is ineffective, it must also consider the impact of the material weakness on its conclusions related to DCP.	A paragraph satisfying the requirements noted must be included under this section of the 9A certification. Note the following about this paragraph. • It indicates where DCP is defined in the regulations and what DCP is designed to accomplish. • It includes a description of who was involved in the evaluation of DCP (which should always include the CEO and CFO). • If there is a material weakness in ICFR, it is expected to indicate that the entity's DCP were not effective. • It should not include caveats related to the conclusion about DCP, such as 'except for the identified material weakness, disclosure controls and procedures are effective'. DCP either 'is' or 'is not' effective.

Item 9A Example paragraph	Source of requirements	Tips and guidance
Per Rules 13a-15(e) and 15d-15(e), the term disclosure controls and procedures means controls and other procedures of an issuer that are designed to ensure that information required to be disclosed by the issuer in the reports that it files or submits under the Exchange Act (15 U.S.C. 78a et seq.) is recorded, processed, summarized, and reported within the time periods specified in the SEC's rules and forms. Disclosure controls and procedures include, without limitation, controls and procedures designed to ensure that information required to be disclosed by an issuer in the reports that it files or submits under the Exchange Act is accumulated and communicated to the issuer's management, including its Chief Executive Officer and Chief Financial Officer, or persons performing similar functions, as appropriate to allow timely decisions regarding required disclosure.	N/A	While this paragraph is not required, it is very common for management to include a similar paragraph in DCP.
Our management, including our Chief Executive Officer and Chief Financial Officer, does not expect that our disclosure controls and procedures or our internal control over financial reporting will prevent all errors and all fraud due to inherent limitations of internal controls. Because of such limitations, there is a risk that material misstatements will not be prevented or detected on a timely basis by internal control over financial reporting. However, these inherent limitations are known features of the financial reporting process. Therefore, it is possible to design into the process safeguards to reduce, though not eliminate, this risk.	N/A	While management is not required to include this paragraph, they *may* include a similar paragraph discussing the inherent limitations of DCP and/or ICFR. Care should be taken by management to not be too broad in indicating the inherent limitations of internal controls. This paragraph may be included in its own section (although not frequently done) in Item 9A called 'Inherent Limitations of Internal Controls'.

Item 9A Example paragraph	Source of requirements	Tips and guidance
In light of the material weakness described below, management performed additional analysis and other procedures to ensure that our consolidated financial statements were prepared in accordance with US GAAP. Accordingly, management believes that the consolidated financial statements included in this Annual Report on Form 10-K fairly present, in all material respects, our financial position, results of operations, and cash flows as of and for the periods presented, in accordance with US GAAP.	N/A	While this paragraph is not required, many entities include a paragraph to this effect when there is a material weakness. This paragraph should not be included in Item 9A 'Management's report on internal control over financial reporting'.
MANAGEMENT'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING[1]		
Management is responsible for establishing and maintaining adequate internal control over financial reporting (as defined in Rules 13a-15(f) and 15d-15(f) of the Exchange Act). The Company's management, with participation of the Chief Executive Officer and Chief Financial Officer, under the oversight of our Board of Directors, evaluated the effectiveness of the Company's internal control over financial reporting as of December 31, 20XX using the framework in Internal Control – Integrated Framework (2013), issued by the Committee of Sponsoring Organizations of the Treadway Commission. Based on that evaluation, management concluded that the Company's internal control over financial reporting was not effective as of December 31, 20XX due to the material weakness in internal control over financial reporting, described below.	**S-K 308(a)** – Provide a report of management on the registrant's internal control over financial reporting (as defined in § 240.13a-15(e) or § 240.15d-15(e) of this chapter) that contains: • **S-K 308(a)(1)** – A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the registrant. • **S-K 308(a)(2)** – A statement identifying the framework used by management to evaluate the effectiveness of the registrant's internal control over financial reporting.	A paragraph satisfying the requirements noted must be included under this section of the 9A certification. Note the following about this paragraph: • It typically includes reference to Rules 13a-15(f) and 15d-15(f) of the Exchange Act. • It or another paragraph must identify the framework used to evaluate ICFR, which in most cases is the COSO Framework. • While it is not required to include 'Under the oversight of our Board of Directors', Principles 2 and 17 of the COSO Framework in particular acknowledge that the Board of Directors is supposed to be involved and including such language in the paragraph indicates the fulfilment of that responsibility.

Item 9A Example paragraph	Source of requirements	Tips and guidance
A company's internal control over financial reporting includes those policies and procedures that: (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements.	N/A	While this paragraph is not required, management may find it helpful to include. If included, the language should be consistent (generally verbatim) with the definition of ICFR in AS 2201, so it is consistent with the auditors' report.
Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.	N/A	While this paragraph is not required, management may find it helpful to include. If included, the language should be consistent (generally verbatim) with the language in AS 2201, so it is consistent with the auditors' report.
A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of our annual or	N/A	While this paragraph is not required, it is generally helpful to define a material weakness in the Item 9A certification when there is a material weakness. Defining a material weakness can be done either

Item 9A Example paragraph	Source of requirements	Tips and guidance
interim financial statements will not be prevented or detected on a timely basis.		before the paragraph discussing the actual control deficiencies (see the next paragraph in this example) or after that paragraph. Either is acceptable because placement is not an important consideration in the appropriateness of management's report on internal control over financial reporting.
Based on this evaluation, our certifying officers concluded that the Company did not have a sufficient number of trained resources with expertise in technical accounting, internal control over financial reporting, and the design and implementation of information technology solutions. As a result, we were unable to maintain effective risk assessment and information and communication processes, placed excess reliance on third-party consultants, and did not have effective process-level control activities over the following areas: • property, plant, and equipment and depreciation expense • purchasing (current liabilities and operating expenses) • treasury (cash, debt, interest expense, derivatives, and benefit obligations) The control deficiencies resulted in immaterial misstatements to revenue. Furthermore, the control deficiencies described above created a reasonable possibility that a material misstatement to the consolidated financial statements would not be prevented or detected on a timely basis. Therefore, we concluded that	**S-K 308(a)** – Provide a report of management on the registrant's internal control over financial reporting (as defined in § 240.13a-15(e) or § 240.15d-15(e) of this chapter) that contains: • **S-K 308(a)(3) –** Management's assessment of the effectiveness of the registrant's internal control over financial reporting as of the end of the registrant's most recent fiscal year, including a statement as to whether or not internal control over financial reporting is effective. This discussion must include disclosure of any material weakness in the registrant's internal control over financial reporting identified by management. Management is not permitted to conclude that the registrant's internal control over financial reporting is effective if there are one or more material weaknesses in the registrant's internal control over financial reporting. • **SEC FRM 4310.12 –** Management should consider disclosing the following with respect to a material weakness:	A paragraph satisfying the requirements in S-K 308(a) must be included under this section of the 9A certification. Note the following about this paragraph. • It should identify and clearly articulate the deficiency that resulted in the material weakness, including the financial statement captions presented in the Form 10-K that were affected. It is in the entity's best interest to be specific and clearly identify the deficiency. • It should describe the actual control that failed or is missing, not what resulted from the ineffective control. • It should indicate why the controls operated ineffectively. Clear discussion around the root cause of the control deficiency can be difficult. Readers need to know why the control was missing, wasn't designed correctly, or didn't operate effectively. There is not a requirement to state the exact COSO principle impacted, but the discussion should be clear as to the affected principles. Using language from the various points of focus related to the COSO principle

Item 9A Example paragraph	Source of requirements	Tips and guidance
the deficiencies represent material weaknesses in the Company's internal control over financial reporting, and our internal control over financial reporting was not effective as of December 31, 20XX.	a) Describe the nature of the material weakness. b) Describe its impact on the financial reporting and ICFR, if any.	can be helpful in clearly articulating the root cause. In addition, while the requirements in SEC FRM 4310.12 state that management 'should consider' disclosing certain information about a material weakness, we believe 'should consider' is a strong indicator that the information should be in management's report on internal control over financial reporting. Our experience indicates there is an expectation by the SEC that such information is disclosed. Note the following about the paragraph that includes the information referred to in SEC FRM 4310.12(a) and (b). • It describes the impact of the material weakness. This can either be done in the paragraph describing the material weakness or, more often, in a paragraph following the discussion of the control deficiencies. • If there was a restatement of financial statements, material or immaterial, to reflect the correction of an error resulting from a material weakness, it should disclose that fact and reference the note describing the restatement. • It should not include the amount of any misstatements.
Our independent registered public accounting firm, KPMG LLP, who audited the consolidated financial statements included in this Annual Report on Form 10-K, issued an adverse opinion on the effectiveness of the Company's internal control over financial reporting. KPMG	**S-K 308(a)** – Provide a report of management on the registrant's internal control over financial reporting (as defined in § 240.13a-15l or § 240.15d-15l of this chapter) that contains:	A paragraph satisfying the requirements noted must be included under this section of the 9A certification. Note the following about this paragraph. • It captures the required statement that the independent auditor has audited

Item 9A Example paragraph	Source of requirements	Tips and guidance
LLP's report appears on page [F-3] of this Annual Report on Form 10-K.	• **S-K 308(a)(4) –** If the registrant is an accelerated filer or a large accelerated filer (as defined in § 240.12b-2 of this chapter), or otherwise includes in its annual report a registered public accounting firm's attestation report on internal control over financial reporting, a statement that the registered public accounting firm that audited the financial statements included in the annual report containing the disclosure required by this Item has issued an attestation report on the registrant's internal control over financial reporting.	the financial statements and the Company's ICFR. • It should state that the auditors' report on ICFR is adverse. • It need not state where the auditors' report is located in the Form 10-K, but may state that it is 'elsewhere in this Form 10-K.' • It may capture the location of the auditors' report in other ways, such as by indicating that it is included in Item 9A(y). • It should not indicate that the adverse auditors' report is 'included herein' or 'is incorporated herein', as it is not part of management's report on internal control over financial reporting. • If the entity is not required to have its auditor provide an audit report on ICFR (e.g. non-accelerated filers), it should be replaced with: 'This annual report does not include an attestation report of the Company's registered public accounting firm due to the established rules of the Securities and Exchange Commission.'
MANAGEMENT'S REMEDIATION PLAN		
The Company is committed to making further progress in its remediation efforts during 20XX. The following steps will continue to be executed until remediation of the material weaknesses is achieved: • Hire, train, and retain individuals with the appropriate skills and experience related to technical accounting,	**SEC FRM 4310.12 –** Management should consider disclosing the following with respect to a material weakness: a) Describe management's current plans or action already undertaken, if any, for remediating the material weakness.	While the requirements in SEC FRM 4310.12 state that management 'should consider' disclosing certain information about a material weakness, we believe 'should consider' is a strong indicator that the information should be in management's report on internal control over financial reporting. Our experience

Item 9A Example paragraph	Source of requirements	Tips and guidance
internal control over financial reporting, and the design and implementation of information technology solutions. • Enhance risk assessment and prioritize remediation activities that most significantly reduce the risk that a material misstatement to the consolidated financial statements would not be prevented or detected on a timely basis. • Implement and monitor our phased approach to remediation of control activities in additional process areas. • Enhance information and communication processes through information technology solutions to ensure that information needed for financial reporting is accurate, complete, relevant and reliable, and communicated in a timely manner. • Report regularly to the audit committee on the progress and results of the remediation plan, including the identification, status and resolution of internal control deficiencies.		indicates there is an expectation by the SEC that such information is disclosed. Note the following about the paragraph that includes the information referred to in SEC FRM 4310.12(c). • It should include remediation plans that match each element of the material weakness. It's often easiest for readers if the remediation steps are listed in the same order as the issues described in the material weakness. • It should include remediation discussion that is consistent with the root cause included in describing the material weakness. If management has remediation steps that are not directly related to the discussion of the reason for the material weakness, they will likely need to further describe the material weakness. • It should include those plans that reflect the entity's reasonable expectations at the time they are made. • It should not be included as part of the section titled 'management's report on internal control over financial reporting'. If it were to be included within management's report on internal control over financial reporting, the external auditor would disclaim on such language in the auditor's report. • It generally should not be too optimistic and be clear that a deficiency has not been remediated

Item 9A Example paragraph	Source of requirements	Tips and guidance
		until the remediated control has been tested and the entity has concluded it is designed, implemented and operating effectively for a reasonable period of time. • While the conclusion that a deficiency has been remediated is a management assertion, it is prudent to coordinate with the auditor in considering the sufficiency of remediation efforts.

Notes:

1. The title of this section should be along the lines of 'Management's Report on Internal Control Over Financial Reporting' or 'Management's Annual Report on Internal Control Over Financial Reporting.' Management should verify the title of management's report lines up with the reference in the external auditors' ICFR report.

Question 9.8.50

What are the entity's disclosure obligations in subsequent periods related to previously disclosed material weaknesses?

Interpretive response: In quarterly filings, including those subsequent to the disclosure of a material weakness in Item 9A on Form 10-K, an entity has an obligation to disclose material changes to ICFR in Item 4 on Form 10-Q. Material changes include both positive and negative developments. Therefore, if management has implemented changes to ICFR to remediate a material weakness, it should disclose those changes.

Management may wish to also disclose in an interim filing that the material changes have remediated the material weakness. However, management should carefully consider whether to do so for the following reasons.

- In general, new controls need to be operating for a sufficient period of time to be tested and allow for a conclusion that they remediated the material weakness.
- The external auditor generally will not be in a position to determine whether the material weakness has been remediated until it completes the next audit. It is best to avoid a situation where the entity has disclosed that the material weakness has been remediated, but the subsequent Form 10-K contains the same material weakness because it is determined that the material weakness still exists after the external auditor has performed the audit.

In lieu of disclosing that the changes have remediated the material weakness, management may disclose that the changes were in response to the material weakness and that it is currently assessing the operating effectiveness of the remediated or new controls.

Question 9.8.60

What if management concludes its original assessment of ICFR was incorrect?

Interpretive response: If an entity's management concludes that its original assessment of ICFR was incorrect, it should consider whether to revise its original report on ICFR. The entity also should reevaluate the appropriateness of its prior disclosures regarding the effectiveness of the entity's DCP and make any necessary revisions.

For example, assume that an entity discloses that its Chief Financial Officer and Chief Executive Officer concluded its DCP was effective in its original Form 10-K. Subsequently, the entity filed a Form 10-K/A to restate its financial statements for errors. In the Form 10-K/A, the entity revises its disclosures to state that the Chief Financial Officer and Chief Executive Officer conclude its DCP was not effective, and the reasons why.

Question 9.8.70
What are the implications if deficiencies are identified at an interim period?

Interpretive response: Even though formal testing is not required at interim periods, a significant deficiency or material weakness may come to the attention of management and auditors during an interim period.

In such cases, there is still a need for management to perform an evaluation of the severity of the deficiency because:

- the certifying officers of the entity state whether all significant deficiencies and material weaknesses have been communicated to the external auditor and those responsible for oversight of the entity's financial reporting; and
- material changes in ICFR need to be disclosed in an interim filing with the SEC as well as a conclusion on DCP.

Part of the evaluation of a deficiency identified at an interim period is to determine whether there is an indication that a similar deficiency in the form of a material weakness existed in a previous period and whether it is necessary to amend a previous filing. This involves a determination of whether the circumstances that gave rise to the material weakness also existed as of the date of the previously issued financial statements (see Question 9.8.100)

Question 9.8.80
How are deficiencies evaluated at an interim period?

Interpretive response: A known misstatement in an interim period is evaluated against the financial results of the interim period for purposes of assessing the severity of the underlying control deficiency.

If the deficient control is designed to operate at a point in time, management evaluates it in relation to the interim financial results for the quarterly period(s) in which the deficiency existed. As such, when assessing the severity of the deficiency, the potential magnitude of the misstatement is compared to the average quarterly materiality thresholds.

If the deficient control operates during a specified period, the deficiency is evaluated in relation to the results during the period (and future periods) the deficient control was intended to operate. For example, deficient controls related to the interim tax provision are different from those over the annual provision and operate at a level that is less precise than the annual provision controls. Deficiencies in the interim controls over the tax provision do not mean that the annual tax provision controls are not present and functioning. In this case, the deficiency should only be assessed for whether there is a reasonable possibility that the interim period (or future interim periods) would be misstated because of the deficiency.

However, if the deficient control is designed to operate continuously throughout the year, the evaluation assumes the deficiency could result in misstatements equally throughout the year. As such, when assessing the severity of the deficiency, the potential magnitude of the misstatement is divided by four and compared to the average quarterly materiality thresholds.

Question 9.8.90

What are management's responsibilities over DCP on a quarterly basis?

Interpretive response: SEC rules require that management evaluate the effectiveness of DCP on a quarterly basis.

There is no requirement for management to perform a full ICFR evaluation at interim periods. Instead, SEC Release No. 33-8238 indicates the following.

Excerpts from SEC Release No. 33-8238

> [A] company must disclose any change in its internal control over financial reporting that occurred during the fiscal quarter covered by the quarterly report, or the last fiscal quarter in the case of an annual report that has *materially affected*, or is reasonably likely to materially affect, the company's internal control over financial reporting. (emphasis added)
>
> [A]lthough the final rules do not explicitly require the company to disclose the reasons for any change that occurred during a fiscal quarter, or to otherwise elaborate about the change, a company will have to determine, on a facts and circumstances basis, whether the reasons for the change, or other information about the circumstances surrounding the change, constitute material information necessary to make the disclosure about the change not misleading.

Generally, if a material weakness is identified in an interim period, entities disclose the material weakness in Item 4 on Form 10-Q, as they otherwise would disclose a material weakness in Item 9A on Form 10-K (see Question 9.8.20). In addition, management should conclude that DCP is ineffective because ICFR is generally a subset of DCP. The material weakness ordinarily is described in the disclosure about ineffective DCP because there is no requirement for management to perform an ICFR evaluation at an interim date. Even if material changes to internal controls have not yet occurred, management may wish to describe planned changes to internal controls intended to respond to the material weakness.

As discussed in Question 9.8.50, sometimes entities wish to disclose in Item 4 on Form 10-Q that the material weakness has been remediated. Entities should use caution when making such assertions, as the external auditors are not likely to be able to conclude that the material weakness has been remediated until the next annual audit has been completed. It is best for management to avoid situations where the entity discloses in an interim period that the material weakness has been remediated only to later conclude upon completion of the external audit that the material weakness still exists.

Question 9.8.100

What are the reporting requirements if a material weakness is identified and remediated in the same interim period?

Interpretive response: In certain situations, a material weakness is identified and remediated within the same interim period. Because the material weakness was remediated before to the end of the reporting period, there is no requirement for entities to disclose the material weakness in Item 4 on Form 10-Q (or Item 9A on Form 10-K in the case of the fourth quarter).

However, when a material weakness was remediated before the end of any reporting period, management should consider its requirements to disclose changes in internal control that have materially affected, or are reasonably expected to materially affect, the entity's ICFR as discussed in Question 9.8.70. The remediation of a material weakness within an interim period would generally constitute a material change in ICFR.

Management should also consider:

- whether the remediated material weakness existed in previous periods;
- the related effect on the appropriateness of prior DCP conclusions; and
- whether the entity should take steps to prevent reliance on a previously issued report on the effectiveness of ICFR.

Key takeaways

- A control deficiency represents the potential for misstatement of the financial statements.
- The absence of a misstatement in the financial statements doesn't mean there is not a control deficiency. Control deficiencies can and do exist in the absence of a misstatement to the financial statements.
- Management performs a root cause analysis to determine the cause of the control deficiency. It may cause multiple levels of evaluation to get the relevant COSO component and principle.
- Management avoids describing the deficient control in terms of the error. The error is not the deficiency – the control that failed to detect or prevent the error is the deficiency.
- Management looks for commonalities to determine if the same type of control deficiency exists in similar controls.
- A control deficiency may indicate a broader issue in another component or principle of ICFR.
- Management evaluates whether there is a reasonable possibility that a material misstatement could occur because of a deficiency. Reasonable possibility means more than remote.
- If the deficiency resulted in a misstatement in the financial statements, the amount of the misstatement is the floor when determining its magnitude. In most cases, the magnitude of the potential misstatement is greater than the floor.
- Material weaknesses can and do exist in the absence of a misstatement to the financial statements.
- A compensating control does not have to operate at the same level of precision as the deficient control but should operate at a level of precision that would prevent or detect a material misstatement of the account assertions effected by the control deficiency.
- At a minimum, management aggregates deficiencies related to the same financial statement account, disclosure or assertion and component/principle in the COSO Framework. Deficiencies may also be aggregated based on other commonalities identified.
- While analyzing the aggregation of deficiencies, management considers the 'big picture', including:
  - the controls within the process that are deficient and those that are effective;
  - the collective likelihood that a misstatement would be undetected and the collective magnitude of that potential misstatement; and
  - whether a prudent official would reach the same conclusion.

10. Artificial intelligence and automation

Detailed contents

10.1 Management’s ICFR journey

When integrating AI and automation into financial reporting, management is responsible for adapting their ICFR to address the new and unique risks introduced by the technology. Management can use the COSO framework and the guidance presented in chapters 1-9 to provide a structured approach to facilitate effective oversight of the use of AI and automation to:

- identify relevant risks; and
- determine appropriate control responses.

This chapter discusses the various types of technologies that are commonly referred to as AI and automation and describes how they may be used in an entity’s financial reporting process. It also discusses management’s responsibilities as it relates to ICFR when AI and automation are used in financial reporting.

Abbreviations

We use the following abbreviations in this chapter.

AI	Artificial intelligence
COSO	Committee of Sponsoring Organizations of the Treadway Commission
GITC	General IT control
ICFR	Internal control over financial reporting

10.2 AI and automation

Question 10.2.10
What are AI and automation?

Interpretive response: AI and automation encompass a fairly wide spectrum of technologies, as further discussed below.

AI

AI is defined as tools with advanced algorithms capable of performing complex tasks that go beyond simple automation, emulating human intelligence to perform cognitive tasks.

AI is not a single technology or platform, instead it represents a multidimensional and sometimes evolving solution that integrates various AI subsets.

Subset	Description
Expert systems	Rule-based
Computer vision	Interpret and understand images
Natural language processing	Process natural language and speech
Effective computing	Understand/respond to human emotions
Machine learning	Learn from training data to develop models, predictions, or insights without explicit programming
Deep learning	Simulate human-like learning and decision-making processes, such as those used in generative AI

Automation

Automation is defined as tools that automate repetitive tasks and processes to augment human activities, improving quality and efficiency.

The spectrum of automation ranges from data analytics and user-enabled automation to bots that automate repetitive, rule-based tasks (e.g. Robotic Process Automation).

See KPMG guide, AI and automation in financial reporting, for additional information related to the definition and examples of AI and automation.

10.3 AI and automation in financial reporting

Question 10.3.10

How are AI and automation used in an entity's financial reporting process?

Interpretive response: Entities use AI solutions and automation at various points in the financial reporting process. These tools may be deployed to:

- initiate, process, record and report transactions or information within a process; and/or
- execute controls.

When AI and automation are used to execute controls, they may be integrated into existing controls or used to autonomously execute control activities such as data validation, access management and exception handling, often enhancing or replacing manual controls.

Common use cases: AI

Detecting fact patterns and establishing models (e.g. predictive models, forecasting)

- Simulate market conditions, cash flow predictions and macroeconomic factors for budgeting
- Analyze supply chain/inventory models for valuation adjustments, reserves and allowances
- Analyze performance targets for bonus or commission calculations

Documenting analysis/scanning large datasets

- Perform customer evaluations (e.g. credit risk, loan decision-making)
- Identify relevant data elements in documents (invoices, purchase orders, cash receipts) using natural language processing and computer vision
- Perform supplier evaluations (e.g. scanning for non-compliant terms)

Providing citations/references

- Perform research (e.g. accounting or legal research using generative AI models)
- Identify financial ratios, exchange rates, or stock analysis information using generative AI tools and input into schedules/models for financial reporting (e.g. stock compensation, FX calculations)

Examples of using AI in process control activities

Activity	Example
Data validation	Use machine learning to analyze data beyond predefined rules or criteria to identify exceptions/conflicts for review.
Access provisioning	Remove/block access to IT systems based on historical behavior, patterns, or unusual activity.
Exception handling	Automatically resolve exceptions/conflicts without human involvement.

Common use cases: Automation

- Open/read emails and attachments to extract data from specified fields
- Log into web applications to perform routine tasks
- Extract structured data from documents
- Copy/paste values, fill in forms, move files and folders
- Collect statistics
- Post recurring journal entries

Examples of automating process control activities

Activity	Example
Data validation	Validate data against predefined rules/criteria to identify exceptions/conflicts for review.
Access provisioning	Compare new user access requests against an approved roles matrix before provisioning access.
Exception handling	Handle exceptions within control activities by following predefined rules or escalation procedures; route exceptions to appropriate individuals or departments for review and resolution.

10.4 Management's responsibilities when using AI and automation

Question 10.4.10

What are management's responsibilities as it relates to ICFR when AI and/or automation is used in the financial reporting process?

Interpretive response: Management remains responsible for designing, implementing, and maintaining an effective system of ICFR. As AI and automation become increasingly integrated into various business and financial reporting processes and the related controls, they create opportunities for efficiency and insight in financial reporting but also present new risks and challenges such as explainability, reliability, exposure to third-party risks, etc. These risks and challenges require a comprehensive response from management and those charged with governance that spans all components of internal control addressed in this Handbook.

Among others, management's responsibilities related to implementation and use of AI and automation include the below examples:

Management's responsibility	Description
Establish a strong control environment	Define the vision and strategy for the use of AI and automation in financial reporting with oversight from the board and audit committee. In addition, set policies, procedures, and guidelines for identifying, acquiring, designing, deploying, and monitoring these tools.
Oversight and accountability	Assign ownership and accountability for AI and automation, including governance, risk oversight, and direction on risk identification, evaluation, and mitigation.
Competence and training	Provide training to upskill employees and enable them to understand the implications of AI and automation.
Risk assessment	Identify and assess risks to financial reporting that may arise from using AI and automation.
Information and communication	Facilitate timely and accurate information flow and communication about the use of AI and automation, their performance, and risks to relevant stakeholders.
Monitoring activities	Implement monitoring controls for AI and automation, such as post-deployment reviews, periodic model validation, and continuous testing for performance, accuracy, and bias.
Implement and/or adapt process control activities and GITCs	Implement and/or adapt process control activities and GITCs to address the unique risks of AI and automation tools.

See KPMG guide, AI and automation in financial reporting, for additional information related to developing and implementing a game plan for the design, development and use of AI and automation in the financial reporting process. The guide includes key considerations for identifying and understanding the related risks and developing strong governance policies and procedures to respond to those risks.

Key takeaways

- When AI and automation are used in financial reporting or the entity's ICFR, management remains responsible for maintaining the effectiveness of the entity's internal controls. That may require addressing new risks introduced by the tools.
- KPMG guide, AI and automation in financial reporting, is a resource available to assist management when they are planning to use AI and automation in their financial reporting process and/or ICFR.

Appendix A

COSO Framework's 17 Principles of Effective Internal Control

This appendix presents the 17 principles of effective internal control and the related points of focus set out in the COSO Framework. It also presents examples of controls that entities might implement to address individual principles. The example controls were generated by KPMG to assist users of the Handbook in identifying the types of controls that may address the requirements of COSO. The control examples are only examples and are not all inclusive. Not all of these examples are relevant in all circumstances. There may be additional or different controls used based on the specific circumstances of an entity and the control would need to be customized to the entity's individual facts and circumstances and the complexity of its business structure and other factors. Also, the order of the examples of controls provided is not intended to reflect their relative importance or frequency of occurrence.

Some control examples may address multiple principles and points of focus and management should consider that when evaluating whether all principles and points of focus are appropriately addressed by controls at the entity.

Points of focus	Example controls
Control environment	
Principle 1: The organization demonstrates a commitment to integrity and ethical values.	
• Sets the tone at the top • Establishes standards of conduct • Evaluates adherence to standards of conduct • Addresses deviations in a timely manner	• The code of conduct defines and communicates expectations on integrity, ethical values and compliance with laws and regulations at all levels of the entity and key external parties. • The ethics and compliance committee determines that all employees and relevant external parties acknowledge receipt of the code of conduct and confirm compliance status annually, and that all employees complete training on the code of conduct. • The ethics and compliance committee has established policies and procedures to identify and address improprieties and noncompliance by employees, third-party service providers and other business partners with the code of conduct and other matters. • The CEO's quarterly newsletter emphasizes the importance of ethics

Points of focus	Example controls
	and compliance with the code of conduct.
Principle 2: The board of directors (or equivalent body) demonstrates independence from management and exercises oversight of the development and performance of internal control.	
• Establishes oversight responsibilities • Applies relevant expertise • Operates independently • Provides oversight for the system of internal control	• The board of directors has established its roles and responsibilities for the oversight of internal control. • The board of directors has established policies for meetings between the board of directors and management, including the frequency of such meetings. • The board of directors has established policies for identifying and reviewing board of director candidates. • The board's risk and governance committee oversees the content and communication of the code of conduct, as well as investigation and resolution of noncompliance. • Based on its charter, the audit committee is primarily responsible for overseeing external financial reporting and ICFR.
Principle 3: Management establishes, with board oversight, structures, reporting lines and appropriate authorities and responsibilities in pursuit of objectives.	
• Considers all structures of the entity • Establishes reporting lines • Defines, assigns and limits authority and responsibilities	• The entity uses organization charts and documented authorization policies to establish reporting lines and to define, assign and limit authorities and responsibilities. This documentation is revised to respond to change, as needed, and is communicated throughout the organization. • The entity maintains job descriptions. • The Operating Policy and Procedures Manual includes policies that detail the monetary commitment and transaction approval authorities of management and employees for each occurrence. Employees who exceed the individual transaction's authority must obtain approval from the appropriate member of higher-level management, up to and including the CEO.

Points of focus	Example controls
Principle 4: The organization demonstrates a commitment to attract, develop and retain competent individuals in alignment with objectives.	
• Establishes policies and practices • Evaluates competence and addresses shortcomings • Attracts, develops and retains individuals • Plans and prepares for succession	• The entity identifies the competence requirements to support effective financial reporting and ICFR, evaluates competence across the entity, including external service providers, and acts to address gaps. • The entity has established policies to attract employees, third-party service providers and other professionals with sufficient competencies, and provides training to maintain and develop sufficiently competent personnel. • The entity established contingency, and succession plans to prepare for assignment of financial reporting and ICFR responsibility in the event of changes in leadership.
Principle 5: The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
• Enforces accountability through structures, authorities and responsibilities • Establishes performance measures, incentives and rewards • Evaluates performance measures, incentives and rewards for ongoing relevance • Considers excessive pressures • Evaluates performance and rewards or disciplines individuals	• Quarterly, the director responsible for compliance with the Sarbanes-Oxley Act (SOX) asks employees with internal control responsibilities (control operators) to confirm accountability and represent that they have fulfilled their internal control responsibilities during the quarter, highlighting any exceptions. • The entity's performance incentive plans establish performance measures that incorporate ICFR and ethical responsibilities, consider excessive pressures and provide rewards or penalties as appropriate. • Annual employee performance reviews and employee incentive rewards reinforce expected standards of behavior, consistent with the entity's code of conduct. Specifically, they consider employees' adherence to their ICFR responsibilities, evaluation of competence and achievement of business goals during the period.

Points of focus	Example controls
Risk assessment	
Principle 6: The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	
• Complies with applicable accounting standards • Considers materiality • Reflects entity activities	• The entity specifies financial reporting and ICFR objectives that are consistent with GAAP and SEC regulations, reflect the entity's activities, and consider materiality. • The entity's accounting policies for all financial statement accounts, underlying transactions and disclosures are maintained by the Financial Reporting Manager, responsible for SEC reporting, and reviewed and approved by the Corporate Controller and CFO. • Management assesses materiality at the consolidated financial statement level at the beginning of the fiscal year, and again as necessary if the entity's business changes (i.e. the results of operations and financial position change significantly). • The entity monitors compliance with laws and regulations that could potentially have a significant effect on financial reporting in the event of noncompliance.
Principle 7: The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	
• Includes entity, subsidiary, division, operating unit, and functional levels • Analyzes internal and external factors • Involves appropriate levels of management • Estimates significance of risks identified • Determines how to respond to risks	• For purposes of the business risk assessment and development of the annual financial plan, the Finance Group identifies, analyzes and assesses the significance of financial reporting risks across the entity, and determines how it will manage those risks.
Principle 8: The organization considers the potential for fraud in assessing risks to the achievement of objectives.	
• Considers various types of fraud (applicable to ICFR) • Assesses incentives and pressures • Assesses opportunities • Assesses attitudes and rationalizations	• The entity's fraud risk assessment process identifies and responds to fraud risks to financial reporting by considering various types of fraud, and assessing incentives and pressures, opportunities, and attitudes and rationalizations.

Points of focus	Example controls
Principle 9: The organization identifies and assesses changes that could significantly impact the system of internal control.	
- Assesses changes in the external environment - Assesses changes in the business model - Assesses changes in leadership	- Change management procedures are in place to enable the entity to identify and respond to changes that could significantly affect financial reporting or ICFR.
Control activities	
Principle 10: The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	
- Integrates with risk assessment - Considers entity-specific factors - Determines relevant business processes - Evaluates a mix of control activity types - Considers at what level activities are applied - Addresses segregation of duties	- The entity uses a risk and control matrix to map identified risks to control activities. See chapter 5 for further discussion as control activities are specific to each entity and its processes.
Principle 11: The organization selects and develops general control activities over technology to support the achievement of objectives.	
- Determines dependency between the use of technology in business processes and technology general controls - Establishes relevant technology infrastructure control activities - Establishes relevant security management process control activities - Establishes relevant technology acquisition, development, and maintenance process control activities	- The entity uses a risk and control matrix to document technology dependencies. See chapter 7 for further discussion as general IT controls are specific to each entity, its processes, and technology.
Principle 12: The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.	
- Establishes policies and procedures to support development of management's directives - Establishes responsibility and accountability for executing policies and procedures - Performs in a timely manner	- The entity periodically reviews control activities to determine their continued relevance and refreshes them when necessary. - The entity has a policy in place that all payments must be authorized before cash is remitted.

Points of focus	Example controls
• Takes corrective action • Performs using competent personnel • Reassesses policies and procedures	See chapter 5 for further discussion as policies and procedures are specific to each entity and its processes.
Information and communication	
Principle 13: The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.	
• Identifies information requirements • Captures internal and external sources of data • Processes relevant data into information • Maintains quality throughout processing • Considers costs and benefits	• The entity maintains a data integrity program to address the relevance and quality of information used throughout the entity in the operation of ICFR. • The entity maintains a central repository of documentation associated with ICFR.
Principle 14: The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	
• Communicates internal control information • Communicates with the board of directors • Provides separate communication lines • Selects relevant method of communication	• Monthly cross-functional meetings are held to provide a forum for communicating information affecting ICFR. • An anonymous hotline is established by the Ethics and Compliance Committee and is externally administered to provide a forum for communicating fraud or ethical matters.
Principle 15: The organization communicates with external parties about matters affecting the functioning of internal control.	
• Communicates to external parties • Enables inbound communications • Communicates with the board of directors • Provides separate communication lines • Selects relevant method of communication	• The entity has a process to identify and capture the relevant sources of external data through assignment of responsibility for capturing the information and communicating it internally. • The entity has a process to enable communication of information regarding stakeholder and/or regulatory compliance that affects external reporting objectives. • The entity has established a Disclosure Review Committee that oversees the effectiveness of the entity's disclosure controls and procedures.

Points of focus	Example controls
Monitoring	
Principle 16: The organization selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	
• Considers a mix of ongoing and separate evaluations • Considers rate of change • Establishes baseline understanding • Uses knowledgeable personnel • Integrates with business processes • Adjusts scope and frequency • Evaluates objectively	• The CFO and Internal Audit (IA) Director maintain a Monitoring Plan that describes how the entity's internal controls over all COSO principles and components are monitored. • An Audit Charter and Work Plan for the entity's IA function are prepared annually and are reviewed and approved by the Audit Committee. • The entity's business process owners perform periodic reviews of key performance indicators (KPIs) and specific metrics as a monitoring activity over their respective process. • A management-directed task force is established to perform targeted monitoring reviews over specific processes and controls.
Principle 17: 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.	
• Assesses results • Communicates deficiencies • Monitors corrective actions	• The entity tracks, evaluates and communicates deficiencies in ICFR to executive management and the Audit Committee. • Deficiency remediation plans and actions are tracked and communicated.

Appendix B

Examples of fraud risk factors, circumstances that indicate the possibility of fraud, and frauds

This appendix includes examples of fraud risk factors that may be encountered in a broad range of situations. Many of the examples are adapted from those provided by the auditing standards, including PCAOB AS 2401 – *Consideration of Fraud in a Financial Statement Audit* and Appendix A to the AICPA's AU-C Section 240 – *Consideration of Fraud in a Financial Statement Audit*, supplemented by KPMG based on practical experience. Separately presented are examples relating to the two types of fraud relevant to management's and external auditors' consideration:

- fraudulent financial reporting, and
- misappropriation of assets.

Although the fraud risk factors cover a broad range of situations, **they are only examples** and, accordingly, **there may be additional or different risk factors in the specific circumstances of an entity**. Not all of these examples are relevant in all circumstances, and some may be of greater or lesser significance in entities of different sizes or with different ownership characteristics or circumstances. Also, the order of the examples of fraud risk factors provided is not intended to reflect their relative importance or frequency of occurrence.

The examples in this Appendix provide an overview of possible fraud risk factors and are meant to serve as **a starting point for the identification of fraud risks specific to the entity**. In most cases, when a fraud risk has been identified, that risk should be associated with a significant account(s) and relevant assertion(s). In the unusual case that such a linkage cannot be established, management and external auditors should consider whether the identified fraud risk has been defined in an overly broad manner. The identified fraud risk factors and related fraud risks should be documented by describing the nature of such risks in a specific manner that is not overly broad or too narrow. This will help both management and external auditors to identify the appropriate responses to the fraud risks.

This appendix also presents examples of fraud that may affect various financial statement accounts.

Fraud risk factors relating to misstatements arising from fraudulent financial reporting

The table below includes examples of fraud risk factors relating to misstatements arising from fraudulent financial reporting. The examples are classified based on the three conditions generally present when material misstatements due to fraud occur (the fraud risk triangle):

a. incentives/pressures;
b. opportunities; and
c. attitudes/rationalizations.

Types of fraud risk factors	Specific examples of fraud risk factors
Incentives/pressures	
Financial stability or profitability of the entity is threatened by economic, industry, or entity operating conditions.	• high degree of competition or market saturation, accompanied by declining margins • high vulnerability to rapid changes, such as changes in technology, product obsolescence, or interest rates • significant declines in customer demand and increasing business failures in either the industry or overall economy • operating losses making the threat of bankruptcy, foreclosure, or hostile takeover imminent • recurring negative cash flows from operations or an inability to generate cash flows from operations while reporting earnings and earnings growth • rapid growth or unusual profitability, especially compared to that of other companies in the same industry • new accounting, statutory, or regulatory requirements
Excessive pressure exists for management to meet the requirements or expectations of third parties.	• profitability or trend level expectations of investment analysts, institutional investors, significant creditors, or other external parties (particularly expectations that are unduly aggressive or unrealistic), including expectations created by management in, for example, overly optimistic press releases or annual report messages • need to obtain additional capital, debt or equity financing to stay competitive, including financing of major research and development or capital expenditures • marginal ability to meet exchange listing requirements, debt repayment, or other debt covenant requirements • perceived or real adverse effects of reporting poor financial results on significant pending transactions, such as business combinations or contract awards • a need to achieve financial targets required in bond covenants • pressure for management to meet the expectations of legislative or oversight bodies or to achieve political outcomes, or both • significant transactions with no economic justification, intended to meet short-term earnings goals • for listed entities: demonstrated history of closely meeting earnings estimates, unusually high

Types of fraud risk factors	Specific examples of fraud risk factors
	price/earnings ratios for the industry, or unexplained trend or pattern in short positions in the entity's stock
Information available indicates that the personal financial situation of management or those charged with governance is threatened by the entity's financial performance.	• significant financial interests in the entity • significant portions of their compensation (for example, bonuses, stock options, and earn-out arrangements) being contingent upon achieving aggressive targets for stock price, operating results, financial position, or cash flows • personal guarantees of debts of the entity • large individual sales of the entity's shares by senior management (e.g. insider trading) • significant related party loans without a clear business purpose
There is excessive pressure on management or operating personnel to meet financial targets established by those charged with governance, including sales or profitability incentive goals.	• management's past performance indicates they are rarely able to meet goals and are consistently managing by crisis
Opportunities	
The nature of the industry, the entity's significance/influence in its local and regional economy/government, or the entity's operations provide opportunities to engage in fraudulent financial reporting.	• significant related party transactions not in the ordinary course of business or with related entities not audited or audited by another firm • a strong financial presence or ability to dominate a certain industry sector or geographic region that allows the entity to dictate terms or conditions to suppliers or customers that may result in inappropriate or non-arm's length transactions • assets, liabilities, revenues, or expenses based on significant estimates that involve subjective judgments or uncertainties that are difficult to corroborate • significant, unusual, or highly complex transactions, especially those close to period end that pose difficult 'substance over form' questions • significant operations located or conducted across international borders in jurisdictions where differing business environments and cultures exist • use of business intermediaries for which there appears to be no clear business justification • overly complex banking arrangements given the nature and size of operations, including significant bank accounts or subsidiary or branch operations in tax-haven jurisdictions for which there appears to be no clear business justification

Types of fraud risk factors	Specific examples of fraud risk factors
	• the entity engages in bill-and-hold or other non-standard transactions • significant, unusual, or highly complex investments, including equity method investees, joint ventures, and variable interest entities, especially those that pose difficult 'substance over form' questions
The monitoring of management is not effective.	• domination of management by a single person or small group (in a non-owner-managed business) without compensating controls (for example, intimidation of subordinates or existence of culture where 'bad news' or 'failing to make the numbers' is virtually not permitted) • oversight by those charged with governance over the financial reporting process and internal control is not effective because, for example, they are not independent of management influence, they are not financially literate, or lack financial management skills and appropriate competencies to oversee the entity's programs and controls to prevent, deter and detect fraud • failure by those charged with governance and key members of the finance function to act as a control in the event that senior management seeks to override established controls or take overly aggressive financial reporting positions, including an inadequate response to significant matters reported in the discussion on financial reporting quality • the internal audit function is not independent of, or is inappropriately influenced by, management (for example, management determines the scope of the function's work or they are directed to not focus on high-risk areas)
There is a complex or unstable organizational structure.	• difficulty in determining the organization or individuals that have controlling interest in the entity • overly complex organizational structure involving unusual legal entities or managerial lines of authority • high turnover of senior management, internal auditors, legal counsel, those charged with governance, or individuals with significant roles in the financial reporting process • senior management or individuals with significant roles in the financial reporting process are from another region or country and may lack knowledge of the local language and the entity's business practices
Internal control components are deficient.	• inadequate monitoring of controls, including automated controls and controls over interim financial reporting • high turnover rates of employment of staff in accounting, information technology, or the internal audit function that are not effective

Types of fraud risk factors	Specific examples of fraud risk factors
	• accounting and information systems that are not effective, including situations involving significant deficiencies or material weaknesses in internal control • weak controls over budget preparation and development • a history of significant adjustments or passed audit adjustments • failure to implement controls to prevent, detect or deter fraud in areas which have been previously reported to those charged with governance • inadequate or no policies relating to the prevention of noncompliance with laws and regulations, including illegal acts
Cultural norms in the business and regulatory environments provide opportunities for management to override controls or intentionally misstate the financial statements.	• criticizing or questioning a figure of authority is contrary to the local culture • whistle blowing channels and protections are less developed
Attitudes/rationalizations	
Attitudes or rationalizations exist that may lead to fraudulent financial reporting.	• ineffective communication, implementation, support, or enforcement of the entity's values or ethical standards by management or the communication of inappropriate values or ethical standards • nonfinancial management's excessive participation in or preoccupation with the selection of accounting policies or the determination of significant estimates • known history of violations of securities laws or other laws and regulations, or claims against the entity, its senior management, or board members alleging fraud or violations of laws and regulations • excessive interest by management in maintaining or increasing the entity's stock price or earnings trend • a practice by management of committing to analysts, creditors, and other third parties to achieve aggressive or unrealistic forecasts • management failing to correct known reportable conditions on a timely basis • an interest by management in employing inappropriate means to minimize reported earnings for tax-motivated reasons • lack of distinction by the owner-manager between personal and business transactions • existence of issues regarding integrity of individuals who have significant influence over financial reporting or are expected to sign the representation letter

Types of fraud risk factors	Specific examples of fraud risk factors
	• management's attempts to unduly influence the reporting of audit findings to those charged with governance • disputes between shareholders in a closely held entity
There is low morale among senior management or lack of skills and experience.	• evaluation of management indicating low or moderate quality of personnel
Management makes recurring attempts to justify marginal or inappropriate accounting on the basis of materiality.	• failure to take appropriate action in response to significant restatements (for example, dismissal of key individuals involved or the installing of appropriate controls) • indication that a restatement may have been due to a possible intentional manipulation
The relationship between management and the current or predecessor auditor is strained.	• frequent disputes with the current or predecessor auditor on accounting, auditing, or reporting matters • unreasonable demands on the auditor, such as unrealistic time constraints regarding the completion of the audit or the issuance of the auditors' report(s) restrictions on the auditor that inappropriately limit access to people or information or the ability to communicate effectively with those charged with governance • domineering management behavior in dealing with the auditor, especially involving attempts to influence the scope of the auditor's work or the selection or continuance of personnel assigned to or consulted on the audit engagement
Management has a history of earnings management or inaccurate estimates.	• indication that management has provided unreasonable, unreliable, or inaccurate estimates or other representations, or management has been less than forthright • there are concerns of apparent earnings management

Fraud risk factors relating to misstatements arising from misappropriation of assets

The table below includes examples of fraud risk factors that relate to misstatements arising from misappropriation of assets. The examples are classified according to the three conditions generally present when fraud exists (the fraud risk triangle):

- incentives/pressures,
- opportunities, and
- attitudes/rationalizations.

These examples are generally consistent with the examples provided in the auditing standards, including PCAOB AS 2401 – *Consideration of Fraud in a Financial Statement Audit* and AICPA's AU-C Section 240 – *Consideration of Fraud in a Financial Statement Audit*. Some of the risk factors related to misstatements arising from fraudulent financial reporting presented above may also be present when misstatements arising from misappropriation of assets occur. For example, ineffective monitoring of management and other deficiencies in internal control may result in misstatements due to either fraudulent financial reporting or misappropriation of assets.

Types of fraud risk factors	Specific examples of fraud risk factors
Incentives/pressures	
Personal financial obligations may create pressure on management or employees with access to cash or other assets susceptible to theft to misappropriate those assets.	• management or employees exhibit signs they are spending outside their personal means (expensive trips, vehicles, etc.)
Adverse relationships between the entity and employees with access to cash or other assets susceptible to theft may motivate those employees to misappropriate those assets.	• known or anticipated future employee layoffs • recent or anticipated changes to employee compensation or benefit plans • promotions, compensation, or other rewards inconsistent with expectations
Opportunities	
Certain characteristics or circumstances may increase the susceptibility of assets to misappropriation.	• large amounts of cash on hand or processed • inventory items that are small in size, of high value, or in high demand • easily convertible assets, such as bearer bonds, diamonds, or computer chips • fixed assets which are small in size, marketable, or lacking observable identification of ownership
Inadequate internal control over assets may increase the susceptibility of misappropriation of those assets.	• inadequate segregation of duties or independent checks • inadequate oversight of senior management expenditures, such as travel and other re-imbursements • inadequate management oversight of employees responsible for assets, for example, inadequate supervision or monitoring of remote locations • inadequate job applicant screening of employees with access to assets • inadequate record keeping with respect to assets

Types of fraud risk factors	Specific examples of fraud risk factors
	• inadequate system of authorization and approval of transactions (for example, in purchasing) • inadequate physical safeguards over cash, investments, inventory, or fixed assets • lack of complete and timely reconciliations of assets, for example, comparison of inventory records to inventory counts • lack of timely and appropriate documentation of transactions, for example, credits for merchandise returns • lack of mandatory vacations for employees performing key control functions • inadequate management understanding of information technology, which enables information technology employees to perpetrate a misappropriation • inadequate access controls over automated records, including controls over and review of computer systems event logs
Attitudes/rationalizations	
Attitudes or rationalizations exist that may lead to misappropriation of assets.	• disregard for the need for monitoring or reducing risks related to misappropriations of assets • disregard for internal control over misappropriation of assets by overriding existing controls or by failing to correct known internal control deficiencies • behavior indicating displeasure or dissatisfaction with the entity or its treatment of the employee • changes in behavior or lifestyle that may indicate assets have been misappropriated • belief by some government or other officials that their level of authority justifies a certain level of compensation and personal privileges • tolerance of petty theft

The following are examples of circumstances that may indicate the possibility that the financial statements may contain a material misstatement resulting from fraud. These examples are generally consistent with the examples provided in the auditing standards, including PCAOB AS 2810 – *Evaluating Audit Results* and AICPA's AU-C Section 240 – *Consideration of Fraud in a Financial Statement Audit*, supplemented based on practical experience.

Circumstance	Examples
Discrepancies in the accounting records	• transactions that are not recorded in a complete or timely manner or are improperly recorded as to amount, accounting period, classification, or entity policy

Circumstance	Examples
	• unsupported or unauthorized balances or transactions • last-minute adjustments that significantly affect financial results • evidence of employees' access to systems and records inconsistent with that necessary to perform their authorized duties • tips or complaints about alleged fraud
Conflicting or missing evidence	• missing documents without a reasonable explanation • documents that appear to have been altered without a reasonable explanation • unavailability of other than photocopied or electronically transmitted documents when documents in original form are expected to exist • significant unexplained items on reconciliations • unusual balance sheet changes, or changes in trends or important financial statement ratios or relationships, for example, receivables growing faster than revenues • inconsistent, vague, or implausible responses from management or employees arising from inquiries or analytical procedures • unusual discrepancies between the entity's records and confirmation replies or other third-party evidence • large numbers of credit entries and other adjustments made to accounts receivable records • unexplained or inadequately explained differences between the accounts receivable sub-ledger and the control account, or between the customer statements and the accounts receivable sub-ledger • missing or non-existent cancelled checks in circumstances where cancelled checks are ordinarily returned to the entity with the bank statement • missing inventory or physical assets of significant magnitude • unavailable or missing electronic evidence, inconsistent with the entity's record retention practices or policies • fewer responses to confirmation requests than anticipated or a greater number of responses than anticipated • inability to produce evidence of key systems development and program change testing and implementation activities for current-year system changes and deployments

Circumstance	Examples
Problematic or unusual relationships between auditors (internal or external) and management	• denial of access to records, facilities, certain employees, customers, vendors, or others from whom audit evidence might be sought • undue time pressures imposed by management to resolve complex or contentious issues or to complete the audit • complaints by management about the conduct of the audit or management intimidation of engagement team members, particularly in connection with auditors' critical assessment of audit evidence or in the resolution of potential disagreements with management • unusual delays by the entity in providing requested information • unwillingness to facilitate auditors' access to key electronic files for testing through the use of computer assisted auditing techniques • denial of access to key IT operations staff and facilities, including security, operations, and systems development personnel • unwillingness to add or revise disclosures in the financial statements to make them more complete, transparent, and understandable • unwillingness to address identified deficiencies in internal control on a timely basis • frequent disputes with auditors (current and former) on accounting, auditing, or reporting matters
Other	• unwillingness by management to permit auditors (internal or external) to meet privately with those charged with governance • accounting policies that appear to be at variance with industry norms • frequent changes in accounting estimates that do not appear to result from changed circumstances • tolerance of violations of the entity's code of conduct

Examples of fraud

The table below includes examples of fraud that may affect various financial statement accounts.

Frauds	Examples of frauds
Revenue	
False sales/customers	• false sales • sales to fake customers

Frauds	Examples of frauds
	• sales to related parties • kickbacks to customers • overcharging customers
Advancing or delaying the recognition of revenue	• sales recognized on the basis of a purchase order • collusive pre-invoicing • undisclosed sales or returns • trade loading • inventories allocated to third-party warehouses under their control • side letters to advance or delay revenue recognition
Manipulation of rebates/discounts	• rebates/discounts that are not accrued • hidden agreements allowing rebates or discounts • credits hidden through price manipulation in subsequent periods • inventory taken back from customers at full valuation • debits/credits transferred to fake account for write-off in subsequent periods
Misrepresentation of credit status of customers	• false information on initial credit status to induce sales to poor credit risk customers • suppression of customer credit information • bribery of credit control staff
Under- or over-provision for bad debts	• false representation of customers' account status • recycled funds that give appearance that customer accounts are current • manipulation of accounts receivable aging
Expenses	
Under- or over-accruals	• under-accruals/reversal of accruals • false accruals • making accruals to meet budget • forward purchase orders • over/understatement of cost of goods sold • false consulting contracts
Delaying or advancing expenses	• non-standard payment terms to compensate for reduced or inflated prices • misrepresentation of accounts payable aging • teeming and lading of suppliers
Manipulation of rebates/discounts	• rebates taken to income early • extra charges against rebates in subsequent periods • postponed charges • hidden agreements

Frauds	Examples of frauds
Misrecording of capital items	• false sales and leaseback arrangements • hiding capital items in revenue or revenue items in capital • allocating costs in contravention of accounting policies
Hidden contract terms	• hidden conditions and terms that impact results • side letters to advance or delay expense recognition
Inventory	
False valuation	• over- or under-valuation of raw materials inventory • over- or under-valuation of work-in-progress • losses on unprofitable contracts hidden in work-in-progress on profitable contracts
False quantity	• inventory already sold or leased included in inventory counts • borrowed inventory • forged quantities at inventory observation • inventory cut-off manipulation • empty boxes included on inventory pallets
False quality	• false documents relating to quality of inventory • suppression of adverse inventory quality data
False ownership status	• forged information on prospects of disposal • misrepresentation of ownership status
Standard cost manipulation	• manipulation of price and other inputs to standard costing • standard cost changes inconsistent with changes in selling price/general costs
Cash	
False cash entries	• cash washing, creating illusion of cash movements • rigged bank reconciliations • recycling funds through subsidiaries, joint ventures, and other related parties
Hidden pledges for cash deposits	• hidden pledges in return for temporary cash flow
Teeming and lading or lapping	• cash receipts posted to reduce another customer’s balance • reasons for reconciling differences given as ‘cash-in-transit’ • misappropriated receipts or overpayments resulting in unauthorized overdrafts

Frauds	Examples of frauds
Other accounts	
Misuse of inter-company and suspense accounts	• hiding transfers to and from merger reserves • items in suspense between inter-company accounts • hiding any form of manipulation in suspense accounts
Improper valuation of other assets	• false valuation of fixed or intangible assets • suppression of test or research data that undermines a valuation or forecast
Manipulation of joint ventures	• parking items in joint ventures until subsequent periods • transactions to inflate or depress revenue or expenses
Manipulation of transfer pricing	• profit shifting • assets exchanged for shares at inflated values • values increased or decreased by moving assets among related parties • assets acquired with concealed or understated liabilities
Misuse of merger reserves	• false credits from merger reserves to profit and loss accounts • hiding false debits in merger reserves • over-providing merger reserve items

Appendix C

Internal control deficiency evaluation

This appendix includes a template that can be used by management to document their evaluation of internal control deficiencies under the six-step process outlined in chapter 9. The template covers steps 1-5 of the deficiency evaluation process which focus on the severity of individual deficiencies. Step 6, which is the evaluation of similar deficiencies in the aggregate, is not included in the template. Instead, step 6 would be performed and documented by management in the overall summary of identified control deficiencies. This appendix also includes examples of how the above-referenced template could be applied in practice.

Step 1: Determine whether a control deficiency exists and identify the deficient control

Key reminders about Step 1

1. Remember: **a deficiency represents the potential for misstatement.** Therefore, a deficiency can exist in the absence of a misstatement and such deficiency may be a significant deficiency or a material weakness.

2. Remember: generally, **a misstatement in the financial statements would not exist without a deficiency** that permitted it to occur. Therefore, each misstatement identified in connection with an external audit is likely to have a related deficiency.

3. **Consider the nature and extent of the remediation plan**. Remediation plans are helpful in more precisely identifying and describing a deficiency.

4. Remember: deficiencies in **controls at service organizations** represent deficiencies in the user entity's ICFR when management relies on these controls for the entity’s ICFR.

5. Describe the deficiency in terms of (1) the **control**; and (2) whether the control was **missing, designed inappropriately**, or **operating ineffectively.**

6. **Avoid describing** the deficient control **in terms of the error**. **The error is not the deficiency**; the control that failed to detect or prevent the error is the deficiency.

Determine whether a control deficiency exists:

(Describe the situation that led to considering whether a deficiency exists, the factors assessed, and the conclusion. If no deficiency exists, do not continue to Step 2.)

Identification of the control that failed:

(Describe the deficient control. The deficient control should not be described in terms of the error in the financial statements. Also, indicate whether the control is missing, designed improperly, or not operating effectively.)

Step 2: Understand the cause of the deficiency

Key reminders about Step 2:

1. **Perform a root cause analysis** to determine the cause of the control deficiency.
2. Ask 'why' questions to peel back the layers of the deficiency to get to what really caused the deficiency.
3. Identify the **COSO component and principle** that the deficient control affected.

Root cause of the control deficiency:

(Describe the root cause of the control deficiency.

Step 3: Determine whether the deficiency is indicative of other deficiencies

Key reminders about Step 3:

1. **Look for commonalities** - the same type of control deficiency may exist in similar controls.

Key reminders about Step 3:
2. Be aware that the control deficiency may indicate a **broader issue** in **another component or principle** of internal control.

Does the control deficiency indicate other deficiencies?
(Based on the identification of the control that failed, including the root cause analysis performed in Step 2, consider whether: (1) the same type of control deficiency may exist in similar controls and (2) the control deficiency may indicate a more pervasive issue in another component or principle of internal control.)

Step 4: Evaluate the severity of the deficiency individually (consider the magnitude and likelihood of it resulting in a material misstatement)

Key reminders about Step 4:

1. Evaluate whether there is a reasonable possibility that a material misstatement could occur as a result of a deficiency. ***Reasonable possibility*** **means more than a remote likelihood** of a material misstatement**.**

2. Remember: if the deficiency resulted in a misstatement in the financial statements, the amount of the misstatement is the floor when determining its magnitude. In many cases, the **magnitude of the potential misstatement is greater than the floor.**

3. Remember: the magnitude of a potential misstatement is **not limited** by the assertion that 'management has learned its lesson,' 'reviews are more thoroughly performed when the stakes are higher,' or other such sentiments.

4. Consider the **volume of activity** in the account balance or class of transactions exposed to the deficiency **in the current period** and that is expected **in future periods** as well as the indirect effects of the potential misstatement (e.g. on compliance with debt covenants, stock compensation arrangements).

Key reminders about Step 4:

5. **Use the flowcharts** in the appendices C.1 and C.2 to the ICFR Handbook to assist you through the steps of determining the severity of the deficiency.

6. As part of the severity assessment, **consider the control's objective** (e.g. the PRP(s) or RAFIT(s) that the control was purported to address) and how that control relates to the entire process and relevant financial statement assertions.

Factors in evaluating severity (including reasonable possibility and magnitude of potential misstatement):

(When evaluating the severity, consider:

- *Was a financial statement misstatement identified? If so, what was the amount? Has it been determined that the actual misstatement is the highest potential magnitude? If so, that would be uncommon.*
- *The magnitude of the significant account affected. Is the effect of the deficiency limited to a portion of the significant account balance? If so, why?)*

Step 5: Evaluate the effect of compensating controls and conclude on the severity of the individual control deficiency

Key reminders about Step 5:

1. Remember: to have a mitigating effect, the compensating control should operate at a level of precision that **would** prevent, or detect and correct on a timely basis, a material misstatement of the account affected by the deficiency.

2. Remember: **high-level analytical procedures** and other monitoring controls generally **do not make effective compensating controls**.

3. When relying on a compensating control to limit the severity of an identified deficiency, **evaluate the design and operating effectiveness of the compensating control**. Compensating controls should be part of management's control process to be considered a compensating control.

Key reminders about Step 5:

4. Consider whether the compensating control **meets the same control objective** (e.g. it addresses the same PRP(s) or RAFIT(s)) and addresses the same period of time as the deficient control.

5. Remember: a compensating control **does not eliminate a control deficiency**, but it might limit the severity of a deficiency.

Compensating controls:
(Discuss which compensating control(s) were identified, how the compensating control(s) address the same PRP(s) or RAFIT(s) as the deficient control, and to what degree the compensating control(s) reduce the severity of the deficiency.)

Conclusion on the individual deficiency (Material Weakness, Significant Deficiency, or Deficiency):

Internal control deficiency evaluation – Example 1

NOTE: The deficiency evaluation documented below is for example purposes only and is not intended to be a comprehensive illustration of all factors which may need to be considered in evaluating the severity of a control deficiency. When using this example, professional judgment needs to be used in applying concepts and evaluating considerations relative to the specific circumstances of the entity, which may not be directly analogous to the facts and circumstances that serve as the basis for this example. For instance, this example assumes that no other controls were affected by the lack of appropriate communication that led to the failure of the control evaluated in this example.

Step 1: Determine whether a control deficiency exists and identify the deficient control

Key reminders about Step 1

1. Remember: **a deficiency represents the potential for misstatement.** Therefore, a deficiency can exist in the absence of a misstatement and such deficiency may be a significant deficiency or a material weakness.

2. Remember: generally, **a misstatement in the financial statements would not exist without a deficiency** that permitted it to occur. Therefore, each misstatement identified in connection with an external audit is likely to have a related deficiency.

3. **Consider the nature and extent of the remediation plan**. Remediation plans are helpful in more precisely identifying and describing a deficiency.

4. Remember: deficiencies in **controls at service organizations** represent deficiencies in the user entity's ICFR when management relies on these controls for the entity’s ICFR.

5. Describe the deficiency in terms of (1) the **control**; and (2) whether the control was **missing, designed inappropriately**, or **operating ineffectively.**

6. **Avoid describing** the deficient control **in terms of the error**. **The error is not the deficiency**; the control that failed to detect or prevent the error is the deficiency.

Determine whether a control deficiency exists:

(Describe the situation that led to considering whether a deficiency exists, the factors assessed, and the conclusion. If no deficiency exists, do not continue to Step 2.)

The entity sponsors two pension plans for its employees. One pension plan covers all of its salaried employees, and another plan covers hourly employees. The entity selects its discount rate for the salaried plan by performing a yield curve analysis and discounts the plan's projected cash flows along the yield curve. The construction of the yield curve is well documented and acceptable. The rate produced from this analysis is used as the discount rate for both the salaried plan and the hourly plan. Historically, the salaried and hourly workforce has a relatively low rate of turnover.

However, in the current year, the external auditors identified, through payroll testing, that hourly employees experienced a significant increase in turnover. The high turnover was significant enough to suggest that the cash flow patterns for the hourly plan need to be changed. Ultimately, the discount rate that was determined for the hourly plan was only marginally different from that of the salaried plan, and no adjustment to the financial statements resulted from this finding. However, given the fact pattern, a deficiency exists because an error to the financial statements could have occurred.

Identification of the control that failed:

(Describe the deficient control. The deficient control should not be described in terms of the error in the financial statements. Also, indicate whether the control is missing, designed improperly, or not operating effectively.)

The deficient control:

Management reviews the discount rate inputs related to its pension plan projected benefit obligation for accuracy.

The control did not operate effectively to identify the need for revision to the discount rate input used for the hourly plan. Specifically, the control operator was not aware of the change in the turnover rate of hourly employees that was relevant to evaluation of the discount rate. Had the reviewer been aware of such information, the review would have yielded a different outcome.

Step 2: Understand the cause of the deficiency

Key reminders about Step 2:

1. **Perform a root cause analysis** to determine the cause of the control deficiency.

Key reminders about Step 2:

2. Ask ‘why’ questions to peel back the layers of the deficiency to get to what really caused the deficiency.

3. Identify the **COSO component and principle** that the deficient control affected.

Root cause of the control deficiency:

(Describe the root cause of the control deficiency.)

As noted in Step 1 above, the reviewer was unaware of certain information relevant to evaluation of the discount rate input. This information was known to other members of the entity’s management and widely distributed in a management meeting discussing the status of different divisions within the organization, but the control operator was not invited to, nor did they receive information from, the management meeting. This represents a breakdown in internal communication of relevant information to the control operator (COSO Principle 14).

Step 3: Determine whether the deficiency is indicative of other deficiencies

Key reminders about Step 3:

1. **Look for commonalities** - the same type of control deficiency may exist in similar controls.

2. Be aware that the control deficiency may indicate a **broader issue** in **another component or principle** of internal control.

Does the control deficiency indicate other deficiencies?

(Based on the identification of the control that failed, including the root cause analysis performed in Step 2, consider whether: (1) the same type of control deficiency may exist in similar controls and (2) the control deficiency may indicate a more pervasive issue in another component or principle of internal control.)

We considered whether this issue could arise in other areas. Based on our process narratives, we identified all of the significant controls that involved a level of management review. Each control operator, with the exception of the control operator reviewing the reasonableness of the discount rate, is present at the management meetings.

Further, we revisited our testing of the identified controls that involved a level of management review and noted no similar deficiency related to a lack of communication. Note, we did note a deficiency related to Information and Communication (I&C) in the area of legal contingencies, but it seems to have a different root cause than this deficiency.

(Note: whether we determine that they are sufficiently similar here, or whether we determine that they are not sufficiently similar here but aggregate the I&C deficiencies in Step 6 of the deficiency evaluation process, the ending severity determination should be the same.)

Based on the above, the breakdown in internal communications related to hourly employee turnover appears to be an isolated incident. In addition, all other controls that involved a level of management review operated effectively during the period. As such, the identified deficiency does not appear to indicate other control deficiencies.

Step 4: Evaluate the severity of the deficiency individually (consider the magnitude and likelihood of it resulting in a material misstatement)

Key reminders about Step 4:

1. Evaluate whether there is a reasonable possibility that a material misstatement could occur as a result of a deficiency. ***Reasonable possibility* means more than a remote likelihood** of a material misstatement**.**

2. Remember: if the deficiency resulted in a misstatement in the financial statements, the amount of the misstatement is the floor when determining its magnitude. In many cases, the **magnitude of the potential misstatement is greater than the floor.**

3. Remember: the magnitude of a potential misstatement is **not limited** by the assertion that ‘management has learned its lesson,’ ’reviews are more thoroughly performed when the stakes are higher,’ or other such sentiments.

4. Consider the **volume of activity** in the account balance or class of transactions exposed to the deficiency **in the current period** and that is expected **in future periods** as well as the indirect effects of the potential

Key reminders about Step 4:

misstatement (e.g. on compliance with debt covenants, stock compensation arrangements).

5. **Use the flowcharts** in the appendices C.1 and C.2 to the ICFR Handbook to assist you through the steps of determining the severity of the deficiency.

6. As part of the severity assessment, **consider the control's objective** (e.g. the PRP(s) or RAFIT(s) that the control was purported to address) and how that control relates to the entire process and relevant financial statement assertions.

Factors in evaluating severity (including reasonable possibility and magnitude of potential misstatement):

(When evaluating the severity, consider:

- *Was a financial statement misstatement identified? If so, what was the amount? Has it been determined that the actual misstatement is the highest potential magnitude? If so, that would be uncommon.*
- *The magnitude of the significant account affected. Is the effect of the deficiency limited to a portion of the significant account balance? If so, why?)*

The deficiency and its root cause do not relate to one of the four indicators of material weakness (as per SEC Staff guidance and paragraph 69 of PCAOB AS 2201).

The following are the pension-related account balances as of and for the year-ended December XX, 20X3 (materiality is $5 million):

- Postretirement benefits liabilities - $50 million
- Postretirement benefits expense - $5 million
- Postretirement amounts impacting other comprehensive income/loss - $6 million.

When considering the potential magnitude of an error resulting from this deficiency, we noted that historical changes to the discount rate have never exceeded +/- 500 basis points from year-to-year. A bigger change would be unlikely, particularly given that management has effective risk assessment controls to identify external industry/environmental/economic factors that might be the source of any unlikely change.

As such, management believes that the +/- 500 basis points represents a reasonable fence whereby movement in the discount rate outside that range would prompt additional follow-up by the entity's personnel and its actuary such that the likelihood of material misstatement in excess of that amount would be remote. The discount rate is used to measure the projected benefit obligation (PBO) and accumulated benefit obligation (ABO) and also the service and interest cost components of the postretirement benefit expense; service cost on the obligation was $3 million and interest cost approximately $1 million during 20X3.

Further, while the sensitivity of pension obligations to changes in the discount rate is high as a result of the way in which changes in the discount rate ultimately flow through to expense, the effect on expense is far less. Management performed a sensitivity analysis that suggests a change in the discount rate of +/- 500 basis points would represent approximately a $1 million change in the pension expense.

We also noted that, with recent changes in the bond market and through discussion with the entity’s and KPMG’s actuaries, it is expected that the discount rate may continue to rise and its increase over time may exceed the 500 basis points in the foreseeable future. That said, chances are remote that it would exceed a 1,000 basis point increase in the foreseeable future (resulting in approximately a $2 million misstatement).

Given the potential effect, the identified deficiency is not a material weakness. However, it does appear to be of sufficient magnitude that the audit committee would want to be informed of the matter. Therefore, it is considered a significant deficiency before consideration of the effect of any compensating controls.

Step 5: Evaluate the effect of compensating controls and conclude on the severity of the individual control deficiency

Key reminders about Step 5:

1. Remember: to have a mitigating effect, the compensating control should operate at a level of precision that **would** prevent, or detect and correct on a timely basis, a material misstatement of the account affected by the deficiency.

2. Remember: **high-level analytical procedures** and other monitoring controls generally **do not make effective compensating controls**.

3. When relying on a compensating control to limit the severity of an identified deficiency, **evaluate the design and operating effectiveness of the compensating control**. Compensating controls should be part of management’s control process to be considered a compensating control.

Key reminders about Step 5:

4. Consider whether the compensating control **meets the same control objective** (e.g. it addresses the same PRP(s) or RAFIT(s)) and addresses the same period of time as the deficient control.

5. Remember: a compensating control **does not eliminate a control deficiency**, but it might limit the severity of a deficiency.

Compensating controls:

(Discuss which compensating control(s) were identified, how the compensating control(s) address the same PRP(s) or RAFIT(s) as the deficient control, and to what degree the compensating control(s) reduce the severity of the deficiency.)

None identified.

Conclusion on the individual deficiency (Material Weakness, Significant Deficiency, or Deficiency):

Significant Deficiency

Internal control deficiency evaluation – Example 2

NOTE: The deficiency evaluation documented below is for example purposes only and is not intended to be a comprehensive illustration of all factors which may need to be considered in evaluating the severity of a control deficiency. When using this example, professional judgment needs to be used in applying concepts and evaluating considerations relative to the specific circumstances of the entity, which may not be directly analogous to the facts and circumstances that serve as the basis for this example. For instance, this example assumes that no other controls were affected by the lack of appropriate communication that led to the failure of the control evaluated in this example.

Step 1: Determine whether a control deficiency exists and identify the deficient control

Key reminders about Step 1

1. Remember: **a deficiency represents the potential for misstatement.** Therefore, a deficiency can exist in the absence of a misstatement and such deficiency may be a significant deficiency or a material weakness.

2. Remember: generally, **a misstatement in the financial statements would not exist without a deficiency** that permitted it to occur. Therefore, each misstatement identified in connection with an external audit is likely to have a related deficiency.

3. **Consider the nature and extent of the remediation plan**. Remediation plans are helpful in more precisely identifying and describing a deficiency.

4. Remember: deficiencies in **controls at service organizations** represent deficiencies in the user entity's ICFR when management relies on these controls for the entity's ICFR.

5. Describe the deficiency in terms of (1) the **control**; and (2) whether the control was **missing, designed inappropriately**, or **operating ineffectively.**

6. **Avoid describing** the deficient control **in terms of the error**. **The error is not the deficiency**; the control that failed to detect or prevent the error is the deficiency.

Determine whether a control deficiency exists:

(Describe the situation that led to considering whether a deficiency exists, the factors assessed, and the conclusion. If no deficiency exists, do not continue to Step 2.)

The external auditors discovered, and we concur, that our legal contingency reserve was overstated by $500 thousand. Given that there is an audit difference, we determined that there is a control deficiency.

Identification of the control that failed:

(Describe the deficient control. The deficient control should not be described in terms of the error in the financial statements. Also, indicate whether the control is missing, designed improperly, or not operating effectively.)

The deficient control is:

Review of the legal contingency reserve by the General Counsel (GC) to determine whether asserted and unasserted matters are probable, reasonably possible, or remote – and if probable – whether the contingency reserve is an appropriate amount.

On a quarterly basis, the entity's GC reviews the status of the asserted and unasserted legal claims, and the proposed contingency reserve amounts on a matter-by-matter basis. The paralegal staff maintain a summary to facilitate the GC's review. In preparing the matter-by-matter summary, the paralegal discusses each matter with the responsible attorney (including an assessment as to the probable cost of settlement) to determine that the summary is up to date.

The control did not operate effectively in two ways:

1. The summary presented to the GC for review was inaccurate with respect to one matter — namely, the effect of a settlement negotiated with reference to the matter was not reflected on the schedule. The schedule indicated that a loss was probable and an amount was reserved; however, the negotiated settlement was $500 thousand less than anticipated and less than the amount that was included in the summary reviewed by the GC.

2. Even though the information provided to the GC was inaccurate, his review is supposed to detect and correct such inaccuracies. It did not.

Step 2: Understand the cause of the deficiency

Key reminders about Step 2:

1. **Perform a root cause analysis** to determine the cause of the control deficiency.

2. Ask 'why' questions to peel back the layers of the deficiency to get to what really caused the deficiency.

3. Identify the **COSO component and principle** that the deficient control affected.

Root cause of the control deficiency:

(Describe the root cause of the control deficiency.)

1. The paralegal did not update the summary of legal matters in a timely manner. The settlement occurred on the second to last day of the quarter. The paralegal had made inquiries of the responsible attorneys a week before the end of the quarter. The best information at that time was that the entity was going to settle for $500 thousand more than it settled for. There was no additional communication between the responsible attorney and the paralegal once the settlement was finalized and, as a result, the summary of legal matters did not reflect the most current relevant information about the settlement at the time of GC's review of the legal contingency reserve. Deficiencies in controls over C&A of information generally relate to the Information and Communication (I&C) component of ICFR, specifically COSO Principle 13. See additional discussion of whether this indicates other deficiencies in Step 3 below.

2. The GC's review of the legal matters did not detect the $500 thousand difference. We believe that it is evident that the GC spends a considerable amount of time focused on whether the legal matters are complete and whether the matters are probable, reasonably possible, or remote. Given that most of the matters do not fall in the probable category, his review of the legal accrual amounts was not as comprehensive as his review of completeness and probability. This is consistent with the fact that neither we nor the external auditors found any issues with respect to the control operating to identify all legal matters or to consider the probability of the matters. The GC is qualified and capable of performing the review. Although the schedule of legal matters given to him to review was inaccurate, given his knowledge of the recent settlement, he should have detected and corrected the overstatement. This indicates a deficiency in the effectiveness of the

review (COSO Principle 12). See additional discussion of whether this deficiency may be indicative of other deficiencies in Step 3 below.

Step 3: Determine whether the deficiency is indicative of other deficiencies

Key reminders about Step 3:

1. **Look for commonalities** – the same type of control deficiency may exist in similar controls.

2. Be aware that the control deficiency may indicate a **broader issue** in **another component or principle** of internal control.

Does the control deficiency indicate other deficiencies?

(Based on the identification of the control that failed, including the root cause analysis performed in Step 2, consider whether: (1) the same type of control deficiency may exist in similar controls and (2) the control deficiency may indicate a more pervasive issue in another component or principle of internal control.)

The first issue related to the deficiency is the completeness and accuracy (C&A) of the information used in the control — in this case, the summary of legal matters maintained by the paralegal was inaccurate. As stated in Step 2 above, deficiencies in controls over C&A of information generally relate to the I&C component of ICFR. We considered whether this issue could arise in other areas where the entity uses information. We reviewed our process narratives to determine that we had identified all information used in the operation of controls. We considered our testing of the design and operating effectiveness of the controls over the completeness and accuracy of the information used in other controls. We noted no deficiencies in these controls.

Further, management is of the view that it understands the importance of having controls over the C&A of information. This particular deficiency, related to the legal accrual, is unique from other controls over C&A because the information does not come from the enterprise resource planning (ERP) system. Rather, the paralegal discusses each matter with the responsible attorney and maintains the schedule in an Excel file.

Based on the above considerations, we noted no other deficiencies in controls over the C&A of information used in controls and, accordingly, there are no indicators of a deficiency in the overall I&C component of ICFR.

The second issue relates to the sufficiency of the GC's review. We note the following with reference to the issue:

1. We reviewed all management review controls and noted no similar deficiency related to the C&A of information. We did note a deficiency related to I&C in the area of pensions, but it seems to have a different root cause than this deficiency. (*Note: whether we determine that they are sufficiently similar here, or whether we determine that they are not sufficiently similar here but aggregate the I&C deficiencies in Step 6 of the deficiency evaluation process, the ending severity determination should be the same.*)

2. We reviewed all other controls that the GC is involved in, noting that they are all controls related to committee reviews (such as the disclosure committee review of the financial statements). All these other controls operated by/involving the GC were tested and deemed to be effective.

Based on the above rationale, this deficiency does not appear to indicate other deficiencies.

Step 4: Evaluate the severity of the deficiency individually (consider the magnitude and likelihood of it resulting in a material misstatement)

Key reminders about Step 4:

1. Evaluate whether there is a reasonable possibility that a material misstatement could occur as a result of a deficiency. ***Reasonable possibility* means more than a remote likelihood** of a material misstatement**.**

2. Remember: if the deficiency resulted in a misstatement in the financial statements, the amount of the misstatement is the floor when determining its magnitude. In many cases, the **magnitude of the potential misstatement is greater than the floor.**

3. Remember: the magnitude of a potential misstatement is **not limited** by the assertion that 'management has learned its lesson,' 'reviews are more thoroughly performed when the stakes are higher,' or other such sentiments.

4. Consider the **volume of activity** in the account balance or class of transactions exposed to the deficiency **in the current period** and that is expected **in future periods** as well as the indirect effects of the potential misstatement (e.g. on compliance with debt covenants, stock compensation arrangements).

Key reminders about Step 4:

5. **Use the flowcharts** in the appendices C.1 and C.2 to the ICFR Handbook to assist you through the steps of determining the severity of the deficiency.

6. As part of the severity assessment, **consider the control's objective** (e.g. the PRP(s) or RAFIT(s) that the control was purported to address) and how that control relates to the entire process and relevant financial statement assertions.

Factors in evaluating severity (including reasonable possibility and magnitude of potential misstatement):

(When evaluating the severity, consider:

- *Was a financial statement misstatement identified? If so, what was the amount? Has it been determined that the actual misstatement is the highest potential magnitude? If so, that would be uncommon.*
- *The magnitude of the significant account affected. Is the effect of the deficiency limited to a portion of the significant account balance? If so, why?)*

The potential magnitude of the overall legal contingency reserve is material to the annual financial statements as completeness is a relevant assertion related to the legal contingency reserve. The total legal contingency reserve at year-end is $7 million relative to a materiality of $5 million. The actual legal contingency reserve adjustment of $500 thousand represents the floor for determining the potential magnitude; the potential or ceiling without consideration of other factors would be higher.

The following factors are critical to evaluating whether the potential magnitude is material and assessing the likelihood:

- The total reserve at year-end is slightly higher than materiality and the identified misstatement was an overstatement (however, the root cause of the deficiency suggests that risk of both under- and overstatement exists).
- The volume of total unasserted and asserted matters is 20 in total.
- Of the 20 cases, only 4 matters are deemed to be probable. As noted above, the ineffectiveness of the control is limited to the determination of the reserve, not the classification of the matters being probable, reasonably possible, or remote.
- The four matters have estimated losses of $1 million, $1.5 million, $2.0 million, and $2.5 million.

- The legal accrual has been between $5 million and $8 million for the past four years.
- Many of the cases transpire over a multi-year timeline and developments that would prompt changes in the accrual are infrequent. It is unlikely that all four matters would have major developments in the same quarter. These four matters have been ongoing for a while — ranging from 6 to 60 months.

Based on these facts, it does not appear likely that a $5 million error would occur in the legal accrual. In fact, it would appear unlikely that an error greater than $2 million would occur in any given period because of the historical range of the legal accrual, the nature of the matters, and the low likelihood that each of the four matters would have developments that would cause the accrual to change all in the same period. We believe that a prudent official would deem the *ceiling* to be less than $2 million based on these facts.

Step 5: Evaluate the effect of compensating controls and conclude on the severity of the individual control deficiency

Key reminders about Step 5:

1. Remember: to have a mitigating effect, the compensating control should operate at a level of precision that **would** prevent, or detect and correct on a timely basis, a material misstatement of the account affected by the deficiency.

2. Remember: **high-level analytical procedures** and other monitoring controls generally **do not make effective compensating controls**.

3. When relying on a compensating control to limit the severity of an identified deficiency, **evaluate the design and operating effectiveness of the compensating control**. Compensating controls should be part of management’s control process to be considered a compensating control.

4. Consider whether the compensating control **meets the same control objective** (e.g. it addresses the same PRP(s) or RAFIT(s)) and addresses the same period of time as the deficient control.

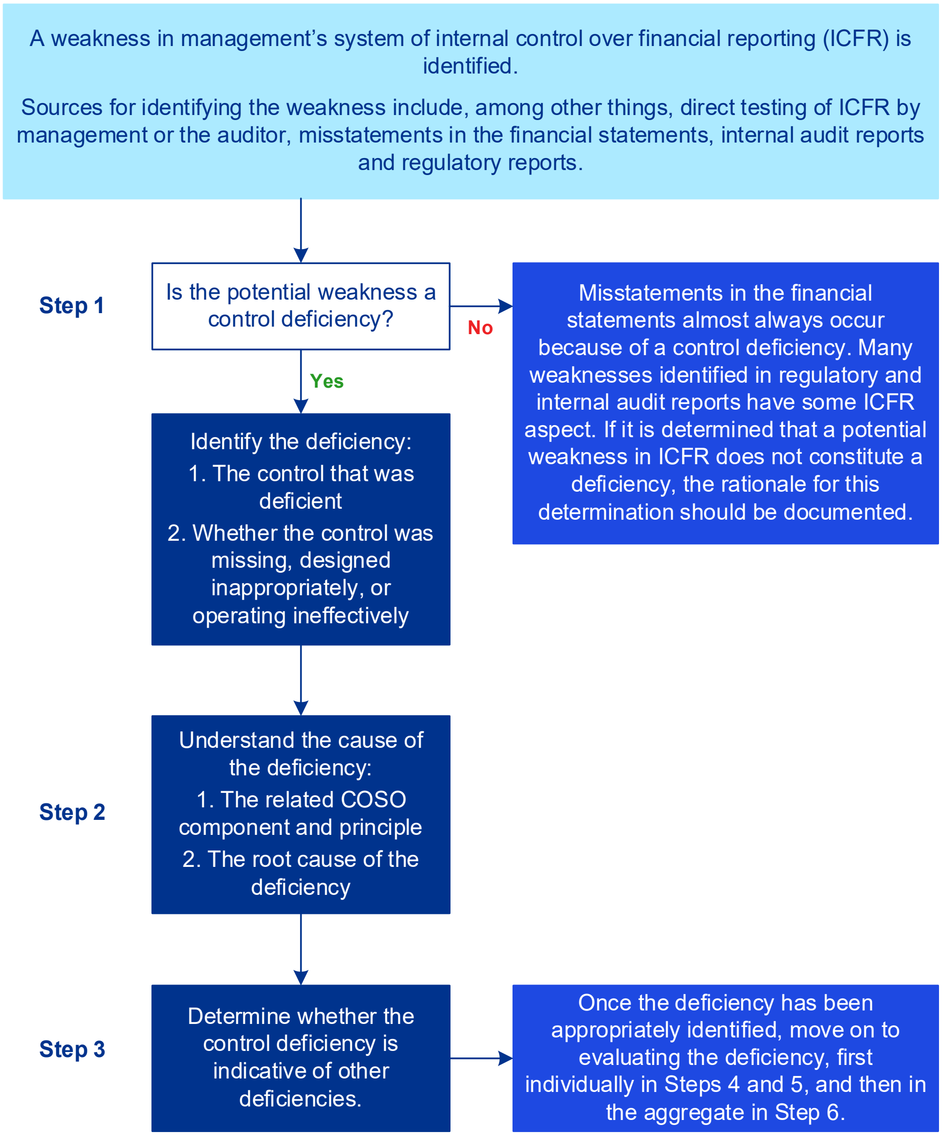
5. Remember: a compensating control **does not eliminate a control deficiency**, but it might limit the severity of a deficiency.

Compensating controls:
(Discuss which compensating control(s) were identified, how the compensating control(s) address the same PRP(s) or RAFIT(s) as the deficient control, and to what degree the compensating control(s) reduce the severity of the deficiency.) There may be some compensating controls, such as the CFO and Audit Committee's review of the legal accrual (that occurs in conjunction with all significant estimates). While such controls did not detect the $500 thousand error, they may detect a $5 million error. However, we have already determined that it is not likely that a material misstatement would occur in the legal accrual and, therefore, we do not place significant weight on the compensating controls and will not further consider whether they are sufficiently precise to compensate for the deficiency in the GC's review of the legal reserve as we determine the severity of the deficiency. Taking into account the severity assessment, we have concluded that the identified deficiency does not rise to the level of a material weakness. However, it does appear to be of sufficient magnitude that the audit committee would want to be informed of the matter.

Conclusion on the individual deficiency (Material Weakness, Significant Deficiency, or Deficiency):
Significant Deficiency

Appendix C.1

Flowchart for identifying and evaluating deficiencies – Phase 1



A weakness in management's system of internal control over financial reporting (ICFR) is identified.

Sources for identifying the weakness include, among other things, direct testing of ICFR by management or the auditor, misstatements in the financial statements, internal audit reports and regulatory reports.

Step 1

Is the potential weakness a control deficiency?

No

Misstatements in the financial statements almost always occur because of a control deficiency. Many weaknesses identified in regulatory and internal audit reports have some ICFR aspect. If it is determined that a potential weakness in ICFR does not constitute a deficiency, the rationale for this determination should be documented.

Yes

Identify the deficiency:

1. The control that was deficient
2. Whether the control was missing, designed inappropriately, or operating ineffectively

Step 2

Understand the cause of the deficiency:

1. The related COSO component and principle
2. The root cause of the deficiency

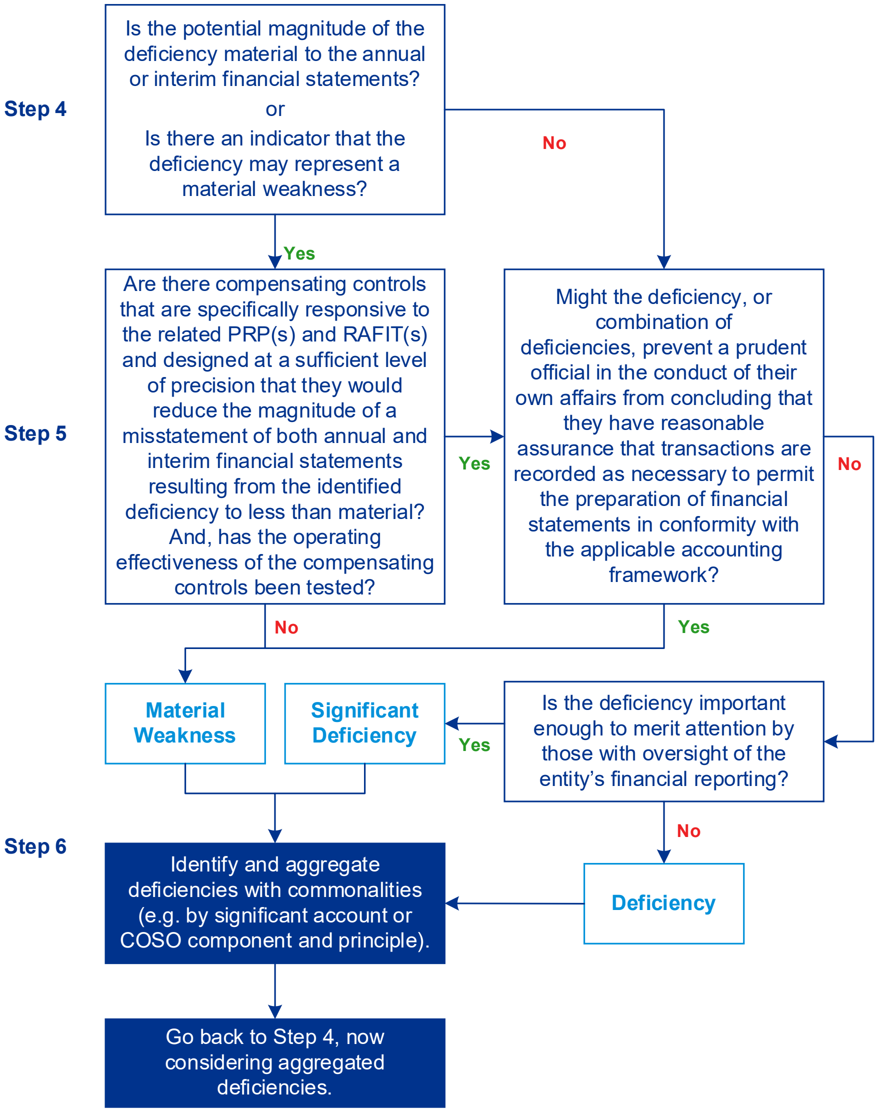
Step 3

Determine whether the control deficiency is indicative of other deficiencies.

Once the deficiency has been appropriately identified, move on to evaluating the deficiency, first individually in Steps 4 and 5, and then in the aggregate in Step 6.

Appendix C.2

Flowchart for identifying and evaluating deficiencies – Phase 2



Is the potential magnitude of the deficiency material to the annual or interim financial statements?

or

Is there an indicator that the deficiency may represent a material weakness?

Are there compensating controls that are specifically responsive to the related PRP(s) and RAFIT(s) and designed at a sufficient level of precision that they would reduce the magnitude of a misstatement of both annual and interim financial statements resulting from the identified deficiency to less than material? And, has the operating effectiveness of the compensating controls been tested?

Might the deficiency, or combination of deficiencies, prevent a prudent official in the conduct of their own affairs from concluding that they have reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in conformity with the applicable accounting framework?

Material Weakness

Significant Deficiency

Is the deficiency important enough to merit attention by those with oversight of the entity's financial reporting?

Deficiency

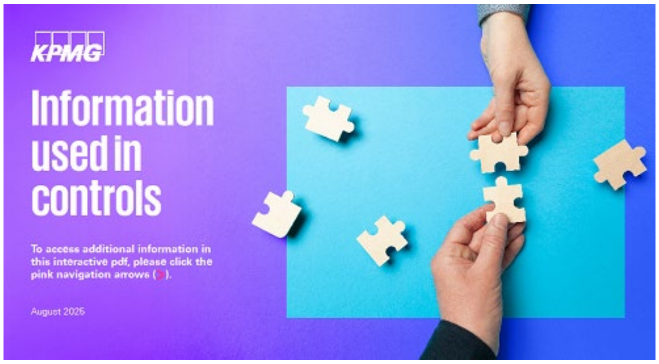
Identify and aggregate deficiencies with commonalities (e.g. by significant account or COSO component and principle).

Go back to Step 4, now considering aggregated deficiencies.

Appendix D

Information used in controls

This interactive PDF summarizes guidance specific to identifying, evaluating, and documenting the information used in internal controls in an easy-to-use document to support management in their evaluation of information that they are using in controls.



KPMG

Information used in controls

To access additional information in this interactive pdf, please click the pink navigation arrows ( ).

August 2025

Appendix E

Precision in practice – documenting precision of controls

This interactive PDF summarizes guidance specific to evaluating and documenting the precision of internal controls in the ACL process and can be used to support management as they design and implement such controls. While focused on the ACL process, the concepts presented are equally applicable to controls over other significant estimates addressed in financial reporting.

Precision in practice— Documenting precision of controls

To access additional information in this interactive pdf, please click the pink navigation arrows (>).

May 2025

Appendix F

What's new

This appendix highlights key changes reflected in this Handbook as compared with its previous version released in 2023.

Overall, the changes are limited in nature and scope and are focused on the following areas:

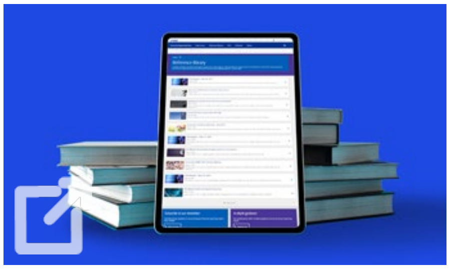
- updates to the discussion of management's responsibilities related to cybersecurity risks and incidents to reflect recent changes in the SEC rules related to cybersecurity disclosures and other developments, and to move what was Question 7.6.50 to be Question 7.6.90 (see section 7.6);
- addition of a new chapter on the use of AI and automation and its impacts on management's ICFR responsibilities (see chapter 10);
- addition of Appendix D, which includes a user-friendly interactive PDF that summarizes the contents of the Handbook related to identifying, evaluating, and documenting the information used in internal controls; and
- addition of Appendix E, which includes an interactive PDF that summarizes key considerations related to precision of internal controls in the ACL process.

KPMG Financial Reporting View

Delivering guidance and insights, KPMG Financial Reporting View is ready to inform your decision making. Stay up to date with us.

Defining Issues

Our collection of newsletters with insights and news about financial reporting and regulatory developments, including Quarterly Outlook and FRV Weekly.



Handbooks and Hot Topics

Our discussion and analysis of accounting topics – from short Hot Topics that deal with a topical issue, to our in-depth guides covering a broad area of accounting.

CPE opportunities

Register for live discussions of topical accounting and financial reporting issues. CPE-eligible replays also available.

Financial Reporting Podcasts

Tune in to hear KPMG professionals discuss major accounting and financial reporting developments.

Visit **Financial Reporting View**
and **sign up** for news and insights

Access our US Handbooks

As part of Financial Reporting View, our library of in-depth guidance can be accessed here, including the following Handbooks.

- Accounting changes and error corrections
- Accounting for economic disruption
- Asset acquisitions
- Bankruptcies
- Business combinations
- Business combinations (SEC reporting)
- Climate risk in the financial statements
- Consolidation
- Contingencies, commitments and guarantees
- Credit impairment
- Debt and equity financing
- Derivatives and hedging
- Discontinued operations and held-for-sale disposal groups
- Earnings per share
- Employee benefits
- Equity method of accounting
- Fair value measurement
- Financial statement presentation
- Foreign currency
- GHG emissions reporting
- Going concern
- IFRS® compared to US GAAP
- Impairment of nonfinancial assets
- Income taxes
- Internal control over financial reporting
- Inventory
- Investment companies
- Investments
- Leases
- Long-duration contracts
- Reference rate reform
- Research and development
- Revenue recognition
- Revenue: Real estate
- Revenue: Software and SaaS
- Segment reporting
- Service concession arrangements
- Share-based payment
- Software and website costs
- Statement of cash flows
- Tax credits
- Transfers and servicing of financial assets

Learn about us: | **kpmg.com**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.