ICOFR reference guide
What’s new in the 2016 version of the ICOFR reference guide?

**Chapter 1 Introduction**

1. Overview of an ICOFR Assessment – A Risk-Based Approach
2. Definition of Internal Control and SEC Regulations
3. The COSO Framework

**Chapter 2 Documentation**

2.1 Documentation Requirements

**Chapter 3 Control environment**

3.1 Principles of an Effective Control Environment
3.2 The Impact of the Control Environment on ICOFR

**Chapter 4 Risk assessment**

4.1 Principles of an Effective Risk Assessment
4.2 Principle 6: Setting the Objective
4.3 Principle 7: Identifying and Analyzing Risks
4.4 Principle 8: Identifying and Assessing Fraud Risks
4.5 Principle 9: Identifying and Assessing Significant Changes

**Chapter 5 Risk assessment – understanding WCGWS**

5.1 Understanding the Process
5.2 Identifying the What Could Go Wrongs (WCGWs)
5.3 IT Considerations When Understanding the Process Activities
5.4 Documentation Considerations

**Chapter 6 Control activities**

6.1 Principles of Effective Control Activities
6.2 Selecting, Developing, and Deploying – Control Activities
6.3 Relationship of Control Activities to Other COSO Framework Components

**Chapter 7 Management review controls**

7.1 Identification and Classification of Management Review Controls (MRCs)
7.2 Test of Design
7.3 Information Produced by the Entity
7.4 Evaluating Operating Effectiveness

© 2016 KPMG LLP a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 580828
Chapter 8 Understanding and responding to information technology (IT) risks

8.1 IT Considerations in Planning 174
8.2 Understanding Process-Level Activities and Related Risks 178
8.3 What are Process-Level Automated Controls and How are They Relevant to ICOFR? 182
8.4 Identifying, Linking, and Testing GITCs 193
8.5 End-User Computing (EUC) 203
8.6 Considerations When a GITC Deficiency is Identified 205
Appendices 210

Chapter 9 Information and Communication 211

9.1 Principles of Effective Information and Communication 213

Chapter 10 Monitoring 218

10.1 Principles of Effective Monitoring 220
10.2 Methods Available to Management to Monitor 225
10.3 Monitoring Components Other than Control Activities 231
10.4 Distinguishing between Monitoring Activities and Control Activities 232
10.5 External Auditor Reliance on Monitoring and General Documentation Considerations 235

Chapter 11 Identifying and Evaluating Deficiencies 238

11.1 Step 1: Determine Whether a Control Deficiency Exists 240
11.2 Step 2: Identify the Deficient Control by Performing a Root Cause Analysis 243
11.3 Step 3: Determine Whether the Deficiency Is Indicative of Other Deficiencies 248
11.4 Step 4: Evaluate the Severity of the Deficiency 252
11.5 Step 5: Identify Relevant Compensating Controls and Conclude on the Severity 261
11.6 Step 6: Aggregate Similar Deficiencies and Evaluate for Severity 265
11.7 Example of the Six-Step Process 268
11.8 Other Considerations 271
11.9 Key Points Regarding SEC Form 10-K, Item 9A Disclosures 272
11.10 Considerations for Deficiencies Identified at an Interim Period 276
Appendices 278

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of
the KPMG network of independent member firms affiliated with KPMG International
Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name
and logo are registered trademarks or trademarks of KPMG International. NDPPS 588628
What’s new in the 2016 version of the ICOFR reference guide?

The summary below highlights key changes in the ICOFR Reference Guide (the Guide) from the previous version released in 2014. It does not include each individual change made to the Guide, many of which were editorial in nature and do not represent key changes. Users are encouraged to read the Guide early in the audit of ICOFR, focusing on understanding each of the concepts contained in the Guide as opposed to isolated paragraphs or illustrations highlighted as changes below.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Reference</th>
<th>Description of Key Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughout</td>
<td>Throughout</td>
<td>Updates throughout the Guide to illustrate the emphasis being placed by the SEC on management’s assessment of ICOFR and by the PCAOB on our audit of ICOFR.</td>
</tr>
<tr>
<td>1</td>
<td>Section 1.2</td>
<td>Expanded guidance on the scope of management’s ICOFR assessment.</td>
</tr>
<tr>
<td>2</td>
<td>Section 2.1</td>
<td>Enhanced guidance on the consideration of the evidence necessary to evaluate the effective operation of controls, including the correlation of that evidence with the assessed level of risk.</td>
</tr>
<tr>
<td>7</td>
<td>Section 7.1</td>
<td>Enhanced guidance on the importance of Management Review Controls (MRCs) and evidential matter necessary to conclude an MRC is capable of achieving its objective, including considerations to document the precision of an MRC 1 and clarified illustrations.</td>
</tr>
<tr>
<td>Section 7.2</td>
<td>Paragraph 7.2.240</td>
<td>Enhanced guidance on the importance of established criteria for investigation in determining the precision of an MRC and expanded discussion on the precision factors introduced in PCAOB SAPA 11.</td>
</tr>
<tr>
<td>Section 7.3</td>
<td></td>
<td>Expanded guidance and illustrations on controls over completeness and accuracy of IPE, procedures to assess those controls, and potential differences between management’s procedures and our approach to testing those controls.</td>
</tr>
<tr>
<td>11</td>
<td>Section 11.1 Section 11.3</td>
<td>New and expanded illustrations on determining whether a control deficiency exists and on evaluating the severity of a deficiency, including its likelihood and potential magnitude. Additionally, new guidance and illustrations to demonstrate the emphasis the SEC is placing on management’s assessment of ICOFR.</td>
</tr>
</tbody>
</table>

1 PCAOB Staff Audit Practice Alert No. 11 – Considerations for Audits of Internal Control Over Financial Reporting (October 2013) pages 20-25
Chapter 1
Introduction
This chapter discusses the importance of following a **risk-based approach** to the evaluation of internal control. Subsequent ICOFR Reference Guide chapters describe key aspects of this risk-based approach in greater detail.

Although a risk-based approach to evaluating internal control can be described as sequential, if properly performed, it is really an iterative process. Each successive step of the process adds to the total body of evidence considered. This cumulative body of evidence causes management and auditors to reassess initial conclusions as new evidence is obtained throughout the assessment. Following a risk-based approach allows management and external auditors to focus more attention on the areas presenting the highest degree of risk.

This chapter also describes the objective of internal control over financial reporting (ICOFR) as established by the SEC. It explains which entities are subject to ICOFR reporting, clarifies which entities are required to provide management’s assessment on ICOFR, and which entities are required to provide both management’s and the external auditor’s assessment on ICOFR.

Finally, this chapter briefly describes some of the key aspects of the COSO Framework, the most commonly used ICOFR framework. Subsequent chapters discuss components, principles, and other relevant aspects of the COSO Framework in more depth.
Management and, if applicable, external auditors, need to determine whether the entity maintained, in all material respects, effective ICOFR as of a specified date, based on the criteria established by a suitable framework. Nearly all U.S. registrants use the Internal Control – Integrated Framework published by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission as the framework.

Management reports its assessment of the effectiveness of the entity’s ICOFR as of the entity’s most recent fiscal year-end. The external auditor provides a separate opinion about the effectiveness of ICOFR, rather than opining on management’s ICOFR assessment. However, to obtain sufficient evidence that all components and principles are present and functioning the external auditor will need to not only test the Control Activities, but also understand management’s assessment, particularly as it relates to Control Environment, Risk Assessment, Information & Communication and Monitoring.

To assess the effectiveness of ICOFR as of a point in time, management and external auditors obtain evidence that ICOFR has operated effectively for a sufficient period of time, which may be less than the period covered by the financial statement audit report. To express an opinion on ICOFR, management and external auditors obtain evidence about the effectiveness of selected controls over all relevant assertions.

The SEC Staff guidance recommends that management follow a risk-based approach to assessing ICOFR. The PCAOB’s Auditing Standard (AS) No. 5 paragraph 21 states that the auditor should follow a risk-based approach to select controls to test in an ICOFR audit. Following a risk-based approach allows management and external auditors to identify the areas of highest risk and focus more attention on those areas. The SEC Staff guidance and AS No. 5 paragraph 11 both state that greater effort should be devoted to areas with higher risk of material misstatement, including fraud risk.

An effective risk-based approach is a cumulative, iterative process, not a linear process. It begins at the planning and scoping phase, with identifying and understanding significant accounts, disclosures and assertions that present a reasonable possibility of material misstatement to the financial statements.

It then continues with obtaining an understanding of the Control Environment, and considering its impact on the rest of the system of ICOFR. See chapter 3 of the ICOFR Reference Guide – Control Environment.

Based on the procedures performed over entity-level controls, an assessment is made of the risk of material misstatement for relevant financial statement account assertions. See chapter 5 of the ICOFR Reference Guide – Risk Assessment. Once the risks are understood, the design and implementation of relevant controls are evaluated. When selecting relevant controls and performing that evaluation, consider the precision of the control’s design in relation to the “what could go wrongs” that the control is intended to prevent, or detect and correct. See chapters 6 – 9 of the ICOFR Reference Guide.

“Preparers must recognize that management’s ability to fulfill its financial reporting responsibilities significantly depends on the design and effectiveness of internal control over financial reporting…. We now generally hear from stakeholders that ICFR requirements of the Sarbanes-Oxley Act have resulted in improved controls and financial reporting.

It is hard to think of an area more important than ICFR to our shared mission of providing high-quality financial information that investors can rely on…. ICFR must remain the strong bulwark of reliable financial reporting that it has become.”

Mary Jo White, SEC Chair
The operating effectiveness of those controls that sufficiently address the assessed risks of material misstatement for each relevant assertion is monitored. See chapter 10 of the ICOFR Reference Guide – Monitoring.

Finally, the severity of any identified deficiencies is assessed and a conclusion is made on the effectiveness of ICOFR. See chapter 11 of the ICOFR Reference Guide – Identifying and Evaluating Control Deficiencies.

Although the risk-based approach is described here as a sequential thought process, it is really an iterative, cumulative process that requires a reassessment of initial conclusions based on evidence obtained throughout the assessment.

As discussed above, a risk-based approach includes assessing the risks of material misstatement and selecting relevant controls for testing. Once management and external auditors have obtained a sufficient understanding of the process and risks, they may find that testing “higher level controls” (HLCs), or controls that operate over multiple processes, is less effective than testing process-level controls. HLCs are often not designed to operate with sufficient precision to prevent (detect and correct) a material misstatement related to the financial statement assertions at the account level. See chapter 7 of the ICOFR Reference Guide – Management Review Controls for more discussion of precision of HLCs.
[1.2.10] According to SEC Rules and Regulations, management must evaluate the effectiveness of the issuer’s ICOFR as of the end of each fiscal year. The SEC defines ICOFR as follows:

— "A process designed by, or under the supervision of, the issuer’s principal executive and principal financial officers, or persons performing similar functions, and effected by the entity's board of directors, management, and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles (GAAP) and includes those policies and procedures that:

– Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the issuer;
– Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with GAAP, and that receipts and expenditures of the issuer are being made only in accordance with authorizations of management and directors of the issuer; and
– Provide reasonable assurance regarding the prevention or timely detection of unauthorized acquisition, use or disposition of the issuer’s assets that could have a material effect on the financial statements.” [Regulations 13a-15(f) and 15d-15(f) of the Securities Exchange Act]

[1.2.20] Management must provide its assessment of the effectiveness of ICOFR as of the end of the most recent fiscal year in its annual report on Form 10-K, or in the case of foreign private issuers, on Form 20-F or 40-F. A management report is required for all registrants that file with the SEC except for newly public companies or entities as discussed in paragraph 1.2.60. This requirement is applicable to entities who file voluntarily; file because of registered debt; or file as a smaller reporting entity, non-accelerated filer, accelerated filer, large accelerated filer or as an emerging growth company as defined by the Jumpstart Our Business Startups Act (JOBS Act).

[1.2.30] Management must provide the auditor attestation report on the registrant’s ICOFR if the registrant is an accelerated filer or a large accelerated filer. Domestic and foreign smaller reporting companies, non-accelerated filers and emerging growth companies are not required to include an auditor attestation report under Regulation S-K 308(b). Management should consult with their SEC counsel to determine their ICOFR reporting requirements.

[1.2.40] During interim periods, management must identify and disclose any change in the registrant’s ICOFR that occurred during the quarter being reported on that has materially affected, or is reasonably likely to materially affect, its ICOFR. This includes the fourth quarter. Such changes in ICOFR are not expected to be rare events.

[1.2.50] Management’s report on ICOFR and the accompanying auditor attestation report are not required in registration statements (whether those are filed under the 1933 Securities Act or the 1934 Securities Exchange Act) or Forms 11-K.

3 Regulation S-K 308(b)
4 Regulation S-K 308(b)
5 SEC Financial Reporting Manual 4310.1
[1.2.60] A newly public entity is required to provide management’s report on ICOFR in the year that follows its initial public offering and after filing its first Form 10-K (or Forms 20-F or 40-F) with the SEC (the IPO grace period). A newly public entity also receives the same IPO grace period related to the auditor’s ICOFR attestation report. In the first annual report on Form 10-K, the registrant should include a statement such as:

— “This annual report does not include a report of management’s assessment regarding internal control over financial reporting or an attestation report of the company’s registered public accounting firm due to the transition period established by the rules of the Securities and Exchange Commission for newly public companies.”\(^6\)

[1.2.70] However, the IPO grace period related to management’s report on ICOFR does not apply to a newly public entity that previously reported under the 1934 Securities Exchange Act voluntarily or because of registered debt, and was required to provide management’s report on ICOFR in accordance with Regulation S-K 308(a). This entity, as a newly public entity, must provide management’s report on ICOFR in its first annual report following the IPO (because it has already been providing management’s report on ICOFR). It will, however, receive the IPO grace period for the auditor’s attestation report because it did not meet the definition of an accelerated filer or a large accelerated filer (because it filed voluntarily or because of registered debt).

[1.2.80] The SEC Staff has stated that it would not object if a registrant did not disclose changes or improvements to ICOFR made in preparation for the registrant’s first management report on ICOFR. However, if the registrant were to identify a material weakness, it should carefully consider disclosing that fact as well as changes made in response to the material weakness.\(^7\)

[1.2.90] During the second fiscal year as a newly public entity, after the entity has filed its initial Form 10-K, management is required to identify and disclose any change in the issuer’s ICOFR that occurred during the issuer’s interim periods (or its fiscal year in the case of a foreign private issuer) that has materially affected, or is reasonably likely to materially affect, the issuer’s internal control over financial reporting.\(^8\)

[1.2.100] The SEC Staff has stated that it would typically expect management’s report on ICOFR to include controls at all consolidated entities, irrespective of the basis for consolidation. This includes, for example, controls at consolidated variable interest entities, controls that have been outsourced to a third party service provider by an entity in the consolidated group, or controls at a business presented as discontinued operations that remains consolidated as of the date of management’s assessment.\(^9\)

---

\(^6\) Instruction 1 to Regulation S-K 308
\(^8\) Regulation 13a-15(d)
\(^9\) See SEC 2007 FAQ Questions 1 and 8
[1.2.110] The SEC has provided clarification on its expectations of management’s report on ICOFR for certain items, including:

— An entity should have controls over recording its interest in an equity method investment, but is not required to have controls over the recording of transactions into the equity method investees accounts as the investment is not consolidated.\(^\text{10}\)

— The SEC Staff has stated it may not always be possible to assess an acquired entity’s ICOFR between the acquisition consummation date and the date of management’s assessment and it would not object to management excluding an acquired business from its report on ICOFR in the year of acquisition.\(^\text{11}\)

  In such instances, disclosure should be provided indicating the significance of the acquired business to the consolidated financial statements. The scope exception for a newly acquired business cannot be applied to the entity’s responsibility to maintain controls over the acquisition accounting and consolidation of the acquired business.

[1.2.120] SEC regulations require management to select a framework to evaluate the effectiveness of the issuer’s ICOFR as of the end of each fiscal year. The framework used by management must be a suitable, recognized control framework that is established by a body or group that followed due-process procedures, including broadly distributing the framework for public comment.

[1.2.130] While the SEC regulations do not specify the use of any particular control framework, the framework developed by COSO is commonly used by management of U.S. public companies to assess the effectiveness of ICOFR.

[1.2.140] Regulation SK-308 requires that management’s annual report on ICOFR include:\(^\text{12}\)

— A statement confirming management’s responsibility for establishing and maintaining adequate ICOFR for the registrant;

---

\(^\text{10}\) SEC 2007 FAQ Question 2
\(^\text{11}\) SEC 2007 FAQ Question 3
\(^\text{12}\) Management is also required to disclose whether its Disclosure Controls and Procedures (DCP) are effective. See chapter 11 of the ICOFR Reference Guide – Identifying and Evaluating Deficiencies for a discussion of DCP and its relationship to ICOFR. In addition, see chapter 11 for a discussion of how management should describe a material weakness, when one has been identified, and the related remediation plans.
— A statement identifying the framework used by management to evaluate the effectiveness of the registrant’s ICOFR;
— Management’s assessment of the effectiveness of the registrant’s ICOFR as of the end of the registrant’s most recent fiscal year, including a statement as to whether or not ICOFR is effective; and
— A statement by registrants who are accelerated filers or large accelerated filers that the registered public accounting firm that audited the financial statements has issued an attestation report on their ICOFR.

External References and Guidance:
SEC Regulations:
— Regulation S-K Item 308
— Regulation 13a-15

SEC Guidance:

SEC Frequently Asked Questions:
The Internal Control – Integrated Framework published by COSO (the COSO Framework) is a comprehensive, integrated framework that includes aspects that have either a direct or indirect relationship (or both) to financial statement assertions. Important aspects of the COSO Framework are embedded in AS No. 5. Various COSO components and principles are discussed throughout this ICOFR Reference Guide.

Since the COSO Framework was first issued in 1992 (the COSO 1992 Framework), it has gained broad acceptance and is widely used for designing, implementing and conducting internal control and for assessing the effectiveness of the internal control system. An effective system of internal control is expected to provide an entity with reasonable assurance that the objective of ICOFR will be achieved.

The COSO 1992 Framework was updated to reflect the changes in the business environment and operations over the last twenty years and was re-released in 2013 (the COSO 2013 Framework).

According to the COSO Framework, internal control is defined as “a process, effected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.”

The COSO Framework definition of internal control accommodates subsets of internal control over operations, financial and non-financial, internal and external reporting, and compliance with laws and regulations. The COSO Framework can be applied at various levels throughout the entity based on the entity-specific needs.

The COSO 2013 Framework, consistent with the COSO 1992 Framework, retains the definition of internal control and the COSO cube, including the three categories of objectives: Operations, Reporting, and Compliance with Laws and Regulations; and the five components of internal control: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities.

Although the COSO Framework has described certain objectives of internal control, the entity’s ICOFR objective is determined by the SEC, as described in paragraph 1.2.10.

The most significant change made in the COSO 2013 Framework, hereafter referred to as the COSO Framework, is the explicit codification of the 17 principles that support the five components. These principles establish the basis for an effective system of internal control designed to achieve the objectives established by management and the board of directors.

Determining whether a particular internal control system is “effective” requires subjective judgment. Under the COSO Framework, maintaining effective internal controls requires that:

1. Each of the five components and the 17 relevant principles be “present” and “functioning”; and
2. The five components must operate together in an integrated manner.
“Present” means that the components and relevant principles exist in the design and implementation of the system of internal control, and “functioning” means that the components and relevant principles continue to exist in the conduct of the system of internal control. Their effective functioning provides the reasonable assurance that the stated objectives are achieved. Not every organization has the same need to articulate all 5 components and/or 17 principles to the same intensity. In order for a component or principle to be effective, one organization may need more or stronger controls than another. All 17 principles are presumed to be relevant.

The COSO Framework does not set out which specific controls should be in place to ensure effective internal control. The Framework requires management and those charged with governance of the organization to use their judgment to establish the appropriate controls to provide reasonable assurance that objectives are met and risk is reduced to an acceptable level.

The COSO Framework provides example characteristics for each of the 17 principles, called points of focus, to help management determine if a principle is present and functioning. The Framework does not require users to implement controls to achieve each point of focus. However, users will find that the points of focus are useful to consider in the design of controls to achieve the relevant principle.

Chapters throughout this Manual will go into additional detail on each of the five COSO components and the 17 principles, including examples and practical guidance.

Key takeaways:

1. **Remember the iterative nature of the ICOFR assessment process.** Consider the risk based approach to the evaluation of internal control as a cumulative, iterative process and not a sequential thought process.

2. **The SEC has continued to stress the importance of effective ICOFR, through public comments and speeches and through comment letters and enforcement actions.**

3. **Remember, focus on the important.** As the degree of risk that a material weakness could exist in a particular area of the entity’s ICOFR, the level of attention that should be devoted and the level of evidence obtained about the design and operating effectiveness of controls in that area should increase.

4. **Know the objective and the framework.** For public entities, the SEC has a defined objective for ICOFR, found in Regulations 13a-15(f) and 15d-15(f) of the Securities Exchange Act.
Chapter 2
Documentation
While *having* an effective system of internal control over financial reporting (ICOFR) is the objective, *evidencing* the effectiveness is also very important.

Louis Fried, a widely published management systems guru and author, once said, “if it is not documented, it doesn’t exist. As long as information is retained in someone’s head, it is vulnerable to loss.”

In addition to supporting the external auditor’s assessment, management’s documentation plays a critical role in supporting management’s assertion about ICOFR. Sufficient, appropriate documentation is a requirement in the COSO Framework and specifically discussed in the SEC Staff guidance.

This chapter outlines the requirements with respect to management’s documentation. The importance of documenting key decisions and findings is highlighted throughout the remaining ICOFR Reference Guide chapters.
[2.1.10] The SEC Staff stated, “as part of its evaluation of ICOFR, management must maintain reasonable support for its assessment.”

[2.1.20] The COSO Framework similarly requires management to maintain documentation for the following reasons:

— To provide clarity around roles and responsibilities, which promotes consistency in adhering to the entity’s practices, policies and procedures;
— To assist in capturing the design of internal control and setting expectations of performance and conduct;
— To assist in training new personnel and to offer a reference for other employees;
— To provide a means to retain organization knowledge; and
— To provide evidence of the conduct of internal control, enable proper monitoring, and support reporting.

[2.1.30] As risk rises, so too does the evidence necessary to evaluate the effective operation of controls and degree of documentation needed to substantiate that evidence. The SEC Staff has provided the following diagram to illustrate how sufficiency of documentation should be evaluated based on risk:

![Diagram](image)

* The references to “more” or “less” include both the quantitative and qualitative characteristics of the evidence (that is, its sufficiency).

[2.1.40] The diagram above demonstrates that the level of evidence needed to support effective operation of ICOFR is a matter of judgment and is dependent on (i) the risk of material misstatement related to a particular area of the financial statements (significant account or disclosure) – which includes misstatement risks due to both quantitative and qualitative aspects, and (ii) the risk the control being evaluated might fail to operate effectively. A control’s risk of failure is a factor of multiple considerations, including, but not limited to:

— The type of control (manual or automated) and the frequency with which it operates;
— The complexity of the control;
— The risk of management override;
— The judgment required to operate the control;

---

— The competence of the personnel who perform the control or monitor its performance;
— Whether there have been any changes in key personnel who either perform the control or monitor its performance;
— The nature and materiality of misstatements that the control is intended to prevent or detect;
— The degree to which the control relies on the effectiveness of other controls (for example, IT general controls); and
— The evidence of the operation of the control from prior year(s).

[2.1.50] The COSO Framework and the SEC Staff guidance are consistent in their documentation requirements for regulatory reporting purposes. The COSO Framework states that management assumes a higher degree of responsibility for maintaining the requisite supporting documentation when it asserts to regulators, shareholders, or other third parties that in their system of internal control: (1) the components and principles are present and functioning, and (2) the components are operating together in an integrated manner.5

[2.1.60] The COSO Framework also states that:6

— “In cases where an external auditor attests to the effectiveness of the system of internal control, management will likely be expected to provide the auditor with support for its assertion on the effectiveness of internal control. That support includes evidence that the system of internal control is properly designed and operating effectively to provide reasonable assurance of achieving the entity’s objective. In considering the nature and extent of documentation needed, management should remember that the documentation to support the assertion will likely be used by the external auditor as part of his or her audit evidence, including the sufficiency of such documentation for those assertions. Management would also need to document significant judgments, how such decisions were considered, and how the final decisions were reached.”

[2.1.70] Management documentation should be sufficient to demonstrate effectiveness for all components and principles, including those outside of control activities. As the COSO Framework points out, “it is important to keep in mind that controls, such as those embedded within monitoring activities or risk assessments, cannot be performed entirely within the minds of senior management without some documentation of management’s thought process and analyses.”7

[2.1.80] Management should pay particular attention to documenting the following:
— Understanding, at the process level, of the flow of information from initiation to reporting and the related financial reporting risks (see chapter 5 of the ICOFR Reference Guide – Risk Assessment – understanding WCGWs);
— Design and operating effectiveness of management review controls (see chapter 7 of the ICOFR Reference Guide – Management Review Controls);
— Monitoring of the operating effectiveness of the controls (see chapter 10 of the ICOFR Reference Guide – Monitoring); and

---

5 COSO Framework, p. 29.
7 COSO Framework, p. 30.
Key takeaways:

1. Management is required to maintain sufficient documentation to support its ICOFR assessment.

2. The level of evidence needed to support management’s ICOFR assessment depends on the misstatement risk and risk that the control being evaluated will fail. As either risk increases, the level of evidence, and level of documentation to substantiate that evidence, needed increases.

3. While the degree and type of documentation required may vary, management should pay particular attention to the documentation in these key areas:
   - Understanding, at the process level, of the flow of information from initiation to reporting and the related financial reporting risks (see chapter 5 – Risk Assessment – understanding WCGWs);
   - Design and operating effectiveness of management review controls (see chapter 7 – Management Review Controls);
   - Monitoring of the operating effectiveness of the controls (see chapter 10 – Monitoring); and
   - Evaluation of any identified deficiencies (see chapter 11 – Identifying and Evaluating Deficiencies).
Chapter 3
Control environment
The COSO Framework describes the Control Environment as a set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. As such, the Control Environment represents the foundation of a sound system of internal control.

The SEC Staff believes that “some entity-level controls, such as certain Control Environment controls, have an important, but indirect, effect on the likelihood that a misstatement will be prevented or detected on a timely basis.”

While the Control Environment may have the most indirect influence of any of the other COSO components on ICOFR, its impact is pervasive and its effectiveness should be considered on its own as well as in relation to the other COSO components.

Management and external auditors are encouraged to assess the effectiveness of the Control Environment throughout the entity early in and continuously through the ICOFR assessment process and to consider how this evaluation influences the approach to assessing other components and principles.

---

3.1 Principles of an Effective Control Environment

[3.1.10] The COSO Framework describes the Control Environment, as:

- A set of standards, processes, and structures that provide the basis for carrying out ICOFR;
- The tone at the top (i.e., the tone set by the board of directors and senior management) with respect to ICOFR, including the integrity and ethical values of the organization; and
- Management’s reinforcement of the tone at the top throughout the rest of the organization.

[3.1.20] In contrast to process-level control activities which directly impact financial reporting, but often impact just one stream of transactions, the Control Environment’s impact to ICOFR is indirect, yet it may have a pervasive impact on multiple business processes throughout the organization.

[3.1.30] The COSO Framework emphasizes that the Control Environment provides the basis for carrying out ICOFR across the organization and at all levels, including third-party service providers (TPSPs) and business partners. This means that the Control Environment may need to be assessed at lower levels such as regions, divisions, operating units, or functional areas and not just at the parent or corporate level.

[3.1.40] Business models and structures have evolved since the COSO 1992 Framework was released and an increasing number of organizations have outsourced various processes—including, for example, payroll processing, IT, or investment management—to TPSPs. Management retains responsibility for the effectiveness of controls over activities performed by TPSPs. When the transactions processed by a TPSP are significant to the financial statements, it is important for management to consider the activities performed by TPSPs in their assessment of ICOFR.

See chapter 5 of the ICOFR Reference Guide – Risk Assessment – Understanding WCGWs for additional discussion regarding TPSPs.

[3.1.50] The COSO Framework uses the term “board of directors” to refer to the entity’s board of directors or an equivalent oversight body that is charged with the governance of the organization. This chapter follows suit.

[3.1.60] The COSO Framework acknowledges that the board of directors may delegate its oversight responsibilities, where appropriate, to committees at the board level that focus on specialized topics (e.g., audit committees).

[3.1.70] As discussed in chapter 1 of the ICOFR Reference Guide – Introduction, the Control Environment is one of the five components of internal control under the COSO Framework. The most significant change made in the COSO 2013 Framework is the codification of fundamental concepts from the 1992 Framework into 17 principles, which are associated with the five components and provide clarity for understanding requirements for effective internal control.
There are five principles necessary for an effective Control Environment within ICOFR.4

### Principles of the Control Environment Component

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 1:</td>
<td>The organization demonstrates a commitment to integrity and ethical values.</td>
</tr>
<tr>
<td>Principle 2:</td>
<td>The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.</td>
</tr>
<tr>
<td>Principle 3:</td>
<td>Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.</td>
</tr>
<tr>
<td>Principle 4:</td>
<td>The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.</td>
</tr>
<tr>
<td>Principle 5:</td>
<td>The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.</td>
</tr>
</tbody>
</table>

Remember that these principles are required to be met in order to demonstrate effective ICOFR. Often, entities attempt to demonstrate that they have met the principles by taking a bottoms-up approach; namely, they map existing controls to each principle to determine whether there are controls for each principle. Mapping controls is important, but not likely to be sufficient to demonstrate that an entity has met each principle. What might be missing from this approach is 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.

Further, testing the “controls” linked to the Control Environment may require a different approach than testing control activities. This is because testing the control environment means testing the “set of standards, processes and structures” rather than specific control activities. Also, because of the indirect nature of the Control Environment, an assessment of the effectiveness of the principles often requires qualitative considerations, as described in Illustration 3.1.

---

4 COSO Framework, p. 31.
**Illustration 3.1:**
Contrasting a bottoms-up versus a top-down approach to demonstrating whether a principle has been achieved

---

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

**Bottoms-up approach to Principle 2:**
The entity specifies that the audit committee meets four times a year; holds private sessions with management, internal audit, and the external auditors; and discusses ICOFR. The agenda and minutes from the meetings are the evidence of the matters discussed and occurrence of those meetings. Using this approach, it is possible that an audit committee could meet all the criteria specified by the entity but still not provide effective oversight of ICOFR.

**Top-down approach to Principle 2:**
The audit committee, management, and the internal auditors take a fresh look by considering the topics discussed at the audit committee meetings and the information shared relative to the design, operation and findings of the system of ICOFR. They determine that ICOFR is broadly discussed when the Internal Audit Director provides a status of SOX testing or when a significant deficiency or material weakness is being evaluated. However, the audit committee, management, and the internal auditors determine that in order to achieve the objectives of Principle 2:

- Management should present to the audit committee more information with respect to the ICOFR risk assessment process in order to allow the audit committee to evaluate and provide suggestions and oversight;
- The audit committee should ask management to include in its annual presentation to the audit committee a discussion of critical accounting policies and estimates – not just the accounting treatment, but also the relevant controls that are in place, the precision at which those controls operate, and a report on the operating effectiveness of those controls;
- The audit committee should provide its insight regarding where a fraud risk may be present and whether the controls that are in place to detect or deter that risk of fraud are appropriate; and
- The internal audit department should present to the audit committee more information about the manner in which controls are tested by the entity, including self-assessments, questionnaires, and direct testing by internal audit or others.

The agenda and minutes of the meetings still serve as evidence, but may be supplemented by a memo that documents the more qualitative considerations of the effectiveness of the audit committee, rather than just noting whether the criteria specified in the bottoms-up approach were met.

---

[3.1.100] Supporting the five principles are “points of focus.” As discussed in chapter 1 of the ICOFR Reference Guide – Introduction, these points of focus are example characteristics that may help both management and external auditors determine if a principle is present and functioning.

[3.1.110] Unlike the principles, the COSO Framework does not require each point of focus to be met in order for management to conclude that ICOFR is effective.
The following Illustrations describe the five principles and underlying points of focus for the Control Environment component under the COSO Framework. The Illustrations provide examples of questions that may be asked to gain an understanding of the entity’s Control Environment. Keep in mind that a “no” answer to any of these questions does not necessarily mean that the particular principle or component is deficient; however, this answer might influence the assessment of other COSO components and principles.

**Illustration 3.2:**
Considerations for Principle 1 of Control Environment

<table>
<thead>
<tr>
<th>Points of Focus</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Sets the tone at the top</td>
<td>— How does the board of directors demonstrate through its directives, actions, and behavior the importance of integrity and ethical values to support the functioning of ICOFR?</td>
</tr>
<tr>
<td>— Establishes standards of conduct</td>
<td>— How does management at all levels of the organization demonstrate through its directives, actions, and behavior the importance of integrity and ethical values to support the functioning of ICOFR? Is this importance communicated throughout the organization?</td>
</tr>
<tr>
<td>— Evaluates adherence to standards of conduct</td>
<td>— Does the entity have a written code of conduct, formal and documented policies, procedures, and means of communication?</td>
</tr>
<tr>
<td>— Addresses deviations in a timely manner</td>
<td>— Do the standards of conduct apply throughout the organization, to all levels and to different geographies and to external partners?</td>
</tr>
<tr>
<td></td>
<td>— How are the standards of conduct communicated to employees (e.g., through regular training, web site postings, newsletters)?</td>
</tr>
<tr>
<td></td>
<td>— How are violations identified, reported, and addressed? How does the entity enforce the standards of conduct? Are violations remedied in a timely and consistent manner? Does the entity perform compliance audits?</td>
</tr>
<tr>
<td></td>
<td>— Are there clear consequences for deviating from the standards at every level?</td>
</tr>
<tr>
<td></td>
<td>— Is this message emphasized by the CEO and key executives?</td>
</tr>
<tr>
<td></td>
<td>— Is the tone at the top consistently demonstrated in the informal and routine actions and communications of the leaders at all levels of the entity?</td>
</tr>
</tbody>
</table>
### Illustration 3.3: Considerations for Principle 2 of Control Environment

<table>
<thead>
<tr>
<th>Points of Focus</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establishes oversight responsibilities</td>
<td>Has the entity formalized its bylaws and committee charters in accordance with applicable regulatory and stock exchange listing requirements?</td>
</tr>
<tr>
<td>Applies relevant expertise</td>
<td>Do management and the board of directors have defined roles, responsibilities, and powers of delegation? Do board members actively oversee external financial reporting and management’s performance of internal control?</td>
</tr>
<tr>
<td>Operates independently</td>
<td>Does the board of directors periodically evaluate the skills and expertise required among its members to enable them to appropriately oversee, probe, and evaluate the senior management team?</td>
</tr>
<tr>
<td>Provides oversight for the system of internal control</td>
<td>Do the board of directors and those charged with ICOFR oversight operate independently of management, and are they sufficiently objective in their evaluations and decision making?</td>
</tr>
<tr>
<td></td>
<td>Does the board of directors provide oversight for management’s design, implementation, and conduct of ICOFR for each of the five components? See pages 42–43 of the COSO Framework for board oversight responsibilities by component.</td>
</tr>
<tr>
<td></td>
<td>Does the board of directors regularly review and assess the performance of key members of management?</td>
</tr>
<tr>
<td></td>
<td>Has the entity established channels of communication between all relevant parties in regular intervals using formal agendas?</td>
</tr>
<tr>
<td></td>
<td>Has the entity established a structure to investigate whistleblower allegations?</td>
</tr>
<tr>
<td></td>
<td>How does the board of directors oversee the risk of management override of ICOFR?</td>
</tr>
</tbody>
</table>
### Illustration 3.4:
Considerations for Principle 3 of Control Environment

<table>
<thead>
<tr>
<th>Points of Focus</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Considers all structures of the entity</td>
<td>— Has the entity created an organizational chart that defines the roles, responsibilities, and reporting lines to support the achievement of ICOFR objectives? Does the organizational chart take into account segregation of duties and include clear reporting lines and communication channels?</td>
</tr>
<tr>
<td>— Establishes reporting lines</td>
<td>— Does this organizational chart support the entity’s control structure? Does it consider departmental responsibilities, geographies, levels of management, and TPSPs?</td>
</tr>
<tr>
<td>— Defines, assigns, and limits authority and responsibilities</td>
<td>— Is authority and responsibility delegated based on demonstrated competence? Are appropriate segregation of duties and potential conflicts of interest considered?</td>
</tr>
<tr>
<td></td>
<td>— Are authorities and responsibilities assigned across the entity and at all levels and are they appropriate and sufficiently well defined to enable accountability over operating units and functional areas?</td>
</tr>
<tr>
<td></td>
<td>— Are the mechanisms employed by management sufficient to monitor the assignment of authorities and responsibilities across the entity and at all levels?</td>
</tr>
<tr>
<td></td>
<td>— Are decentralized decision makers sufficiently knowledgeable? How do they learn about new regulations or changes to regulations? How strong are the lines of communication?</td>
</tr>
<tr>
<td></td>
<td>— Is management effectively managing outsourced service providers through service level agreements?</td>
</tr>
</tbody>
</table>
### Illustration 3.5:
Considerations for Principle 4 of Control Environment

<table>
<thead>
<tr>
<th>Points of Focus</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establishes policies and practices</td>
<td>Has the entity established competence requirements for people in key financial reporting and internal audit roles across the organization as well as for members of the audit committee?</td>
</tr>
<tr>
<td>Evaluates competence and addresses shortcomings</td>
<td>Does the entity properly address any identified knowledge gaps through hiring of qualified individuals, training of existing employees, or the use of qualified external experts or service providers, where necessary?</td>
</tr>
<tr>
<td>Attracts, develops, and retains individuals</td>
<td>Does the entity develop and maintain policies that reflect the entity’s values and objectives? Does the entity review and update these policies regularly?</td>
</tr>
<tr>
<td>Plans and prepares for succession</td>
<td>Does the entity ensure these policies are used as a basis for making hiring, retention, termination, and promotion decisions?</td>
</tr>
<tr>
<td></td>
<td>Does the entity have programs in place (e.g., mentoring, training, etc.) that demonstrate management’s commitment to attract, develop, and retain competent personnel?</td>
</tr>
<tr>
<td></td>
<td>Has the entity implemented a process to ensure adequate staffing levels, including contingency and succession plans?</td>
</tr>
</tbody>
</table>
Illustration 3.6: Considerations for Principle 5 of Control Environment

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

<table>
<thead>
<tr>
<th>Points of Focus</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Enforces accountability through structures, authorities, and responsibilities</td>
<td>— Does the entity hold individuals within the entity accountable? Do employees certify that they have fulfilled their internal control responsibilities during any given period—i.e., are employees asked to certify their results to instill responsibility and accountability?</td>
</tr>
<tr>
<td>— Establishes performance measures, incentives, and rewards</td>
<td>— Is there a performance measurement and reward plan aligned with the entity’s ethical values and ICOFR objectives?</td>
</tr>
<tr>
<td>— Evaluates performance measures, incentives, and rewards for ongoing relevance</td>
<td>— Is the incentive plan balanced towards the pressures of achieving performance objectives and maintaining effective ICOFR and financial reporting objectives?</td>
</tr>
<tr>
<td>— Considers excessive pressures</td>
<td>— Do management and the board of directors monitor the appropriate amount of pressure on achieving financial reporting results and the impact that it has on people and the effectiveness of ICOFR?</td>
</tr>
<tr>
<td>— Evaluates performance and rewards or disciplines individuals</td>
<td>— Does the entity evaluate performance of key personnel within the financial reporting process against the established performance measures?</td>
</tr>
<tr>
<td></td>
<td>— Are shortcomings appropriately addressed?</td>
</tr>
</tbody>
</table>

[3.1.130] Demonstrating that an entity complies with the principles of an effective Control Environment may be difficult. Remember, the Control Environment consists primarily of processes, standards, and structures, rather than discrete control activities. Entities may be accustomed to producing evidence that a particular, discrete control activity is designed appropriately and operating effectively. Evaluating the Control Environment, at least initially, will require a different approach.

[3.1.140] Documentation can vary from entity to entity. One possible approach is to answer the relevant questions posed in the Illustrations above and maintain supporting documentation that led to the answers. Ask, “based on the supporting documentation that has been assembled, would a prudent official be able to answer the same relevant question in the same manner?” If not, the supporting documentation may need to be supplemented with further evidence or explanation.
The Impact of the Control Environment on ICOFR

[3.2.10] The Control Environment has a pervasive effect on an entity’s system of internal control and therefore, forms the foundation of effective ICOFR. The assessment of the effectiveness of the Control Environment throughout the entity should take place early in and continuously throughout the ICOFR assessment process. This evaluation will influence the assessment of other components and principles.

[3.2.20] Sometimes an assessment of the Control Environment will yield an obvious conclusion that there are no deficiencies, or there is a material weakness because the Control Environment is deficient.

**Illustration 3.7:** Obvious conclusion on the Control Environment

<table>
<thead>
<tr>
<th>No deficiencies:</th>
</tr>
</thead>
<tbody>
<tr>
<td>An entity is very control conscious and is exemplary in all principles and points of focus described in the COSO Framework.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Material weakness:</th>
</tr>
</thead>
<tbody>
<tr>
<td>An entity’s board of directors (or the appropriate committee) neither discusses ICOFR nor oversees management’s ICOFR. The entity has no published code of conduct, and the people assigned to financial reporting in the entity do not have the skills necessary to produce accurate financial statements.</td>
</tr>
</tbody>
</table>

[3.2.30] More often, though, the findings pursuant to an assessment of the Control Environment are not so extreme and therefore, the conclusion is not so obvious. There may be some weaknesses in the Control Environment that need to be considered in the context of the rest of the COSO components and principles before concluding that a deficiency exists or determining the severity of that deficiency.

[3.2.40] Weaknesses (or potential weaknesses) in the Control Environment should be carefully considered to determine the appropriate response. Most often, a weakness in the Control Environment will impact Risk Assessment (discussed in chapter 4 of the ICOFR Reference Guide – Risk Assessment). The following examples illustrate how different Control Environments may impact the ICOFR assessment.
**Illustration 3.8:**
Contrast the impact on Risk Assessment and response of two different Control Environments

**Entity 1:**
An entity has a code of conduct, distributes it to every employee, requires regular self-assessments against that code of conduct, and even has routine examinations by internal audit related to aspects of the code that are critical to effective ICOFR. In addition, when violations to the code are discovered, they are summarized in the entity's monthly newsletter, including the adverse consequences affixed for violating the code of conduct (e.g., termination, ineligibility for a bonus, etc.).

**Entity 2:**
Entity 2 is in the exact same line of business, with similar business processes and financial reporting risks. Entity 2 has a code of conduct and each employee receives a copy, but there are no formal mechanisms in place to ensure adherence to the code of conduct.

**Impact on Risk Assessment and Response:**
While the financial statement assertion risks may be the same for the two entities because they offer the same product and have similar processes, the programs enacted by Entity 1 to support its Control Environment are clearly more robust than those at Entity 2. One may or may not reach the conclusion that there is a deficiency in Entity 2's Control Environment, but the nature, timing, and/or extent of evidence necessary to conclude that the remaining COSO components are present and functioning may be, out of necessity, greater than what may be required when assessing ICOFR at Entity 1.

Reaching a conclusion as to whether there is an indicator of a potential deficiency in Entity 2's Control Environment will depend on the reason(s) as to why there are no formal mechanisms in place to ensure adherence to the code of conduct. For example, in a smaller entity where management can determine compliance without official programs, lack of the existence of formal compliance mechanisms may be sufficiently mitigated such that a deficiency does not exist. But the objective in question is not to simply have a code of conduct in the organization—it is to have everyone in the entity adhere to a proper code of conduct. Therefore, for many entities a lack of a mechanism to ensure adherence to the code of conduct would be a strong indicator of ineffective ICOFR.
Illustration 3.9:
How a weak Control Environment may impact Risk Assessment

An entity may have a weakness related to Principle 3—specifically, management may not have established reporting lines with appropriate responsibilities and authorities consistent with control objectives across the organization.

This weakness in a single-location entity may yield risks significantly different from the same weakness in an entity with multiple subsidiaries in multiple locations or an entity that is rapidly expanding through acquisitions.

This weakness in the Control Environment may be mitigated by implementing control activities that address the identified risks demonstrating the integrated nature of the principles. For example, performing a proper evaluation of the Control Environment, recognizing the weakness, and appropriately assessing the resulting risks to the entity as part of Risk Assessment can lead to the establishment of controls in another COSO component, such as Control Activities, to effectively compensate for the risks to the financial statements.

Illustration 3.10:
Control Environment for smaller companies can be different

Scenario:
A small decentralized entity lacks a formal written code of conduct but its commitment to integrity and ethical values is widely demonstrated in several ways by the actions and behavior of the board of directors, its management, and employees across all levels of the entity. Management views integrity as essential to successful business operations and regularly communicates this in its communications with employees, customers, and suppliers. The board and senior management set a strong tone at the top that supports a strong culture of internal control, which is cascaded downward throughout the entity by divisional management.

All new employees participate in onboarding training where the employee compliance policies and procedures are reviewed. Annually, the audit committee surveys all officers, directors, and employees on awareness and compliance to internal control policies and procedures. The audit committee also surveys customers and suppliers on their perception of the integrity and ethical values of entity personnel. There is regular interaction with suppliers and customers. Management strictly enforces use of appropriate licensed software, and individuals are held accountable for compliance with laws and regulations applicable to the organization. The audit committee chair manages the whistleblower hotline.

A portion of the annual incentive award available to employees is based on their achievement of control objectives and on their feedback from suppliers, customers, and other employees.
Why these actions may be more effective for a small entity:
Smaller entities may be in a position to develop a culture that emphasizes the importance of integrity and ethical behavior through oral communication and by management example. Communication may be less structured and easier to achieve in a smaller entity than in a larger entity since there may be fewer levels of responsibility, and management may be more visible and available. The level of direct interaction between management and employees is greater.

What this means for the ICOFR assessment:
The COSO Framework states that the principles underlying the components of internal control are as applicable for a small organization as they are for a larger organization. However, the approaches regarding implementation may be different. In this scenario, the entity’s commitment to integrity and ethical values as described by the COSO Framework appears evident in the variety of policies and procedures it employs.

Evidence of effective elements of the Control Environment in smaller entities may be available in a variety of forms. The COSO Framework typically requires effective documentation when management asserts to regulators and shareholders on the design and operating effectiveness of its system of internal control and/or where auditor attestation occurs. However, the COSO Framework does not require all documentation to be formal. Nonetheless, the organization should present persuasive evidence to show that the components and relevant principles are present and functioning.

In making an assessment, management and external auditors may consider the available evidence and adjust testing and documentation accordingly. For example, if no formal written code of conduct is available for testing, management and auditors might need to extend evaluation procedures to include inquiry, corroborative inquiry, or observation of several individuals employed by the entity to confirm the existence of the code of conduct and to understand the extent to which this code of conduct is adhered to and enforced.
Because the Control Environment component is the foundation of the system of internal control, its relative strength will influence the nature, timing, and extent of testing of control activities that have a direct impact on financial statement assertions. In general, an effective control environment may have the following positive effects on evaluation of an entity’s control activities:

- Less persuasive process-level control tests (i.e., nature)—e.g., inquiry and observation, self-assessments—may be appropriate in lower risk areas (see chapter 6 of the ICOFR Reference Guide – Control Activities);
- Smaller control sample sizes may be appropriate (i.e., extent) when there is an effective Control Environment; and
- Testing the operating effectiveness of controls at an interim period versus year-end may be appropriate (i.e., timing) when there is an effective Control Environment. (Note: It is important to consider appropriate roll-forward procedures when testing is performed at an interim period.)

Conversely, a deficient Control Environment may adversely impact the nature, timing, and extent of the ICOFR assessment procedures. And while deficiencies in the Control Environment (and in the other indirect components of internal control) may have a pervasive impact on an entity’s ICOFR because of the nature of the Control Environment as the foundation of a sound system of internal control, it is nevertheless critical to thoroughly understand such deficiencies and the specific impact they may have on the entity’s financial reporting process. It is particularly important to determine which process level controls and related financial statement assertions could be affected by the identified deficiencies. Not every deficiency in the Control Environment may have an equally severe impact on all controls across the entity’s various business processes.

However, given the pervasive nature of the Control Environment (and other indirect components of internal control), it may be difficult to associate a deficiency in the Control Environment with a specific financial statement account and/or assertion. Therefore, it also is important to understand whether there are suitable compensating controls for the identified deficiencies. Such compensating controls may exist in other components and principles of the entity’s system of ICOFR. They are also more likely to be available in situations where the entity follows the duplication strategy and designs multiple processes and controls to achieve the same objective. Refer to chapter 11 of the ICOFR Reference Guide for further guidance regarding evaluation of deficiencies in pervasive controls, including a decision flowchart for such evaluations.

If there are unmitigated deficiencies in the Control Environment (or other indirect components of internal control), they should be carefully evaluated by both management and external auditors with respect to their impact on the ICOFR assessment at the process level. Such deficiencies increase the risk that the control activities at the process level are not properly designed or do not operate effectively. That increased risk is considered when determining the nature, timing, and extent of the tests to be performed on the control activities potentially impacted by the deficiencies in the Control Environment. Responses to the increased risk may include:

- Applying tests that are likely to deliver more persuasive evidence of the operating effectiveness of controls impacted by the deficient elements of the Control Environment (e.g., re-performing a control rather than performing an inquiry and corroborative inquiry or inspection of historical records related to the control);
- Extending the sample of control operations subject to evaluation; or
- Testing the impacted controls closer to the ICOFR assessment date and shortening or eliminating the period between any interim testing performed and the year-end ICOFR assessment date (the roll-forward period).
**Illustration 3.11:**
Determining the impact of deficiencies in the Control Environment on process level controls

**Scenario:**
Entity A, a widget manufacturer, recently relocated its headquarters from Dayton, Ohio to Atlanta, Georgia. While most of the key financial reporting personnel moved with the entity, several individuals responsible for the sales and A/R process left the entity upon the relocation. Absent in-place succession planning, management hired several replacement personnel in Atlanta and decided to re-assign remaining activities in the sales and A/R process to other individuals in the entity. Over the next several months, the entity struggled with timely accounting for its sales and A/R, including calculation of a key estimate – the allowance for doubtful accounts, although no errors in the related accounts were identified in the course of the year. Nevertheless, in performing their annual ICOFR assessment, both management and external auditors identified deficiencies in the entity’s Control Environment, including in particular Principle 4, related to the policies and procedures in place for retaining competent individuals and preparing for succession in key financial reporting roles.

**Response:**
In analyzing the identified deficiencies, management and external auditors noted that while the deficiencies require improvements in entity-wide processes for hiring and retention of competent personnel, they only impacted the sales and A/R process in the current year. In addition, the deficiencies were more likely to impact those manual controls within the process which require specialized skills, knowledge, and experience. Taking this into account, management responded to the identified deficiencies in the Control Environment by:

- Extending the period of time allowed for the month-end close of the accounts related to the sales and A/R process;
- Increasing the frequency of ongoing monitoring activities over the controls within the sales and A/R process, including monitoring the level of unapplied cash, A/R write-offs, A/R allowance as a percentage of gross A/R and other key performance indicators for the process;
- Requesting assistance from Internal Audit in performing direct tests of the key controls within the sales and A/R process on a monthly or quarterly basis, as appropriate.

Similarly, external auditors considered the identified deficiencies in the Control Environment in their ICOFR audit approach for the sales and A/R process by:

- Assigning more experienced personnel to perform the walkthrough of the process, identify relevant risks and related controls;
— Focusing on identification and testing of automated controls within the process which are less exposed to the risk of error;
— Performing detailed testing of the controls within the process throughout the rollforward period;
— Increasing the number of control operations tested for each manual control within the process;
— Incorporating elements of reperformance into the testing of key controls within the process, in particular those controls over the valuation of the entity’s allowance for doubtful A/R.

Illustration 3.12:
Response to a less effective Control Environment

Scenario:
The entity does not have enough skilled employees in the finance and tax departments to be able to perform and review the accounting for some of the entity’s complicated transactions. In COSO terms, the entity has a deficiency related to Principle 4; they do not have an effective process in place to ensure that they attract, develop, and retain competent individuals that are knowledgeable about the regulatory and financial reporting environment in which the entity operates.

What this means for the ICOFR assessment:
Certain controls are highly dependent upon the control operator having specific knowledge and expertise about the regulatory and financial reporting environment in which the entity operates. The effective operation of these control activities is suspect because of the deficient Control Environment.

If management understands and evaluates this weakness in the Control Environment, it may be able to mitigate the impact by, among other things, identifying the areas of accounting where additional skills are needed and hiring sufficiently skilled personnel or contractors.

However, if this weakness remains unaddressed, management and external auditors would likely determine that additional evidence about the proper functioning of controls in areas of complex transactions will be necessary. Additional evidence may come in the form of more thorough testing, testing of more samples of the operation of the control, testing samples closer to the assessment date, etc. In this way, management and the auditors can better understand the impact that the deficiency in the Control Environment had on the operation of controls. Documentation of this thought process is important.
Understanding the effectiveness of the Control Environment will also serve to inform the walk-throughs of the business processes and build awareness of how the entity integrates the other four COSO components into the control activities. For example, if those evaluating ICOFR are aware of how the organization identifies and communicates important information internally, they can be alert for how control operators receive and use information necessary for the effective functioning of a process-level control.

The following Illustration summarizes the relationship between the effectiveness of Control Environment and the ICOFR assessment. The other indirect components of internal control (Risk Assessment, Monitoring, and Information and Communication) may have a similar impact.

**Illustration 3.13:**
Relationship of Control Environment effectiveness to the ICOFR assessment procedures

---

**More Effective Control Environment**
- More persuasive control tests. Control sample sizes above the minimum.
- Performing procedures closer to final

**Less Effective Control Environment**
- Less persuasive control tests. Minimum/smaller control sample sizes.
- Performing more procedures at interim.

---

An assessment of ICOFR is iterative. Management and external auditors should continually reassess preliminary conclusions based on evidence obtained throughout the assessment. Evidence obtained in each subsequent activity or phase of the assessment may cause management and external auditors to reassess their preliminary conclusions about the effectiveness of the Control Environment. This reassessment also may give reason to reconsider the initial determination of the nature, timing, and extent of evidence necessary to reach a final conclusion on the effectiveness of internal control.
Illustration 3.14: Recurring deficiencies

Scenario:
For the past two years, internal audit has identified recurring deficiencies in the operating effectiveness of a system access control. While the internal control deficiencies were evaluated and communicated in a timely manner to senior management and to those department heads responsible for taking corrective action, the entity has not corrected the deficiency. The external auditors identified system access control deficiencies again this year. Historically, the entity was able to demonstrate a sufficient suite of compensating controls that operated effectively. This limited the severity of the access control issue to a deficiency.

What this means for the ICOFR assessment:
Deficient controls over security management (Principle 11 of the COSO Framework) have implications for automated process-level controls and the integrity of financial reporting. In addition, this lack of response raises concerns about Principle 5 in the Control Environment and management’s attitude towards the importance of internal controls and actions to hold individuals accountable for their internal control responsibilities.

If the matter was significant enough to be communicated to the audit committee (i.e., if it was determined to be a significant deficiency previously), it may also call into question how the board of directors exercises its oversight of Control Activities and Monitoring Activities related to this control deficiency.

Management and external auditors should investigate the reasons for the lack of a timely response and perform a thorough assessment of the severity and pervasiveness of the system access control deficiencies for the third year. Despite the fact that no financial statement errors have been identified, recurring security management control deficiencies are cause for concern if there are no compensating controls in place to contain and monitor the incidence and nature of inappropriate access. Even if there are compensating controls, recurring control deficiencies may be a cause for concern. Depending on the facts and circumstances, those compensating controls may not operate at a sufficiently precise level.

A root cause analysis also will include considerations of the repeated nature of the deficiency and the lack of response by management to the monitoring control deficiency (Principle 17). Management and auditors may need to consider how the board of directors provided (or did not provide) oversight of management actions and consider the severity of any deficiency in Principle 2. Consideration of whether the failure to remediate identified control deficiencies may result in additional control deficiencies is also needed. Are there other business processes or functional units that may not be subject to board oversight of controls? This may cause a reconsideration of the manner in which the ICOFR assessment is performed.

[3.2.120] Chapter 11 of the ICOFR Reference Guide – Identifying and Evaluating Deficiencies sets out the various steps and considerations in assessing the implications of deficiencies in the Control Environment and other indirect, pervasive areas of ICOFR.
Key takeaways:

Control Environment

1. **Be familiar with the points of focus** described in the COSO Framework related to the Control Environment. They will help you understand what is required to maintain an effective Control Environment.

2. The assessment of the Control Environment should be conducted across the organization and at all levels, including TPSPs and other external partners.

3. The assessment of the **Control Environment has a significant impact on the other components and principles** of the COSO Framework. Weaknesses in the Control Environment may drive changes to the nature, timing, and extent of evidence necessary to reach a conclusion on whether ICOFR is effective. Therefore, the initial evaluation of the Control Environment should be conducted early in the ICOFR assessment process.

4. **The ICOFR assessment is iterative.** The Control Environment is a key building block for the rest of the assessment. Continually reassess initial conclusions based on evidence obtained throughout the assessment.
Chapter 4
Risk assessment
In his book titled, *Risk Assessment: Theory, Methods, and Applications*, Marvin Rausand stated that “the possibility of harmful events is an inherent part of life. Such events can be caused by natural forces, such as flooding, earthquake, or lightning; technical failures; or human actions. In many systems, various safeguards are installed to prevent harmful events or to mitigate the consequences should such events occur. Risk analysis is used to identify the causes of harmful events, to determine the possible consequences of harmful events, to identify and prioritize barriers, and to form a basis for deciding whether or not the risk related to a system is tolerable. A risk analysis is carried out to provide answers to the following three main questions: Q1 – What can go wrong?; Q2 – What is the likelihood of that happening?; and Q3 – What are the consequences?”. \(^1\)

The author then clarifies that risk analysis is typically followed by risk evaluation during which judgments are made on the tolerability of the identified risks. And when risk analysis and risk evaluation are carried out in a joint process, they form a risk assessment.\(^2\)

The theoretical model of risk assessment outlined above can be applied to internal control over financial reporting (ICOFR). In fact, identifying the relevant risks to financial reporting is an essential component of ICOFR because failure to understand the likely sources of misstatements (what could go wrong) 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 Securities and Exchange Commission (SEC) Staff who stated that to accomplish the objective of effective ICOFR, management must identify the risks to reliable financial reporting prior to identifying controls and monitoring them for effectiveness.\(^3\)

---

2 Ibid. pp. 8-9
The objective of the assessment of ICOFR under Regulation 13(a)-15(d) of the Securities Exchange Act of 1934 is to evaluate whether management has implemented controls that will achieve the objective of ICOFR (that is, to provide reasonable assurance regarding the reliability of the entity’s financial reporting).

The guidance published by the SEC Staff states that before deciding which controls to evaluate, “management should identify those risks of misstatement that could, individually or in combination with others, result in a material misstatement of the financial statements (financial reporting risks). Ordinarily, the identification of financial reporting risks begins with evaluating how the requirements of GAAP apply to the company’s business, operations and transactions.”

The SEC Staff has also pointed out that management should consider internal and external risk factors, as well as sources of risk such as the initiation, authorization, processing and recording of transactions and other adjustments that are reflected in financial reporting elements.

The guidance provided by the SEC Staff is consistent with the COSO Framework. The Framework states that Risk Assessment is a dynamic and iterative process for identifying and assessing risks to the achievement of the entity’s objectives. It forms the basis for determining how risks will be managed through strategies including the design, implementation, and operation of appropriate control activities. The COSO Framework establishes four principles necessary for effective Risk Assessment:

<table>
<thead>
<tr>
<th>Principles of the Risk Assessment Component</th>
<th>Principle 6: The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Principle 8: The organization considers the potential for fraud in assessing risks to the achievement of objectives.</td>
</tr>
<tr>
<td></td>
<td>Principle 9: The organization identifies and assesses changes that could significantly impact the system of internal control.</td>
</tr>
</tbody>
</table>

These principles are required to be met in order to conclude that ICOFR is effective. Understanding what constitutes an effective Risk Assessment is critical to determining whether these principles have been achieved.

5 Ibid. p. 13.
7 Ibid. p. 59.
Supporting the four principles listed above are “points of focus.” As discussed in chapter 1 of the ICOFR Reference Guide – Introduction, these points of focus are example characteristics that may help both management and external auditors determine if a Principle is present and functioning. Unlike COSO principles, the COSO Framework does not require each point of focus to be met in order for management to conclude that ICOFR is effective. This chapter will focus on the principles and the supporting points of focus.

This chapter and chapter 5 of the ICOFR Reference Guide use the terms “financial reporting risks,” “likely sources of misstatement,” and “what could go wrongs (WCGWs)” interchangeably. These terms are used by standard-setters and regulators to refer to the risk of material misstatement of the entity’s financial statements.

An important point to keep in mind when considering the guidance in this chapter is the iterative nature of an effective risk assessment process. Evaluating the four principles within Risk Assessment cannot be done linearly because there is considerable overlap among the principles. Further, as an entity performs and monitors controls, items may come to management’s attention that will necessitate a reassessment of earlier risk determinations.
The first Principle in the Risk Assessment component of ICOFR relates to setting the objective. The following Illustration provides examples of questions that may be asked to get a broad understanding of whether the Principle has been met. The rest of this section will provide additional commentary and illustrations that further discuss the principle.

Illustration 4.1:
Considerations for Principle 6 of Risk Assessment

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

<table>
<thead>
<tr>
<th>Points of Focus (external financial reporting)</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Complies with applicable accounting standards</td>
<td>— Does the entity understand the objective of ICOFR as defined in Reg. 13a-15(f)?</td>
</tr>
<tr>
<td>— Considers materiality</td>
<td>— Does the entity review and update its understanding of applicable accounting and financial reporting standards considering the impact of changes on ICOFR?</td>
</tr>
<tr>
<td>— Reflects entity activities</td>
<td>— How does the entity determine materiality and is the amount consistent with what a reasonable investor might determine?</td>
</tr>
<tr>
<td></td>
<td>— What qualitative and quantitative factors does the entity consider in determining materiality?</td>
</tr>
<tr>
<td></td>
<td>— How does the entity identify its significant components (segments, subsidiaries, divisions, operating units, or functions)?</td>
</tr>
<tr>
<td></td>
<td>— How does the entity identify significant accounts, the related assertions, and disclosures in the financial statements?</td>
</tr>
<tr>
<td></td>
<td>— How is overall materiality cascaded down to each component and each significant account (risk tolerance)?</td>
</tr>
</tbody>
</table>

You will notice as you read through this chapter that some topics seem to relate to multiple principles. For example, the objective of ICOFR which is set forth by the SEC and requires preparation of reliable financial statements in accordance with Generally Accepted Accounting Principles (GAAP) is primarily a consideration under Principle 6 of the COSO Framework. In order to achieve that objective, an entity should have sufficient knowledge of GAAP, including any new accounting or reporting standards or interpretations. Understanding those changes is also critical to meeting.
Objective of Internal Control over Financial Reporting

Principle 6 of the COSO Framework requires that the entity specify objectives with sufficient clarity to enable the identification and assessment of risks to the achievement of these objectives.8

The COSO Framework refers to three broad categories of objectives of a system of internal control: (1) Operations; (2) Reporting (including external financial reporting, external nonfinancial reporting, and internal reporting); and (3) Compliance. However, for SEC registrants and for purposes of compliance with Sarbanes-Oxley Act Section 404 (SOX 404), the term Internal Control Over Financial Reporting and the specific objectives of internal control are defined in the rules and regulations of the SEC. Specifically, Regulation 13a-15(f) states:

“The term Internal Control Over Financial Reporting is defined as a process designed by, or under the supervision of, the issuer’s principal executive and principal financial officers, or persons performing similar functions, and effected by the issuer’s board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes 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 issuer;

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 issuer are being made only in accordance with authorizations of management and directors of the issuer; and

3. Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer’s assets that could have a material effect on the financial statements.”

For SEC reporting purposes, the objective of ICOFR is limited to providing reasonable assurance regarding the reliability of the financial statements and the preparation of the financial statements in accordance with GAAP. The objective of ICOFR does not extend to any other forms of financial reporting. However, entities may wish to extend their application of ICOFR beyond the financial statements, because management has responsibilities outside of SOX 404 to prepare accurate financial information for earnings releases, for other parts of Form 10-K or Form 10-Q (which would fall under management’s responsibilities with respect to Disclosure Controls and Procedures, or DCP), and for other reports. However, management’s assessment of ICOFR under SOX 404(a), and the accompanying external auditor’s attestation under SOX 404(b), if applicable, cover only those aspects of internal control that relate to financial statements and the accompanying footnotes.

Overlaying the SEC’s objective for ICOFR onto the COSO Framework can be confusing at times because the SEC’s objective of internal control does not fit exactly into any of the three categories of objectives specified by COSO (Reporting, Operations, and Compliance).

8 COSO Framework, p. 62.
As a general rule, if it is reasonable to assume that a risk could not lead to a misstatement of the financial statements, then the risk is not within the scope of ICOFR. However, there are certain exceptions to this general rule:

<table>
<thead>
<tr>
<th>Exception</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receipts and expenditures are not authorized by management or the board of directors</td>
<td>If an unauthorized expenditure is made, for example a cash disbursement that has not been authorized, the entity may nonetheless reflect the cash balance in the financial statements appropriately. However, according to the SEC's definition of ICOFR, the unauthorized disbursement would still be considered a deficiency and should be evaluated for severity. Risks and controls around authorization of receipts and expenditures are scoped into ICOFR by the SEC's definition of effective ICOFR.</td>
</tr>
<tr>
<td>Failure to safeguard assets</td>
<td>If assets are lost via theft, for example the theft of inventory from a warehouse, the entity may nonetheless reflect the inventory on hand at the reporting period appropriately. However, according to the SEC's definition of ICOFR, the entity is expected to safeguard its assets to the extent a loss of assets could be material to the financial statements. Therefore, management of the entity should consider whether there is a reasonable possibility that the theft of inventory could be material to the entity's financial statements. If there is a reasonable possibility of a material misstatement, theft of inventory is a relevant risk to the entity's ICOFR. However, this is not always the case. In some instances, inventory shrinkage is demonstrably immaterial every period and the nature of the inventory and the entity's business is such that the entity incurs normal inventory shrinkage, the misappropriation of which inventory is not relevant to the entity's ICOFR. In other cases, the nature of inventory and/or the historical shrinkage experience may indicate that safeguarding of inventory is a relevant risk to effective ICOFR and controls aimed at preventing inventory theft would need to be scoped into the entity's ICOFR.</td>
</tr>
</tbody>
</table>
Illustration 4.2:
Risks related to safeguarding of assets and authorization of receipts and expenditures

Risks related to the theft of petty cash are not likely to be a relevant ICOFR risk because the risk of a material misstatement to the financial statements due to theft of petty cash is, for most entities, remote.

In contrast, risks related to unauthorized cash distributions may present a risk of material misstatement to the financial statements. Controls such as appropriate segregation of incompatible job duties (writing a check, authorizing an invoice, setting up a vendor, etc.) may be necessary controls to mitigate those risks. Consider the following two scenarios.

Scenario A:
Entity A is a manufacturer with a large network of suppliers. One day, the 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 method of payment for Supplier X’s invoices from a check to a wire transfer and provides the number of the bank account to which the payments 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 and several million dollars in payments later, a representative of Supplier X contacts Entity A to complain about missing payments for several recent deliveries. He also does not recognize the bank account number on file with Entity A. An internal investigation shows that Entity A fell victim to a fraud scheme perpetrated by an unidentified third party and lost several million dollars in cash.

Analysis:
In this scenario, Entity A failed to safeguard its assets in violation of the SEC’s definition of effective internal control which 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 of internal control under the COSO Framework which requires that entities select appropriate methods of communication with external parties. In this case, Entity A either did not have a policy in place that would require 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 ICOFR assessment under the rules of the SEC and, unless Entity A 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 A’s financial statements, the control deficiencies, as described above, would likely represent a material weakness in Entity A’s ICOFR.
Scenario B:
At the end of a busy day, the head of Entity B’s A/P Department 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 investigation that follows shows that the CFO never requested the $50-million wire transfer and Entity B 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 of internal control under the COSO Framework which requires that entities select appropriate methods for internal communication. In this case, Entity B either did not have a policy in place that would require an appropriate supporting documentation for a significant cash transaction or failed to effectively operate relevant controls under such a policy. In addition, the wire transfer was likely processed in violation of Principle 3 of internal control which requires that entities 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 into the scope of management’s ICOFR assessment under the rules of the SEC and, unless 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, the control deficiencies, as described above, would likely represent a material weakness in Entity B’s ICOFR.

While 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 designed against the entity by internal or external parties, the 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, as discussed in section 4.4 of this chapter.

[4.2.80] In general, and as illustrated below, compliance with laws and regulations that do not have a direct impact on the preparation of the financial statements only comes into the scope of an ICOFR assessment when the entity has been notified of a potential violation or claim. This presupposes that the entity’s Control Environment and Information and Communication components of internal control are effective, including proper channels or programs (e.g., a whistleblower hotline) for identifying, communicating to appropriate management, and responding timely to potential claims.
Illustration 4.3:
When do I consider compliance with laws that have an indirect financial statement impact?

If members of management violate the law by trading securities using insider information, the risk of this illegal act occurring is not a relevant risk for ICOFR purposes. Representatives of management who use insider information for their personal benefit and act outside their role as entity representatives do not act directly in an illegal manner on behalf of the entity. While an entity may want to have preventative and detective controls in this area, such controls are not within the scope of ICOFR as defined by the SEC.

Violations of insider trading laws do not have a direct impact on the entity's financial statements although they may have an indirect (and potentially delayed) impact.

— Example: Investigation of management's illegal actions may lead to the loss of confidence in the entity, which may result in its inability to raise capital and refinance the entity's debt on a timely basis, which in turn may impact presentation of debt balances in the entity's financial statements.

However, the entity should consider (and have controls in place to address) the risks related to the impact that an illegal act may have on financial reporting.

— Example: In case it is notified that a potential illegal act may have occurred, an entity should have a process and controls to ensure that the potential violation is dealt with timely and appropriately. This process and the related controls should provide reasonable assurance that the financial impact, including any relevant contingency and/or disclosure, is included in the financial statements on a timely basis.

Materiality

[4.2.90] Another concept addressed by both the SEC’s and the COSO Framework’s objective and definition of effective internal control is the concept of materiality. The SEC uses the following definition when evaluating materiality:

“A substantial likelihood that the...fact would have been viewed by the reasonable investor as having significantly altered the ‘total mix’ of information available.”

The COSO Framework defines materiality in a similar manner. It states:

“Information is material if its omission or misstatement could influence the decisions of users taken on the basis of the financial reporting. Materiality depends on the size of the item or error judged in the particular circumstances of its omission or misstatement.”

[4.2.100] Determination of materiality in financial statement presentation is an important step in management’s design of an effective system of ICOFR and in the subsequent assessment of the ICOFR by both management and external auditors. Applying materiality to the financial reporting process and the resulting financial statements enables management and external auditors to focus attention on those financial statement amounts and disclosures that could influence the decisions of the users of the financial statements. That, in turn, is key to management’s and external auditors’ ability to properly identify risks of material misstatement and controls that mitigate those risks.

11 COSO Framework, p. 66.
Given the common purpose in establishing materiality, the materiality amounts determined by management and external auditors should be within close proximity to one another and — given management’s obligation to maintain accurate books and records, as required by the SEC’s definition of effective ICOFR — materiality determined by management generally should not be higher than materiality determined by the external auditors.

As explained in more detail in chapter 11 of the ICOFR Reference Guide — Identifying and Evaluating Deficiencies, materiality also is a key consideration when evaluating the severity of identified deficiencies in internal control in connection with Principle 17 of the COSO Framework. A material weakness is defined as a deficiency, or a combination of deficiencies, in ICOFR such that there is a reasonable possibility of a material misstatement of the entity’s annual or interim financial statements. Given this definition, evaluation of ICOFR deficiencies and conclusion on the effectiveness of the entity’s ICOFR require management to carefully determine an appropriate measure of materiality in the entity’s financial statement presentation.

There are subtle but distinct differences between materiality used in Risk Assessment for scoping and understanding risks and the materiality used in connection with the Monitoring Activities component of internal control to evaluate deficiencies. In general, there is only one amount determined as materiality for planning purposes, and that planning materiality is cascaded through the organization so a proper ICOFR scoping and control design can be accomplished. Materiality used when evaluating deficiencies, on the other hand, is an evaluation of whether a known deficiency would be viewed by the reasonable investor as having significantly altered the total mix of information available. The planning materiality used in Risk Assessment can be a data point when considering whether a known deficiency would rise to the level of a material weakness, but there are many other factors to be considered, including those factors set forth in the SEC Staff Accounting Bulletin No. 99 (SAB 99). Chapter 11 of the ICOFR Reference Guide — Identifying and Evaluating Deficiencies explains the process of determining the severity of known deficiencies in further detail.

While the planning materiality used in Risk Assessment and the materiality measure used to evaluate identified control deficiencies impacting specific financial statement amounts or disclosures may be different amounts, they nonetheless should be within a reasonable proximity to one another as they are closely related. For example, if an entity determined planning materiality in Risk Assessment to be $100 million, but determines that there is a deficiency that could result in a misstatement in, for example, revenue of $10 million that is a material weakness, this may call into question whether planning materiality was correctly determined and may impact the reasonable investor’s conclusions as to whether the entity correctly scoped components and significant accounts for purposes of its ICOFR design and assessment.

To establish a measure of planning materiality that is not likely to stray too far from materiality used when evaluating a known deficiency, management should consider both quantitative and qualitative factors (those described in SAB 99) when establishing its planning materiality.

Planning materiality is set at the consolidated financial statements level and should be established or re-evaluated on an at least annual basis — more frequently, if changes in external or internal factors indicate a need for re-evaluation. It is also important to remember that consideration of materiality in the design or assessment of ICOFR does not remove or lessen management’s obligation to maintain accurate accounting records under the rules of the SEC.

As discussed later in this chapter, management may wish to apply a lower level of planning materiality to specific risks identified as fraud risks.
Financial Statements Should Reflect the Entity’s Activities

[4.2.170] The third point of focus underlying Principle 6 of the COSO Framework requires that the financial statements prepared by management be reflective of the entity’s business activities. Therefore, when determining whether the entity’s system of ICOFR complies with Principle 6, management and external auditors also should consider the qualitative characteristics of the entity’s financial statements and the controls designed to achieve these characteristics. The relevant qualitative characteristics include consideration of whether the financial statements: 13

— Are relevant, including whether the financial statements include information that is capable of making a difference in user decisions;
— Provide a faithful representation of the entity’s financial position and results, including whether the information is complete, neutral, and free from error;
— Are comparable, including whether the information can be compared with similar information about other entities or information about the same entity for other periods of time;
— Are verifiable, including whether reasonable, informed persons can reach consensus that a particular depiction is a faithful representation;
— Are timely; and
— Are understandable, including whether the information is classified, characterized, and presented clearly and concisely.

In general, entities comply with the requirements of the third point of focus of Principle 6 by consistently applying appropriate GAAP in their financial reporting.

13 COSO Framework, p. 66.
4.3 Principle 7: Identifying and Analyzing Risks

The second Principle in the Risk Assessment component relates to identifying and analyzing risk. This is a very broad principle that overlaps considerably with Principles 8 and 9. In fact, those principles could be viewed as sub-principles of Principle 7. The following Illustration provides examples of questions that may be asked to get a broad understanding of whether the Principle has been met. The rest of this section will provide additional commentary and illustrations that further discuss the principle.

### Illustration 4.4:
Considerations for Principle 7 of Risk Assessment

<table>
<thead>
<tr>
<th>Points of Focus</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Includes entity, subsidiary, division, operating unit, and functional levels</td>
<td>— Based on planning materiality, has the entity scoped its components appropriately?</td>
</tr>
<tr>
<td>Analyzes internal and external factors</td>
<td>— Based on planning materiality, has the entity scoped its significant accounts appropriately?</td>
</tr>
<tr>
<td>Involves appropriate levels of management</td>
<td>— Does the entity perform or update its risk assessment on an at least annual basis and more frequently if changes in circumstances indicate a need for a reassessment?</td>
</tr>
<tr>
<td>Estimates significance of risks identified</td>
<td>— Does the entity’s risk assessment process involve appropriate levels of management, including key personnel from throughout the entity, such as Legal, HR, IT, or management in other locations?</td>
</tr>
<tr>
<td>Determines how to respond to risks</td>
<td>— Does the entity-wide risk assessment process focus sufficiently on risks to achieving effective ICOFR?</td>
</tr>
<tr>
<td></td>
<td>— Is the entity’s risk assessment process designed to capture both internal factors (e.g., change in management responsibilities, IT changes) as well as external factors (e.g., economic changes, changes in customer demand)?</td>
</tr>
<tr>
<td></td>
<td>— Does the entity link the identified risks to the relevant financial statement assertions, significant accounts and disclosures across all levels?</td>
</tr>
<tr>
<td></td>
<td>— Does the entity consider the significance of the identified risks in terms of the likelihood of the risk occurring and its impact as well as velocity (or speed) to impact upon occurrence of the risk and persistence (or duration of time) of impact after occurrence of the risk?</td>
</tr>
<tr>
<td></td>
<td>— Does the risk assessment process address how the risks are managed, how much risk is tolerated, and what is done to accept, avoid, reduce or share the risk at the appropriate level across the entity?</td>
</tr>
<tr>
<td></td>
<td>— Is the entity’s board of directors or its designated committee appropriately involved in the risk assessment process?</td>
</tr>
</tbody>
</table>
Risk Assessment at the Process Level

One particular aspect of Principle 7 is so critical to ICOFR that an entire chapter of the ICOFR Reference Guide has been devoted to it: namely, understanding the business process activities and the flow of data from initiation to reporting and then identifying the “what could go wrongs” within each business process so that the control activities can be designed appropriately. That information is discussed in chapter 5 of the ICOFR Reference Guide – Risk Assessment—Understanding WCGWs. The rest of this chapter will discuss other important aspects of identifying and analyzing risks.

Risk Assessment at the Entity Level

Both the SEC Staff and the COSO Framework make it clear that risk assessment should be performed at various levels within the entity, following a top-down approach starting at the entity level and moving down to the business process level. The remainder of the discussion in this section will focus on risk assessment at the level of the consolidated entity and its significant components which may be subsidiaries, divisions, or operating units. We will refer to this risk assessment as “entity-level risk assessment.”

The identification and assessment of ICOFR-related risks at the entity level helps ensure that the entity has identified a comprehensive population of risks to the achievement of its financial reporting objectives. Risk assessment under Principle 7 of the COSO Framework is focused on the identification and assessment of risks of error before consideration of the effect of any related controls. Risks of fraud are considered in connection with Principle 8 which is analyzed in greater detail in section 4.4 of this chapter.

An entity-level risk assessment is not the same as an Enterprise Risk Management (ERM) analysis, which focuses on risks both inside and outside of financial reporting. A robust ERM or similar analysis performed by the entity (see Illustration 4.7 below) may, however, provide a good starting point to a comprehensive risk assessment under Principle 7 of the COSO Framework. Management may be able to use the results of the ERM analysis to determine whether any of the identified risks have a potential ICOFR implication or whether there are specific ICOFR risks at the entity level that were not contemplated in the broader ERM analysis.

---

Illustration 4.5: Entity-Wide Risk Assessment

The following are examples of entity-wide events that may have a financial reporting risk:

**Layoffs** – may lead to disgruntled employees who may be incentivized to commit fraud before leaving, may leave resources constrained, may result in new lower-skilled people assuming roles that require them to perform important ICOFR controls.

**New personnel** – may perform controls in an inadequate manner due to unfamiliarity or lack of qualification.

**Changes in GAAP** – may cause the need for changes in how underlying data is captured, generated, analyzed, or reported, also resulting in new WCGWs and a need to design controls to mitigate those new WCGWs.

**Changes in third-party service providers** – may cause changes to the way the data is provided to and received from the third-party, and may cause a change to the way the third-party processes data.

**Changes in business strategy** – may cause some assets to be discontinued and impaired, may cause a change in the entity’s determination of materiality.

**Entrance into new geographic markets** – may present unknowns with respect to valuation of receivables, may cause new risks for safeguarding of assets.

[4.3.60] If identified events have no financial reporting impact, they are not required to be considered further when evaluating ICOFR. If the identified events have or could have a financial reporting impact, like the ones identified in the Illustration above, the entity considers the significant accounts and relevant assertions that may be impacted, as well as the significance of each risk impacting ICOFR.

[4.3.70] 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 its impact on the entity’s financial statements.
### Illustration 4.6: Assessing the Significance of Risks

<table>
<thead>
<tr>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>A large reduction in force (RIF) across the entity or within the finance department may be more likely to have an ICOFR impact (and thus merit an ICOFR response) than a small RIF concentrated in an area that doesn’t handle ICOFR directly (and thus may merit no ICOFR response).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pace of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>The entrance into a new geographic market may not cause an immediate ICOFR impact if the entrance is slow and methodical (and thus may merit monitoring but no ICOFR response in the current year). But if the new market is expected to be one of high growth relatively quickly, the risk may have greater significance in the current year (and thus merit an ICOFR response).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Potential Magnitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>A change in a third-party service provider that handles processing of 50% of revenue transactions would have a higher potential magnitude (and thus merit an ICOFR response) than a third-party service provider that handles processing of legal claims where the entity has multiple methods to determine the complete population of legal claims (and thus may merit no ICOFR response).</td>
</tr>
</tbody>
</table>

---

[4.3.80] Once identified and assessed as to significance, risks to the achievement of the entity’s financial reporting objectives require an appropriate ICOFR response. Not all ICOFR responses are required to be fashioned with the same level of effort or intensity—a risk of fraudulent revenue recognition likely 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 the next section for a discussion of significant accounts);
- The accounting literature governing the significant accounts should be understood;
- The process of the transaction or estimate that drives the accounting should be understood from initiation to reporting and process-level WCGWs should be identified (see chapter 5 of the ICOFR Reference Guide – Risk Assessment – Understanding WCGWs); and
- Appropriate controls should be designed, implemented, operated and monitored (see chapter 6 of the ICOFR Reference Guide – Control Activities, and chapter 10 – Monitoring).

[4.3.90] Risk assessment at the entity level should be formally performed, or updated, and documented on an at least annual basis and more frequently if changes in internal or external factors indicate a need for re-evaluation.
Entity-level risk assessment should be **conducted by appropriate levels of management** with sufficient knowledge and understanding of the entity’s business, its organization, operations, and processes to properly consider the sources and likelihood of potential misstatements in the entity’s financial statements. 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 the entire board of directors to assist these bodies in fulfilling their oversight responsibilities regarding the entity’s development and performance of internal control over financial reporting under Principle 2 of the COSO Framework.

Given that much of the risk assessment process at the entity level may take place in meetings and discussions, including at the board of directors and senior management level, **timely documentation of the risk assessment activities** undertaken by the entity and their results is key to an effective assessment of the entity’s ICOFR by both management and external auditors. The documentation may take the form of meeting agendas and minutes, memoranda documenting the key steps of the risk assessment process, presentation materials summarizing findings and conclusions from risk assessment, as well as matrices showing evaluation of the significance of the identified risks and linking those risks to the relevant assertions over significant accounts and disclosures.

**Illustration 4.7:**
Comprehensive Risk Assessment

Scenario:
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, FP&A personnel meet with senior management and representatives of the various functions of the entity and all of its significant locations. 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 which might 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 team meet with FP&A personnel to establish that the process gives appropriate consideration to risks to reliable financial reporting in accordance with U.S. GAAP and SEC rules and regulations. They also join FP&A personnel in various planning and risk assessment activities (meetings, workshops, brainstorming sessions, etc.), as considered necessary, to provide appropriate representation in the process of personnel with sufficient understanding of the entity’s financial reporting objectives.
All risks identified in connection with the annual planning and risk assessment led by FP&A personnel are summarized in a spreadsheet and analyzed for potential impacts on the financial reporting process. Risks identified as relevant to financial reporting are then separately analyzed as to their severity by representatives of internal audit and the finance management team, including the entity’s CFO and Controller, and linked to the impacted 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 significant financial reporting risks to the entity’s audit committee on an annual basis in connection with the committee’s review and approval of the internal audit’s annual testing plan. They also provide an overview of the risk assessment process undertaken by management. Audit committee members consider the reasonableness of the identified population of significant risks 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 the internal audit’s annual testing plan.

Scoping of Significant Accounts

[4.3.130] Planning materiality established at the consolidated entity level corresponds with the ultimate objective of effective ICOFR, defined in SEC Regulation 13a-15(f) as “reliable financial reporting and financial statements prepared in accordance with GAAP.” Given the complex and multilayered structure of many of today’s businesses, it is important for management to “translate” these consolidated entity level concepts into relevant sub-objectives and measures of materiality at the component (i.e., division, subsidiary, operating unit) and business process level.

[4.3.140] The Internal Control over External Financial Reporting: A Compendium of Approaches and Examples, a companion document to the COSO Framework, defines sub-objectives 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 GAAP. However, in order 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, existence, accuracy, valuation, obligations and rights, and presentation.

[4.3.150] 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.

[4.3.160] 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 ICOFR response.
Illustration 4.8: Consideration of Significant Accounts

Accounts that are of particular interest to investors:
If 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, the revenues, costs, and other accounts associated with that new line of business may be considered to be “significant accounts”—a material misstatement could arise in those accounts—even if they are quantitatively less than planning materiality.

Accounts that contain particular risks:
Some accounts, like the litigation accrual, or assets/liabilities associated with hedging activities, may be significant even if the current balance is less than planning materiality because the risk that they could be misstated by more than planning materiality exists (i.e., the completeness assertion is relevant).

Combination of accounts:
Some accounts may be individually insignificant, but a combination of multiple insignificant accounts may give rise to a risk of material misstatement in combination.

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 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.

 Appropriately defined significant accounts and disclosures will typically fall somewhere in between these two limits (a financial statement caption on one end and an individual general ledger account on the other end), depending on the specific circumstances of the entity, including factors such as the level of detail disclosed in the external financial statements and organization of the entity’s chart of accounts.
Thoughtful determination of significant accounts and disclosures is important for both management and external auditors. Without it, it will be difficult (or even impossible) 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 ICOFR 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. That, in turn, may require a control response that is more pervasive than what would be necessary if the account had been appropriately disaggregated and the related risk associated with an appropriate disaggregated portion of the account.

Illustration 4.9: Identifying significant accounts at an appropriate level

**Beginning with financial statement captions:**
An industrial manufacturing entity has two material revenue streams which are 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. Despite the combined presentation in the entity’s financial statements, it makes sense to identify the two streams of revenue as separate significant accounts because each of them has a different risk profile with more significant risks likely attached to revenue from multiple-deliverable arrangements. Each revenue stream also results from a different process and is subject to a separate set of controls. Without disaggregating the financial statement caption of “revenues” into the two components described above, management and external auditors will face challenges with precisely defining risks attached to the two components of revenue, assessing the significance of those risks, and linking the significant accounts to the relevant processes and controls.

**Beginning with general ledger accounts:**
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. In these circumstances, it makes sense to aggregate all general ledger sales accounts related to the physical store locations into one significant account as all these general ledger accounts have a similar risk profile and are subject to a similar set of controls. At the same time, sales made through the e-commerce sales platform will be identified as a separate significant account as they are a result of a separate process and are exposed to different risks, including risks attached to the delivery of the entity’s merchandise to its e-commerce customers and the timing of the related revenue recognition.
Scoping of Components

[4.3.220] Similar to the analysis done regarding significant accounts, management and external auditors determine which of the entity’s components (i.e., subsidiaries, divisions, or operating units) present a risk that the financial statements contain a material misstatement. 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.

[4.3.230] The only “out of scope” components (i.e., components which may be excluded from the scope of management’s and external auditors’ ICOFR assessment) are those components for which the risk that the component individually or in combination with other insignificant components includes a material misstatement is remote. Note that the term “remote” has the same meaning as in FASB Accounting Standards Codification 450 – Contingencies and relates to a future event or events whose 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.

[4.3.240] That does not mean, however, that identification and testing of process-level control activities should be performed for every significant account at every “in scope” component. Rather, there may be entity-level controls that are sufficiently designed to mitigate risks at smaller components.

[4.3.250] The SEC has been very specific about using the entity-level controls in an appropriate manner when designing and evaluating the system of ICOFR. The SEC staff stated that some entity-level controls, such as those associated with the Control Environment, are too indirectly linked to financial reporting risks and therefore “it is unlikely that management will identify only this type of entity-level controls as adequately addressing a financial reporting risk identified for a financial reporting element.”

[4.3.260] On the other hand, other entity-level controls may be designed to identify possible breakdowns in lower-level controls. For example, an entity-level control that monitors the results of operations may be designed to detect potential misstatements and investigate whether a breakdown in lower-level controls occurred. However, if the amount of potential misstatement that could exist before being detected by the monitoring control is too high, then the control may not adequately address the financial reporting risks of a financial reporting element. Such control should not be relied upon by management or external auditors to address the risk of a material misstatement in the entity’s financial statements.

[4.3.270] The third type of entity-level controls highlighted by the SEC are those controls that are “designed to operate at the process, application, transaction or account-level and at a level of precision that would adequately prevent or detect on a timely basis misstatements in one or more financial reporting elements that could result in a material misstatement. In these cases, management may not need to identify or evaluate additional controls related to that financial reporting risk.”

---

16 Ibid. pp. 18-19
17 Ibid. p. 19.
[4.3.280] If management or external auditors decide to use entity-level controls to reduce or eliminate reliance on and testing of process-level controls at some smaller components:

— Those entity-level controls must operate in a sufficiently precise manner to prevent or detect, on a timely basis, a material misstatement in the financial statements at the *would* level of assurance; and

— The greater the risk that the entity-level controls are intended to address, the more robust the entity-level controls should be.

[4.3.290] Analytical reviews and comparisons of actual results to budget are common entity-level controls exercised by management over components of the entity. If such analytical reviews are used to address risks of material misstatement in the entity’s financial statements, they need to be performed at an appropriate level of precision. The *level of precision of these controls should be documented* and evidence of their operation, including follow-up questions and related answers, are likely to be a necessary part of evidence.

[4.3.300] There is no bright line for the size of components (individually or in the aggregate) that an entity can address with these types of controls. That is because a poorly designed analytical review may not be sufficient to address the risk of a component that represents only 3% of total assets, equity, or revenue, while a well-designed and thoroughly documented analytical review may be sufficient to address the risk of material misstatement in multiple components that represent 25% or even 30% of total assets, equity, or revenue. Nonetheless, the burden is on the entity to demonstrate that these controls operate in a manner that would prevent or detect, on a timely basis, a material misstatement in the entity’s financial statements. Refer to chapter 7 of the ICOFR Reference Guide – *Management Review Controls* for further guidance regarding the design, operation, and evaluation of analytical reviews and other similar review controls that management intends to rely upon to address risks of material misstatement of the financial statements.

[4.3.310] While there is no bright line, typically if the components being covered by the kind of entity-level analytical review controls described above represent more than 25% to 30% (not to be interpreted as a bright-line safe harbor) of the entity’s assets, equity, or revenue, there will often be a need to design, operate, and evaluate some process level controls at some or all of these components. Practically speaking, it is difficult to design, execute, and test entity-level analytical review controls that are sufficient to mitigate risks in an individual component or aggregated components of an entity that are greater than, say, 25% to 30% of the entity’s consolidated financial statements.

[4.3.320] Full walkthroughs and testing of process level controls should be performed at those components that are not being covered by these types of entity-level controls (i.e., walkthroughs and process level control testing are necessary at components that would typically cover 70% to 100% of total assets, equity, and revenue).

[4.3.330] Even if a component has been classified as an insignificant component, both management and external auditors should consider whether the component includes any specific significant risks. Significant risks should be addressed through ICOFR even if they reside in components that have otherwise been determined to be individually insignificant. *Full walkthroughs and testing of process level controls are performed with reference to the relevant assertions over significant accounts associated with significant risks.*
Need for “risk tolerance” at the significant account level

In order to achieve the objective that the financial statements as a whole are free from material misstatement, the relevant assertions for each significant account should be controlled at a level lower than planning materiality.

Consider an entity that determines a planning materiality of $10 million and then designs controls to prevent or detect misstatements of $10 million or more for each significant account in its financial statements. That means that Entity A is willing to tolerate an error the size of planning materiality in each of its significant accounts. That level of risk tolerance does not adequately address the aggregation risk. In this scenario, a misstatement of $8 million in revenue and receivables and $4 million in costs and A/P might go undetected. These errors could aggregate to $12 million which is likely material to the entity’s financial statements given the planning materiality threshold of $10 million. To address the aggregation risk, the entity should establish risk tolerance for the relevant assertions over significant accounts at a level that is lower than the determined planning materiality amount.

Corresponding with the sub-objectives established at the business process level in the form of relevant assertions over significant accounts and disclosures is the concept of risk tolerance which is newly introduced by the COSO Framework. The Framework formally defines risk tolerance 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 (and external auditors) are 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 planning materiality for the financial statements as a whole.

Risk Tolerance for Significant Accounts and for Components

18 COSO Framework, p. 61.
[4.3.360] Risk tolerance is not a pro-rata allocation of planning materiality to the significant accounts. However, an amount should be assigned to each significant account that will account for aggregation risk. Typically, the amount assigned, referred to commonly as “performance materiality” or “tolerable misstatement,” is between 50% and 75% of planning materiality. However, in some cases, based on risk, the performance materiality can be lower than 50% of planning materiality. 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. As further explained in this ICOFR Reference Guide’s chapter 6 – Control Activities, and chapter 7 – Management Review Controls, risk tolerance forms the basis for determining the precision of controls the entity should design and implement to mitigate the identified risks and achieve sub-objectives of relevant business processes.

[4.3.370] Another type of risk tolerance should be considered to address an additional aspect of aggregation risk—namely, aggregation risk related to entities comprised of multiple components (i.e., divisions, subsidiaries, or operating units) where consolidated (or group) financial statements are prepared by aggregating financial information prepared for each component by either group or corporate management. For such entities, planning 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 financial statements, at the division, subsidiary, or operating unit level. Component materiality is always lower than planning materiality established at the consolidated entity level.

Illustration 4.11:
Need for “risk tolerance” at the components

In order to achieve the objective that the financial statements as a whole are free from material misstatement, aggregation risk related to components should be addressed.

Consider an entity that determines a planning materiality of $10 million and then has each component design, implement, operate, and monitor controls to prevent or detect a misstatement at the $10 million level. That level of materiality allocated to each component (component materiality) does not adequately address aggregation risk. In such a scenario, the controls are not designed to prevent or detect errors of less than $10 million and, therefore, multiple locations could have undetected errors that may aggregate to an amount greater than $10 million at the consolidated entity level. To address the aggregation risk, the entity should establish component materiality for its individual components at a level that is lower than the determined planning materiality at the consolidated entity level.
Similar to performance materiality established for significant accounts and disclosures, component materiality is typically not a simple pro-rata allocation of planning materiality to the components (i.e., the sum of the assigned component materiality for all components is likely to exceed 100% of the consolidated planning materiality). However, component materiality for individual components should be established at a sufficient discount from planning materiality to adequately address the aggregation risk that exists at the consolidated financial statement level. The size of the discount from planning materiality may differ for each component and should be commensurate with the assessed aggregation risk taking into consideration factors such as:

- The number and relative size of the components;
- Nature and extent of misstatements expected in each component in the current period;
- Nature and extent of accounting judgments made at the component level;
- Proportion of the consolidated entity which is not subject to effectively designed and operating controls that would prevent or detect a material misstatement of the entity’s financial statements.

As a general rule of thumb, careful consideration should be afforded whenever the sum of individual component materiality is greater than, say, 3–4 times materiality determined at the consolidated financial statement level for entities comprised of 5–20 components. As the number of components increases above 20 and the sum of individual component materiality rises to be greater than the above rule-of-thumb multiple of 3–4 times, the aggregation risk is also likely to increase, thus necessitating an even more careful analysis. On the other hand, the aggregate of component materiality for groups consisting of a smaller number of similarly sized components should be carefully evaluated at potentially an even lower multiple to group materiality than the rule-of-thumb multiple indicated above.

Further, when a component determines performance materiality (for use at the significant account level), it uses component materiality as the benchmark from which to apply the 50% to 75% amount; it does not use the entity-wide planning materiality. The combination of component materiality and performance materiality determined based on the component materiality amount is an effective way to address the aggregation risk at the consolidated financial statement level. The higher the aggregation risk identified, the lower performance materiality may need to be set relative to component materiality.

Determination of component materiality requires a significant degree of judgment. Certain exceptions from the general rules described above may exist depending on the specific circumstances of the entity, its composition, and organization of its financial reporting process. For example:

- If one component (i.e., division, subsidiary, or operating unit) represents substantially all (say, 85% or more) of the consolidated financial statements, it may be appropriate to establish component materiality for that component using a pro-rata allocation of the planning materiality determined at the consolidated financial statements level.
— Also, for certain significant accounts in the consolidated financial statements which are concentrated in only one component of the group or which are established by management (and audited by external auditors) in a centralized, groupwide manner, it may be appropriate to address the aggregation risk related to those accounts by simply reducing the applicable performance materiality relative to planning materiality determined at the consolidated financial statements level.

[4.3.420] It is important for management to document their determination of planning materiality and ICOFR objectives at the entity level and their translation of these entity-level concepts into relevant sub-objectives and measures of risk tolerance at the division, subsidiary, operating unit and business process level. Timely documentation of these considerations is key to an effective assessment of the entity’s ICOFR by both management and external auditors. The documentation may take the form of memoranda documenting entity-level considerations, such as planning materiality, and scoping matrices presenting 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 how these items link to the related business processes and internal controls.
Key takeaways:

Identifying and Analyzing Risks

1. Conduct risk assessment at all relevant levels within the entity, from the consolidated entity level down to the business process level. Involve appropriate members of management and other employees in the assessment process.

2. Link the identified risks to the relevant assertions over significant accounts and disclosures.

3. Determine significant components of the entity and their significant accounts as part of scoping.

4. Establish component materiality for components and performance materiality for significant accounts.

5. Carefully evaluate situations in which the aggregate of established component materialities is greater than, say, 3–4 times the planning materiality for entities comprised of a large number of components.

6. Prepare timely documentation of appropriate consideration of planning materiality, components, significant accounts, component materiality and performance, materiality.
[4.4.10] Principle 8 of the Risk Assessment component of the COSO Framework addresses the risks of fraud in the organization. The following Illustration provides examples of questions that may be asked to get a broad understanding of whether the Principle has been met. The rest of this section will provide additional commentary and illustrations that further discuss the assessment of fraud in the organization for purposes of designing and evaluating ICOFR.

Illustration 4.12: Considerations for Principle 8 of Risk Assessment

<table>
<thead>
<tr>
<th>Points of Focus</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Considers various types of fraud (applicable to ICOFR)</td>
<td>— Does the entity have a process for a continuous comprehensive fraud risk assessment that can identify various types of fraud (including fraudulent financial reporting, material safeguarding of assets issues, and management override of controls) which could impact the entity?</td>
</tr>
<tr>
<td>— Assesses incentives and pressures</td>
<td>— Does the entity consider in its fraud risk assessment process the various factors which may impact or create fraud risks, including incentives and pressures, opportunities, and attitudes and rationalizations (the “fraud risk triangle”)?</td>
</tr>
<tr>
<td>— Assesses opportunities</td>
<td>— Does the entity involve appropriate personnel at various levels across the organization in its fraud risk assessment, including interviews with employees to assess the incentives and pressures to manipulate earnings, misappropriate assets, or alter records?</td>
</tr>
<tr>
<td>— Assesses attitudes and rationalizations</td>
<td>— Does the entity consider, assess, and reassess compensation programs, if necessary?</td>
</tr>
<tr>
<td></td>
<td>— How does the entity manage fraud risk across the organization and at all levels (including its segments and subsidiary, division, operating unit, and functional levels) regarding the financial statement accounts and assertions?</td>
</tr>
<tr>
<td></td>
<td>— How does the board of directors oversee the identification, assessment, and evaluation of fraud risks, including opportunities for and occurrences of management override of controls?</td>
</tr>
<tr>
<td></td>
<td>— Do management and the board of directors maintain adequate oversight, an appropriate level of skepticism, and allow for proper reporting of actual or suspected fraud by implementing a whistleblower program?</td>
</tr>
<tr>
<td></td>
<td>— Has the entity identified controls that are responsive to the identified fraud risks, including the risk of bias and management override of controls?</td>
</tr>
</tbody>
</table>
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. At the same time, as shown by major corporate fraud scandals in nearly every decade of the past century, fraud can have a significant negative impact on an entity’s financial reporting process, the reliability of its financial statements, and investor confidence.

Therefore, both the SEC Staff and the COSO Framework make it clear that an appropriate Risk Assessment should specifically consider the vulnerability of the entity to fraudulent activity.19

Principle 8 of the COSO Framework identifies four types of fraud that require consideration in an entity’s risk assessment process:

- Fraudulent financial reporting;
- Misappropriation of assets;
- Corruption and other illegal acts; and
- Management override of controls.

As discussed in section 4.2, compliance with laws and regulations comes into the scope of ICOFR when it relates to laws and regulations that have a direct impact on the preparation of the financial statements. Entities should have controls in place that are directed at mitigating the risk of noncompliance with such laws and regulations. In the case of other illegal acts, entities are only expected to have controls in place that will allow them to timely evaluate (and record or disclose, as appropriate) impacts on the financial statements of alleged violations of laws and regulations of which they have become aware. The other types of fraud are generally within the scope of ICOFR, subject to materiality considerations. See examples and Illustrations following paragraph 4.2.70 of this chapter for further guidance.

It is expected that fraud risk assessment under Principle 8 will follow a similar approach and process as the wider risk assessment under Principle 7, i.e., that it will be comprehensive, performed at various levels within the entity, and involve appropriate members of management and other employees with an appropriate oversight from the entity’s board of directors. Fraud risk assessment under the COSO Framework should not be viewed as a compliance exercise owned solely by internal audit or a SOX compliance group.

This expectation is based on the guidance in the COSO Framework which indicates that fraud risk assessment under Principle 8 of the Framework represents an aspect of the wider risk assessment process described in Principle 7. Taking this into account, the COSO Framework specifies that the actions being conducted as part of applying Principle 8 link closely to the preceding Principle 7. This is reasonable given that both fraud risks (assessed under Principle 8) and risks of error (assessed under Principle 7), if not mitigated by controls, may lead to a material financial statement misstatement. The key distinguishing factor between fraud and error is whether the underlying action that results in the misstatement is intentional or unintentional.

20 COSO Framework, p. 78
While the extent of activities required for the evaluation of fraud risks is commensurate with the size and complexity of the entity's operations and financial reporting environment, this evaluation is never a cursory assessment. The SEC Staff has stated:

“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 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.”

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 crosses over with many of the processes, controls, and programs considered in the Control Environment, such as whistleblower hotlines, tone at the top, and how it is communicated throughout the organization, and how the organization responds when fraud or potential fraud has been identified. These broad considerations and programs are critical to effective fraud prevention, and therefore are considered when determining whether fraud is effectively mitigated.

However, consideration of the 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; and

— Identifying specific fraud risks at the financial statement and assertion level.

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 (see chapter 6 of the ICFR Reference Guide – Control Activities), and then monitors the effectiveness of those controls (see chapter 10 – Monitoring).

Identifying Fraud Risk Factors

Identifying fraud risk factors means to assess the three factors of the “fraud risk triangle”: incentives and pressures, opportunities, and attitudes and rationalizations. At least one of these factors is generally present when fraud exists. However, 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.

Incentives and pressures is typically assessed 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, etc.) and who is exposed to those incentives and pressures (e.g., management, sales representatives, finance personnel, etc.).

An analysis of compensation plans for key individuals is likely necessary to fully understand whether an incentive 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 an employee to commit the fraud (e.g., inventory that is not properly secured and thus subject to theft and resale by an employee, or sensitive financial statement estimates that may be manipulated resulting in a material impact on an entity’s earnings).

**Attitudes and rationalizations** is a subjective analysis which 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 members of management understand the importance of accurate financial reporting (e.g., a CEO who is unduly interested in improving financial results may either have an attitude or create rationalization in others that foster an environment where fraud might be tolerated).

The COSO Framework identifies the following factors that may influence the various ways that fraud in financial reporting could occur:

- 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 (Incentives);
- Nature of technology and management’s ability to manipulate information (Opportunity);
- Unusual or complex transactions subject to significant management influence (Opportunity or Attitude); and
- Vulnerability to management override and potential schemes to circumvent existing control activities (Opportunity or Attitude).

See Appendix 4.1 for a more comprehensive list of examples of fraud risk factors, circumstances that may indicate a possibility of fraud, and frauds.

**Identifying Assertion Level Fraud Risks**

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. Refer to chapter 6 of the ICOFR Reference Guide – Control Activities for guidance regarding the design and evaluation of antifraud controls. In the unusual case when it is not possible to link the identified fraud risk to a specific financial statement assertion, management and external auditors should consider whether the identified fraud risk is defined in an overly broad manner or whether it truly has a pervasive impact on the entity’s financial statements (which will require an appropriately robust control response).
Illustration 4.13:
Linking a fraud risk to a financial statement assertion

Consistent with the factors set forth in the COSO Framework, an entity determined that there is pressure on senior management to manipulate earnings. While this is a good start, it is necessary for management to link this fraud risk to specific financial statement accounts and assertions. For example, depending on the entity:

- Management may increase earnings artificially by recording fictitious entries to increase revenue or decrease expenses.
- Management may have the ability to enact certain favorable transactions with related parties that can be reversed or unwound in a later period.
- Management may have the ability to manipulate significant estimates to inflate earnings now or establish “cookie jar” reserves.

It is critical to link the fraud risk to an assertion level risk so that the appropriate controls that mitigate those risks can be identified and evaluated.

[4.4.190] When assertion-level fraud risks are identified, the entity and external auditors 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 should be identified:

- Posting a journal entry to record additional revenue (management override of controls);
- Entering into side agreements with customers (e.g., an agreement by the customer to take delivery of the goods before they are wanted or needed with an understanding that the goods can be returned after period-end or 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 or the determination or allocation of fair value in multiple element arrangements).

[4.4.200] 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. In addition, documentation concerning management’s thought process for identifying or not identifying certain risks as relevant (i.e., requiring an ICOFR response) is important so that a prudent official can understand and evaluate the 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 in order to truly achieve Principle 8:

- 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 discussion with key personnel at the entity's corporate head office and all significant locations;
- These discussions 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, Risk Management Office personnel should analyze the "fraud risk triangle" – indicators of 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 reported to the Audit Committee on an at least annual basis.

The various fraud risk assessment activities summarized above (meetings, presentations, analyses, etc.) will be added to the “COSO 2013 Mapping” tool and linked with Principle 8. The agendas and minutes from the various meetings, the completed Risk and Control Matrix, presentation to the Audit Committee, and inquiries of participants in the fraud risk assessment activities will serve as evidence of the entity's thoughtful top-down and comprehensive approach to fraud risk identification and analysis under Principle 8.
Designing and Monitoring Controls Responsive to Fraud Risks

Once the fraud risks are clearly defined, the entity designs, implements, operates, and monitors controls that are responsive to the fraud risks. For example, appropriate controls for the following assertion-level fraud risks may include:

<table>
<thead>
<tr>
<th>Fraud Risks:</th>
<th>Example controls:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Posting a journal entry to record additional revenue</td>
<td>Review by an objective party of all manual journal entries posted to the revenue account and a subledger to general ledger reconciliation</td>
</tr>
<tr>
<td>Entering into side agreements with customers</td>
<td>Confirmations with customers for side agreements, or a post-period-end review of returns or aged receivables looking specifically for indicators of side agreements</td>
</tr>
<tr>
<td>Marking items as shipped in the system when they have not yet been physically shipped</td>
<td>Sweeps of loading docks and warehouse facilities, review of shipping terms to customer requests, or similar controls by appropriate personnel</td>
</tr>
<tr>
<td>Manipulating estimates related to revenue</td>
<td>Review of key estimates by appropriate personnel, including comparison of key estimates to prior periods</td>
</tr>
</tbody>
</table>

Designing and monitoring of controls are discussed in more detail in chapters 6 and 10 of the ICOFR Reference Guide, respectively. See also Appendix 4.1 for a more comprehensive list of examples of fraud risk factors, circumstances that may indicate a possibility of fraud, and frauds.

One important note to remember is that if an entity has identified an assertion-level fraud risk, it is expected that there will be incremental effort—either additional controls added to mitigate the risk, or specific changes to the design or operating effectiveness of existing controls, to mitigate the risk. In the example of the side agreements 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.
Other Considerations With Respect to Fraud Risks

**[4.4.240]** Recognizing that the objective of effective ICOFR is to prevent, or detect, on a timely basis a **material misstatement** due to fraud or error, 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 as a result of those fraud risks are lower than the **quantitative measure of planning materiality**. This is due to the **qualitative considerations** related to misstatements caused by fraud in the financial statements such as intent to achieve a particular outcome (e.g., meet analysts' expectations, which in some cases could be achieved through manipulation in an amount that is lower than planning materiality), involvement in the fraud by members of senior management, questions about pervasiveness of the fraud and its impact on the reliability of the entire financial statements, etc. Management and external auditors should appropriately consider these qualitative impacts of fraud in addition to the quantitative materiality of any potential misstatements when identifying and evaluating risks of fraud in the entity's financial reporting process and designing and evaluating relevant antifraud controls.

**[4.4.250]** The COSO 2013 Framework emphasizes the **important role of an appropriate oversight of an entity’s fraud risk assessment process by the board of directors** or its subset (e.g., audit committee). This is particularly important with reference to the risk of management override of controls. The COSO Framework states that the board of directors should oversee the assessment of the risk of fraud, and in particular the risk of management override of controls, and challenge management depending on the circumstances.²³ For example, based on the results of the entity’s risk assessment process, the board might select a sample of significant accounting estimates in the entity’s financial statements and review and challenge (as part of the oversight role, not the role of management) management’s key judgments about these estimates on a periodic basis. Similar oversight might be warranted when it comes to accounting and financial reporting for significant unusual transactions and other matters which may be prone to bias and override of controls.

**[4.4.260]** See Appendix 4.2 for a template that entities may use to help document considerations of fraud risk factors, assertion-level fraud risks, and related controls.

---

²³ COSO Framework, p. 81.
Key takeaways:

Assessing the Risk of Fraud

1. **Both the SEC and the COSO 2013 Framework require an assessment of the risk of fraud.** Management and external auditors should consider the incentives and pressures, opportunities as well as attitudes and rationalizations of employees (the fraud risk triangle) which may lead to fraud risks within the entity.

2. **Fraud risk assessment should be comprehensive,** cover various levels within the entity and involve appropriate members of management and employees. It should not be viewed as a compliance exercise owned solely by internal audit or a SOX compliance group.

3. **Identified fraud risks should be cascaded across the organization and linked to relevant financial statement assertions.** In order for controls to be designed to mitigate the fraud risks, an assessment should be performed to determine which financial statement accounts and assertions are likely to be manipulated because of the fraud risks.

4. **Identify and design controls that are responsive to fraud risks.** As discussed in chapter 6 of the ICOFR Reference Guide – Control Activities, the fraud risk assessment serves as the basis for determining what controls are needed to address the fraud risk.
Principle 9: Identifying and Assessing Significant Changes

[4.5.10] The COSO Framework describes Risk Assessment as a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Principle 9 of the COSO Framework represents the continuous portion of the risk assessment process. It focuses on changes in the entity's business model, its leadership, and external environment and thus bridges the period in between the periodic risk assessment activities that entities perform under Principles 7 and 8.

[4.5.20] One could argue that Principle 9 is really a subset of Principle 7 (that Principle 7 really cannot be performed appropriately without also performing Principle 9). This may also be true for the relationship between Principles 7 and 8. However, COSO wanted to emphasize the importance of Principles 8 and 9 and, therefore, created separate principles for them. Entities do not need to be concerned about the overlap among the principles as long as the risk assessment procedures performed cover all aspects of effective risk assessment.

[4.5.30] The following Illustration provides examples of questions that may be asked to get a broad understanding of whether Principle 9 of the COSO Framework has been met. The rest of this section will provide additional commentary and illustrations that further discuss the entity's monitoring of changes that could significantly impact its systems of ICOFR.

“As part of an ongoing assessment of “what could go wrong” within a financial reporting element, it is critical that management consider the nature and extent of any changes in the risks to reliable financial reporting. Such changes can result from a variety of sources, including company reorganization, nature of transactions entered into, overall business environment, and accounting requirements. A few recent examples of such events discussed with registrants in the comment process include:

— Expansion into a new foreign location;
— Growth in operations through the use of variable interest entities (VIEs);
— Reaching a sales agreement with a new customer under terms different from those with any existing customer; and
— Increases in expenditures for environmental clean-up of existing remediation sites.”

— Kevin Stout, SEC Senior Associate Chief Accountant

24 COSO Framework, p. 59.
25 Kevin M. Stout (December 2015), SEC Senior Associate Chief Accountant, Remarks before the 2014 AICPA Conference on Current SEC and PCAOB Developments
Principle 9 of the COSO Framework requires management to assess changes in the external environment (e.g., new laws, new accounting pronouncements, new stock exchange regulations), the business model (e.g., launch of new products, geographical expansion, restructuring) and changes in leadership of the organization (e.g., new executive leadership, turnover in key financial reporting positions) and consider how such changes may impact the entity’s system of ICOFR.

Achieving Principle 9 requires having controls in place to early identify and communicate changes that may have a significant impact on financial reporting and assess the risks resulting from those changes. The COSO Framework refers to such controls as "early warning systems."

Experience suggests that routine business processes are well controlled by entities. But very often when something new or unusual happens, the existing system of ICOFR is not prepared to process the new events or transactions in a controlled manner. This, in turn, may lead to material errors in the financial statements and material weaknesses in internal control. Identifying new transactions and events ahead of time through an entity’s “early warning systems” allows the entity time to make the necessary adjustments to the existing system of ICOFR.

---

Illustration 4.15: Considerations for Principle 9 of Risk Assessment

<table>
<thead>
<tr>
<th>Points of Focus</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Assesses changes in the external environment</td>
<td>— Does the entity have a process to identify and assess internal and external changes in operations that could impact the design and operating effectiveness of ICOFR?</td>
</tr>
<tr>
<td>— Assesses changes in the business model</td>
<td>— Does this process include monitoring of external information sources (i.e., news channels, trade publications, Web sites, etc.) to identify changes in the marketplace and other external factors that could directly or indirectly affect their business operations and, therefore, ICOFR?</td>
</tr>
<tr>
<td>— Assesses changes in leadership</td>
<td>— Does the entity consider the effect of changes in the organization, whether through acquisitions or changes in business model, or changes in personnel and the implications to ICOFR?</td>
</tr>
</tbody>
</table>

[4.5.40] Principle 9 of the COSO Framework requires management to assess changes in the external environment (e.g., new laws, new accounting pronouncements, new stock exchange regulations), the business model (e.g., launch of new products, geographical expansion, restructuring) and changes in leadership of the organization (e.g., new executive leadership, turnover in key financial reporting positions) and consider how such changes may impact the entity’s system of ICOFR.

[4.5.50] Achieving Principle 9 requires having controls in place to early identify and communicate changes that may have a significant impact on financial reporting and assess the risks resulting from those changes. The COSO Framework refers to such controls as "early warning systems."

[4.5.60] As discussed earlier in this chapter, these early warning systems likely overlap with programs discussed in the Control Environment and the concepts discussed related to Principle 7 in section 4.3.

[4.5.70] Experience suggests that routine business processes are well controlled by entities. But very often when something new or unusual happens, the existing system of ICOFR is not prepared to process the new events or transactions in a controlled manner. This, in turn, may lead to material errors in the financial statements and material weaknesses in internal control. Identifying new transactions and events ahead of time through an entity’s “early warning systems” allows the entity time to make the necessary adjustments to the existing system of ICOFR.
Illustration 4.16:  
Example of significant changes

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

Action:
This change should be identified and analyzed for any potential impact on ICOFR. 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 ICOFR in the area of valuation of securities will need to be enhanced given the new risks.

Other situations of significant change may include:
— Business combinations and other nonroutine transactions, such as issuance of debt, restructuring, unusual sales transactions, or related-party transactions—given the nonroutine nature of these transactions, management may need to identify risks and design controls that were not previously part of ICOFR.
— Changes in organizational structure, potentially altering how the Chief Operating Decision Maker views the business and whether there is a change in reporting units.
— Deterioration of the results of operations, increasing the risk of impairment, and potentially, the robustness of the analysis and related controls over impairment.

Key takeaways:
Identifying and Assessing Significant Changes

1. **Risk assessment considers changes that could have an impact on ICOFR.** Identified changes are typically analyzed down to the process level.

2. Many material weaknesses in ICOFR are rooted in circumstances where changes occurred, but the ICOFR implications were not identified or thoroughly considered.
4.1 Examples of Fraud Risk Factors, Circumstances that Indicate the Possibility of Fraud, and Frauds

4.2 Template for Documenting Fraud Risk Factors, Assertion-Level Fraud Risk, and Related Responses
Chapter 5
Risk assessment - understanding WCGWS
The COSO Framework emphasizes that entities should consider risks at various levels of their organizational structure, including the overall entity and its subunits, and processes such as sales, human resources, marketing, production, and purchasing.\(^1\) The COSO Framework further explains that dealing with risks at the process level helps management focus on the achievement of objectives and/or sub objectives of internal control that have cascaded down from the entity-level objectives. Furthermore, successfully assessing risks at the transaction level also contributes to maintaining acceptable levels of risk at the entity level.\(^2\)

The COSO Framework’s emphasis on Risk Assessment at the process level is consistent with the guidance of the Public Company Accounting Oversight Board (PCAOB) for external auditors. To understand the likely sources of misstatement of the financial statements and select the appropriate controls to test, PCAOB Auditing Standard (AS) No. 5 paragraph 34 states that external auditors should:

— **Understand the flow of transactions** related to the relevant assertions, including how these transactions are initiated, authorized, processed, and recorded;

— Verify that they have identified the **points within the entity’s processes at which a misstatement—including a misstatement due to fraud—could arise** that, individually or in combination with others misstatements, would be material;

— **Identify the controls** that management has implemented to address these potential misstatements; and

— Identify the controls that management has implemented over the prevention or timely detection of unauthorized acquisition, use, or disposition of the entity’s assets that could result in a material misstatement of the financial statements.

An entity’s understanding of the likely sources of misstatements can be documented in the form of flowcharts or narratives, or some combination of the two. Generally, it is more effective and efficient to use flowcharts supplemented by brief narratives, rather than narratives alone.

---

2 Ibid. p. 73.
As discussed in chapter 4 of the ICOFR Reference Guide – Risk Assessment, there is one particular aspect of Principle 7 of the COSO Framework that is so critical to internal control over financial reporting (ICOFR) that it needs to be captured in this separate chapter of the Guide: namely, understanding the business process activities and the flow of data from initiation to reporting and then identifying the risks within the process (the so called “What Could Go Wrongs” or WCGWs) so that the necessary control activities can be designed appropriately.

Inadequate understanding of a business process and the related WCGWs 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 ICOFR assessment process.

Typically an entity demonstrates that it understands the process by describing it in a flowchart, a narrative, or a combination of the two. See section 5.4 for further discussion on documentation.

To thoroughly understand the process, an entity and its external auditors must:

- Distinguish between the process and control activities;
- Start with the initiation of the transaction;
- Understand each step in the process focusing on when data moves from one step to the next; and
- End with when the transaction gets recorded in the general ledger (and ultimately reported).

With respect to distinguishing between the process and the control, the importance of understanding the concept cannot be overstated. Outside of ICOFR, the terms “process” and “controls” may be used interchangeably. However, when discussing ICOFR, the term “process” refers to activities that happen from initiation of the transaction until the transaction is recorded and reported in the financial statements absent any controls. The term “controls” refers to activities that are put in place by management to mitigate risks that may affect the transaction. Processes and controls involve separate independent members of the organization (process owners and control owners) performing tasks to achieve the relevant objectives.

There are many ways an entity may obtain an understanding of the process, including interviewing people in the process, but generally a walkthrough is an essential element in confirming that understanding. That is because someone can describe how a process works, but following a transaction through the process validates what is being described. The rest of this section will focus on the use of a walkthrough to obtain sufficient understanding of a business process and will use the terms “walkthrough” and “obtaining an understanding” interchangeably given the importance of walkthroughs to achieving appropriate process understanding.

Use of Walkthrough

In a walkthrough, a single transaction is followed from origination through the entity’s processes, including 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 affecting 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. It also is important to walk through the process, not the individual controls within the process. A walkthrough is about understanding the process, which is not the same as, but will lead to, identifying WCGWs and controls to mitigate those WCGWs. Concentrating the walkthrough procedures on the previously identified controls creates the risk that additional WCGWs existing between the identified points of control are missed, and that relevant controls to mitigate those WCGWs are not identified for evaluation of their design and effectiveness.

Illustration 5.1:
Pitfalls of walking through controls instead of through the process

Scenario:
Management requests process owners to describe in a narrative how each control operates, and provide example documentation.

What was missed:
This is not a sufficient procedure to obtain or validate management’s understanding of the entity’s business processes. Walkthrough procedures should focus on more than just the controls. They should follow transactions through the entire process, from the initiation of the transaction to the recording of the transaction in the general ledger.

The purpose of the walkthrough is to gain an understanding of the process that will enable management and external auditors to identify relevant financial reporting risks and related controls. When walking through the controls instead of the process, there is a risk of not identifying sources of misstatement (i.e., WCGWs) for which controls are needed.

Illustration for the audit:
Pitfalls of walking through controls instead of through the process

Scenario:
Management performs an annual update of their business process narratives and then we select a completed transaction for a walkthrough of each process. In the conduct of the walkthrough, we obtain evidence that the selected transaction was subjected to the relevant controls management identified.

What was missed:
This is not an appropriate approach to obtaining an understanding of a process and identifying relevant controls within the process. The scenario described above represents one of the most common shortcomings in auditing ICOFR. As stated in the previous Illustration, the purpose of a walkthrough is to first identify the WCGWs so that the proper controls can be identified for testing. Ineffective walkthroughs may lead to ineffective ICOFR testing.
Walkthroughs that combine inquiry, observation, and inspection of relevant documentation are ordinarily sufficient to evaluate the design and implementation of identified controls. Inquiry alone, however, is generally not sufficient.

At points within a process where important processing activities occur, the person performing the walkthrough places himself or herself 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. These probing questions, combined with the other walkthrough procedures:

- Allow management and external auditors to understand the process and identify important activities within the process, potential opportunities for misstatement, and points at which a necessary control is missing or designed ineffectively;
- Allow 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 the abuse of controls or indicators of fraud.

To corroborate information at various points in the walkthrough, the person executing the walkthrough might ask entity personnel some or all of the following:

- To describe their understanding of previous and successive steps in the process or control activities;
- To demonstrate how they perform the activity or control;
- To 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);
- To explain what they do when they find an error;
- To explain what kinds of errors they have found, what happened as a result of finding the errors, and how the errors were resolved;
- To describe whether they have ever been asked to override the activity or controls and, if so, to describe the situation; and
- To 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.
**Illustration 5.2:**
How detailed of an understanding should I obtain as part of my walkthrough?

**Scenario:**
Prior to performing a walkthrough related to the purchasing process, the internal audit manager considered how best to perform the walkthrough and what pertinent questions to ask of the process owners. She considered the risks inherent in the purchasing process and decided to choose a transaction that was already recorded in the general ledger. She followed that transaction through the process. She inspected documentation and inquired of various employees who participated in the processing of the transaction from the point at which a purchase request initiated the transaction, through the creation and approval of the purchase order, to the receipt of goods and recording of the vendor’s invoice in the entity’s general ledger. Relevant questions posed to the process owners included:

— Describe for me what happens next in the process?
— Where does the information come from? Does the information always come to you this way?
— Has anyone ever asked you not to do it this way?
— Are there differences in the way you process a purchase order depending on the item (e.g., for inventory as opposed to other items)?
— Who decides what general ledger accounts the transactions should be recorded to?
— Have you ever found an error, and if so, what did you do?

By asking these questions, she determined that there are different processes (and therefore likely different opportunities for misstatement) depending on what the entity is purchasing. She also determined that there are occasions when (for legitimate reasons) similar transactions go through different processes. She decided 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 WCGWs.

[5.1.130] To fully understand the flow of transactions, it is necessary to understand how data enters into an information technology (IT) system, 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 information 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. See guidance in section 5.3 for an additional discussion on IT-specific considerations in a walkthrough.
An entity's warranty reserve and its sales process are closely linked: information relevant to accounting for the warranty reserve is extracted from the same transactions that are part of the entity's sales process. Both processes rely on quantity of units sold. However, each also relies on distinct data from the sales process: accounting for the warranty reserve relies on the make and model of a part (e.g., a part number), while accounting for revenue relies on price per unit.

Because distinct relevant data elements exist within the warranty reserve and sales process, it is necessary to identify all relevant data elements and understand the flow of information related to each one of them. It may be helpful to start with amounts recorded in the general ledger or input to the warranty reserve model and follow the flow of information back to initiation of those relevant data elements.

Illustration 5.3:
Often, significant estimates are closely linked to significant classes of transactions...which cause us to think about whether all relevant data elements are identified in our walkthrough.

Scenario:
An entity's warranty reserve and its sales process are closely linked: information relevant to accounting for the warranty reserve is extracted from the same transactions that are part of the entity's sales process. Both processes rely on quantity of units sold. However, each also relies on distinct data from the sales process: accounting for the warranty reserve relies on the make and model of a part (e.g., a part number), while accounting for revenue relies on price per unit.

Action:
Because distinct relevant data elements exist within the warranty reserve and sales process, it is necessary to identify all relevant data elements and understand the flow of information related to each one of them.

It may be helpful to start with amounts recorded in the general ledger or input to the warranty reserve model and follow the flow of information back to initiation of those relevant data elements.

A walkthrough begins where the transaction begins. Even though the same transaction can be initiated in different ways, it might be possible to achieve the objectives of a walkthrough without selecting a separate transaction for each way a transaction can be initiated. When determining whether the objectives of a walkthrough may be achieved through selection of a single transaction (versus multiple transactions), consider whether any unique WCGWs related to authorization and safeguarding exist. Also consider the various data elements that may be used to determine the relevant assertions over the significant accounts associated with the business process subjected to 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.
Illustration 5.4:
Deciding where to begin our understanding of the process

**Scenario 1:**
A retailer sells a product on its Web site and also through several retail locations. It is unclear whether both types of transactions go through the same process or whether different WCGWs might need to be addressed. In this case, it may be appropriate to select both an Internet sales transaction and a retail store sales transaction, then trace each transaction until the two processes merge.

**Scenario 2:**
A commercial bank offers a customer multiple options for initiating a transaction such as a customer deposit (CD) account. A CD can be opened through the Web site, a branch location, or the U.S. 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 WCGWs related to the different ways a CD may be opened, following a single transaction might achieve the objective of a walkthrough related to the CD/account origination process.

[5.1.160] It is necessary to perform procedures to update and corroborate the process understanding each year, even if such understanding was obtained in prior years. The dynamic nature of both the internal and external environment in which entities operate may impact and alter the flow of transactions and the nature and significance of risks which may need to be addressed through control activities.

Illustration 5.5:
How much can we rely on our prior year knowledge?
After all, we’ve been performing ICOFR assessments for a long time...

**Leading Practice:**
A manufacturing entity determines that it will classify each process (e.g., sales order process, treasury process, etc.) into categories based on the types of transactions performed, the degree of change from 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, management decides to perform a walkthrough each year to update their understanding of the processes, determine the WCGWs, 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 WCGWs. If they determine that there are no such changes, a walkthrough is performed every two years instead of every year. Note, however, that while such an approach may be appropriate for management’s assessment of ICOFR, an external auditor is likely to perform a walkthrough every year.
Why this is important:
Many material weaknesses in ICOFR originate from an inadequate risk assessment process. Processes change over time due to a variety of factors (including personnel changes, changes in the way transactions are effected, changes in technology, etc.). As these changes occur, new risks (WCGWs) may arise. If these new risks 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 in the aggregate render the existing suite of controls inadequate and lead to a material weakness in the entity’s ICOFR.
Illustration for the audit:
How much can we rely on our prior year knowledge?
After all, we have been the auditors for the last 10 years and not much has changed…

Scenario:
We are confident that, because we audited the entity last year, we know which controls to test. We ask management if anything has changed with respect to its ICOFR. Management indicates that nothing has changed within the entity. We obtain management’s list of “key” controls, compare them to the controls tested in the prior year, and test the identified controls in the same manner we tested them in prior audits.

What was missed:
In this instance, we did not obtain sufficient audit evidence in the current year to meet the first objective of paragraph 34 of PCAOB AS No. 5. We inappropriately relied on management’s assertion that nothing has changed and, as a result, we failed to identify changes to the process and related risks that could require different or additional controls, or more robust testing of existing controls. In general, professional standards require that we, as auditors, obtain persuasive evidence to support our audit conclusions. Relying on a statement by management does not constitute obtaining persuasive audit evidence.

[5.1.170] 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, including how these transactions are initiated, authorized, processed, and recorded. This 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. One business process may include several significant accounts and disclosures. For example, a revenue process for a commercial enterprise will likely also cover such accounts as deferred revenue, accounts receivable, and sales returns.

[5.1.180] The responsibility for obtaining an appropriate understanding of each relevant business process, the flow of information, and the risks (WCGWs) within the process starts with management of the entity. That responsibility cannot be delegated to external auditors. In fact, it may be impossible for 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 are missing or deficient. The Securities and Exchange Commission (SEC) Staff has stated that management should identify those risks of misstatement that could, individually or in combination with others, result in a material misstatement of the financial statements. Management should use its knowledge and understanding of the business, and its organization, operations and processes, to consider the sources and potential likelihood of misstatements in financial reporting elements. Otherwise, a deficiency exists in the Risk Assessment component of management’s ICOFR.

Illustration for the audit:
How we might alter our walkthrough procedures to obtain sufficient audit evidence

**Scenario 1:**
If the underlying accounting requirements or judgments involved are complex and we assess inherent risk as high, we may:

- Have an experienced member of the engagement team perform the walkthrough;
- Use an IRM professional or another KPMG specialist;
- Include techniques such as reperformance or other corroborative procedures, and ask more probing questions.

**Scenario 2:**
When the process is routine and inherent risk is low, we may:

- Have junior members of the team perform the walkthrough;
- Consider using more inquiry and observation (and less reperformance and corroborative inquiry) because we do not need the same persuasiveness of audit evidence.

We should still consider involving IRM if the process is very dependent on technology. This could be particularly relevant when the entity has a highly automated or centralized processing center that handles voluminous transactions (e.g., payables processing and cash disbursements for a large multinational manufacturer, or online sales of an Internet retailer). It is important to work collaboratively with IRM to determine the appropriate level of audit evidence needed for this largely routine process.

---

[5.1.190] An understanding of business processes and the flow of transactions related to significant accounts and disclosures is obtained **early in the ICOFR assessment process.** New information may come to light as the ICOFR assessment process progresses throughout the reporting period. If new relevant information is identified, it may be necessary to revisit the preliminary determination of relevant assertions over significant accounts or disclosures. If it is determined that there are additional relevant assertions, it is then necessary to obtain an understanding of the related financial reporting risks and whether there are controls in place to address those risks.

[5.1.200] Similarly, in the course of the ICOFR assessment, previously unidentified risks within a business process may come to light. This may require management to supplement their understanding of the process and design additional controls to address the newly identified risks. External auditors would then test those controls as part of their ICOFR assessment. Business processes and the transaction flow also are susceptible to change during the year and in some cases after the initial understanding of these processes and transactions had been obtained by management and external auditors. For example, the entity may undergo restructuring, turnover in personnel, and reassignment of certain control responsibilities, or other major changes. In such situations, it is necessary to update the understanding of relevant business processes and any risks and controls that might have been impacted by the changes.
Illustration 5.6:
Additional information or new facts discovered during the SOX assessment may lead to additional control work!

<table>
<thead>
<tr>
<th>Scenario:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management originally determined that valuation was not a relevant assertion related to the Accrued Liability account. However, during the annual risk assessment procedures, a change in the entity’s business practices was identified — management commenced issuance of share-based payments to non-employees with the resulting liability balance recorded in the Accrued Liability account.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action:</th>
</tr>
</thead>
<tbody>
<tr>
<td>These awards present a new risk of material misstatement. It is necessary to understand how these awards are initiated, authorized, processed and recorded to be able to identify financial reporting risks and related controls. Because awards issued to non-employees may result in different accounting than those issued to employees, it is likely that previously existing controls related to share-based payments are insufficient to address the newly created risks of material misstatement.</td>
</tr>
</tbody>
</table>

Multiple Physical Sites

| [5.1.210] An entity may have multiple physical sites (e.g., warehouses, not to be confused with separate subsidiaries). These sites may be homogenous, or centrally controlled, or not fall into either one of these two categories. |

| [5.1.220] Homogenous locations are multiple physical sites which have common process activities, systems, risks (WCGWs), and process level controls and are subject to the same entity-level controls. Careful consideration should be given in determining whether locations are homogenous. |

<table>
<thead>
<tr>
<th>[5.1.230] If multiple physical sites are concluded to be homogeneous, it may be possible to conclude that walkthroughs at each location are unnecessary after considering the following factors:</th>
</tr>
</thead>
<tbody>
<tr>
<td>— The effectiveness of the entity’s risk assessment and monitoring processes;</td>
</tr>
<tr>
<td>— The effectiveness of entity-level controls developed by management in response to its risk assessment;</td>
</tr>
<tr>
<td>— The assessment of risk of failure of controls in the process;</td>
</tr>
<tr>
<td>— The results of management’s or internal audit’s procedures relevant to the homogenous locations; and</td>
</tr>
<tr>
<td>— The knowledge obtained in the previous year’s audit, including the nature and extent of any misstatements and deficiencies within ICOFR.</td>
</tr>
</tbody>
</table>

| [5.1.240] In most instances, it may be necessary to perform a walkthrough or other procedures at multiple locations to support the assertion that the locations are in fact homogeneous. The determination of homogeneity and the number of locations to be visited as well as the ability to conclude on a population by testing a subset of items or, in this case, performing a walkthrough at fewer than all locations are a matter of professional judgment and require a careful consideration of the relevant facts and circumstances. |
Multiple physical sites are **centrally controlled** if transactions for these sites are processed centrally based on information provided by each site.

If multiple physical sites are determined to be centrally controlled, it may be most effective to perform a walkthrough at the central location and determine whether the controls identified at that location sufficiently address relevant risks at the individual physical sites.

In the case of **multiple physical sites that are neither homogenous 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.

At various points during the ICOFR assessment, evidence may arise that suggests that the sites that were originally determined to be homogeneous may not actually be homogeneous. Such evidence may include:

- Differences in the design of controls at locations selected for testing;
- Deficiencies in the operating effectiveness at only one or some of the locations selected for testing; or
- Indications from other sources (for example, Internal Audit site visits that were not ICOFR related) that the design or operating effectiveness of controls may be different or ineffective at locations not selected for testing.

When this contrary evidence arises, both management and external auditors consider whether more evidence is needed to affirm or disaffirm the original conclusion that the locations are homogeneous. Once sufficient evidence has been obtained, if the locations are ultimately concluded to be not homogeneous, the assessment of controls at the individual locations may need to be reScoped in order to obtain sufficient evidence that the controls are in fact operating effectively at the various locations. Alternatively, to the extent possible, management and external auditors may identify and evaluate appropriately designed entity level controls that operate with a level of precision that would prevent or detect, on a timely basis, a material misstatement of the entity’s financial statements that could arise out of the locations that were previously designated as homogeneous. See chapter 10 of the ICOFR Reference Guide – Monitoring for additional guidance regarding entity level controls that are designed to monitor controls at multiple physical sites of an entity.

Considering contrary evidence requires judgment and an understanding of the root cause of the identified problem. The following are guidelines to consider when evaluating contrary evidence about the homogeneity conclusion:

- The presence of significant differences in the design of controls at multiple sites is a strong indicator that the sites are not homogeneous.
- Minor deficiencies (both in number and in impact to ICOFR) at a small number of locations do not necessarily mean that the locations are not homogeneous.
- If there is a particular reason that the deficiencies occurred at one or more locations (e.g., there was significant turnover of management, or the geographic location suggests an additional risk not previously considered), then one might conclude that all sites with that particular risk trait (new management or a similar geographic situation) may need to be excluded from the homogeneous population and considered for extent of testing separately.
— Even if there is a particular reason that the deficiencies occurred at one or more (or even all) locations but the severity of the deficiency would not be material, further evidence may not be needed to conclude on internal controls over the relevant assertions impacted by the deficient locations. However, careful consideration is required when assessing the severity of the identified deficiencies in such situations.

— If there is no identifiable reason for the variation but rather the nature of the control is such that it is not expected to operate effectively 100% of the time (e.g., a manual recurring control such as a daily inventory cycle count that is largely effective but on one day experienced a minor discrepancy in the execution of an individual inventory count), then — absent other contrary evidence — an entity may still be able to conclude that the sites are homogeneous. In such situation, the identified control deficiency would simply be evaluated for severity but would not automatically call into question whether the sites are homogeneous. Furthermore, if the control is a manual control and the observed rate of deviation in the operation of the control does not exceed the tolerable rate of deviation established for the control, it may even be possible to consider the control to be operating effectively.

[5.1.310] Note that the scenario in the last bullet point of the preceding paragraph is similar to one in which there is only one location with multiple control operators, one of whom makes a small inadvertent error in one instance of a control’s operation (e.g., one inventory warehouse that is subject to cycle counting by several independent counters who are largely effective but, on one day, one of them makes a small unintentional error in the count of an inventory item). Such an error is a deficiency that needs to be evaluated for severity but, given the facts, it is not likely that a prudent official would conclude that there is a material weakness, even absent mitigating controls. Similarly, minor deficiencies identified at locations that were determined to be homogeneous do not automatically mean that the locations should no longer be considered homogeneous. Careful consideration of the above bullet points may or may not support the determination that the multiple sites are homogeneous.
Illustration 5.7:
Contrary evidence about homogeneous locations

An entity has 40 warehouses spread across multiple countries, but they all perform similar activities with respect to receiving, managing, and shipping inventory. Management believes that all of the warehouses are homogeneous because each warehouse is directed to have the same internal controls over inventory and shipping. Management and the external auditors choose to perform walkthroughs and test controls at 15 locations, which covers approximately 40% of the inventory.

Contrary Evidence Scenario:
There were no issues with respect to the design of the controls, and the walkthroughs confirmed that each of the 15 locations has the same process, risks, and controls. However, when testing the operating effectiveness of the controls, it was discovered that there were deficiencies with respect to the shipping cut-off at two of the 15 locations. Further investigation showed that these were two relatively new warehouses and were located in Eastern Europe and Russia, where the entity had only recently began to do business.

Given the situation, management and the external auditors determined that these two locations likely were not homogeneous with the other locations. Further, they considered whether there were any locations in the remaining 25 untested locations that also shared the traits of being relatively new and located in an emerging geographic location. One other warehouse was identified and segregated out from the other population for separate evaluation.

Therefore, the entity has 37 homogeneous locations and 3 non-homogenous locations. Out of the 37 homogenous locations, walkthrough procedures and testing of controls was performed at 13 locations (15 locations originally selected less the two locations in Eastern Europe and Russia). The results of that testing will be evaluated in the context of all 37 locations believed to be homogenous, much like the results of a substantive test of a sample of A/R balances would be extrapolated to the entire balance of A/R for which the sample-based test has been performed. The three non-homogenous locations will require reevaluation to determine whether more evidence needs to be obtained about the design and operating effectiveness of the controls at those three locations (based on the qualitative and quantitative considerations discussed in chapter 4 of the ICOFR Reference Guide – Risk Assessment, regarding scoping).

Service Organizations
[5.1.320] More and more entities use and depend on services provided by third-party service organizations. 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.5 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 ICOFR cannot be limited in its scope to exclude processes and controls performed by service providers engaged by the entity.6

---

[5.1.330] If services obtained from a third-party organization are part of the entity’s information system, those services are part of the entity’s ICOFR. Management and external auditors should consider the risks associated with the transactions processed by the service organization and the controls performed by the service organization (and the entity itself) to manage those risks, and determine how these controls affect the entity’s ICOFR.

[5.1.340] The extent to which management and external auditors address each service organization in their assessment of the effectiveness of ICOFR (including obtaining an understanding of the business processes effected by the service organization and identification of relevant risks and controls) depends on a number of 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 processed 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 ensure that the objectives of effective ICOFR are met; and

— The extent to which the entity depends on the effective internal controls of the service organization.
Illustration 5.8:
Understanding the processes affected by service organizations

Scenario:
In an effort to reduce general and administrative expenses, management of a nursing home operator decided to outsource its entire back office (including accounting, payroll administration and processing, tax compliance, and other functions) to a service organization that provides these services using its own IT systems. The nursing home operator is one of the largest customers of the service organization. The controls in place at the service organization are assessed on a semiannual basis by a large accounting firm, as evidenced by a Service Organization Control (SOC) 1 – Type II report.

Actions:
Given the significant extent of the entity’s reliance on the service organization and the importance of the outsourced processes to the entity’s financial statements, the entity would likely include the service organization directly in its ICOFR assessment. It would not rely solely on the SOC 1 report. Instead, management would use the report to assess risks posed by the service organization and perform a preliminary assessment of the relevant controls described in the report. It would then plan and perform walkthroughs at the service organization to obtain an appropriate understanding of the significant business activities processed by the service organization and the risks of material misstatement of the entity’s financial statements within those processes.

Contrasting Scenario:
An online retailer outsourced its payroll processing to a large service organization that specializes in the field of payroll services. The organization serves large and small companies around the world and has reputation for quality, timeliness, and strong internal controls. The controls of the service organization are assessed on a semiannual basis by a large accounting firm, as evidenced by a SOC 1 – Type II report.

Actions:
Given the routine, nonjudgmental nature of the process outsourced to the service organization, the limited scope of the outsourcing arrangement, and the reputation of the service provider, both management and external auditors will likely be able to obtain sufficient evidence to achieve the objectives of the payroll process walkthrough from a combination of procedures performed at the entity level and a review of the SOC 1 report provided by the service organization. It would likely be unnecessary to perform a walkthrough of the payroll process at the service organization.
Key takeaways:

Understanding the Process

1. **Before identifying WCGWs and relevant controls, understand the business process and the flow of transactions.** Perform procedures to update and corroborate the understanding every year. Generally, those procedures include a walkthrough.

2. Obtain an understanding of the flow of transactions for **all relevant assertions of every significant account and disclosure.**

3. **When performing a walkthrough, remember to:**
   - **Include the entire process** from initiation of the transaction to recording amounts in the general ledger;
   - **Follow the flow of the transaction data,** not the related documents or controls, through the process;
   - Follow the transaction **through the IT system, not around it**;
   - Follow the transaction **through third-party service organizations**;
   - **Ask probing questions to** understand if the transactions always occur in the same manner to help identify WCGWs, relevant controls, and potential for (or actual instances of) management override.

4. **Document the process and the flow of transactions.** Documentation should be robust enough to show major activities in the process but concise enough to allow for an effective and efficient review. A combination of a flowchart and a brief narrative is likely the most effective manner to document an understanding of a process.
5.2 Identifying the What Could Go Wrongs (WCGWs)

[5.2.10] Part of the risk assessment process is to understand the financial reporting risks. Documenting the flow of information and the related controls alone is insufficient to demonstrate that management and external auditors understand the risks and have selected the appropriate controls.

[5.2.20] Therefore, after obtaining an understanding of the flow of transactions, management and external auditors identify the points within the entity’s processes at which a misstatement, including a misstatement due to fraud, could arise that, individually or in combination with other misstatements, would be material (i.e., the WCGWs). See chapter 4 of the ICOFR Reference Guide – Risk Assessment, for more discussion about fraud risks.

[5.2.30] A WCGW is not simply a risk that the data could be misstated. It also is not the absence of a control. Rather, a WCGW is any condition that could allow misstatements to enter the system or could allow the data to lose its integrity. There are likely to be multiple WCGWs in every business process.

[5.2.40] WCGWs also include a risk of unauthorized acquisition, use, or disposition of assets that could result in a material misstatement of the financial statements.

[5.2.50] There are many considerations in the identification of WCGWs. 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;
— Points in the process at which data is summarized, accumulated, subjected to calculations or otherwise manipulated;
— Manual processes that affect the data (e.g., manual journal entries);
— Management review processes over the data and how management ensures the data has and maintains its integrity;
— Judgments made by management in determining whether or not to adjust data, and 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).

[5.2.60] Relevant WCGWs should be documented in sufficient detail to allow a reviewer to understand 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 controls that are appropriately responsive to that particular risk. A properly defined risk also is critical to the effective evaluation of the controls by management and the external auditors. Failure to define risks with sufficient clarity often results in a control that is not appropriately designed to address the actual risk or a missing control.

[5.2.70] Each WCGW should link to a relevant financial statement assertion. Frequently, multiple WCGWs link to a relevant assertion. If a WCGW does not link to a relevant assertion, it is likely not a relevant WCGW for ICOFR.
Let us look at some common WCGWs from the purchase-to-pay process:

Example 1

Poorly Worded: Accounts Payable and accrual balances (A/P and Accruals) are incomplete.

How can this be improved? The WCGW is stated very generally and it may be difficult to identify a specific control (or controls) that will mitigate the risk. By including more detail in the description of the risk, management and external auditors will be in a better position to identify controls that will properly address timely accounting for invoices received after period-end, as well as accruals required for more technical accounting matters resulting from significant agreements. When WCGWs are described generically, there is a risk of missing relevant controls.

Better: Invoices received after period-end relate to the current period but are not accrued for. [CEA of A/P and Accruals.]


Example 2

Poorly Worded: Expenditures are overstated.

Better: Payment of duplicate vendor invoice numbers. [E of Expenses.]

Example 3

Poorly Worded: Accounts Payable is not accurately presented in the financial statements.

Better: Receivables and Accounts Payable are offset and inappropriately reported under a net presentation. [P of Receivables and Accounts Payable.]

Better: Accounts Payable debits inappropriately exist within the Accounts Payable subledger and are netted against the ultimate credit recorded on the financial statements. [P of Accounts Payable.]

Example 4

Poorly Worded: Selling, General, and Administrative expense are incomplete.

Better: Cash disbursements are coded to incorrect GL accounts. [CEA of SG&A Expenses; CEA of PP&E.]

Better: Vendor invoices are not submitted on a timely basis to Accounting by various Corporate head office departments. [C of SG&A Expenses and Accounts Payable.]
Illustration 5.10:
How a poorly worded WCGW might lead to ineffective design or assessment of controls

A heavily aggregated or overly general WCGW may lead management to design a control or external auditors to select a control for evaluation that appears to address the WCGW; however, in actuality, the control only addresses a portion (or none) of the potential for misstatement (i.e., the WCGW). For example:

**WCGW = The statement of cash flows is incorrect**
To address the WCGW, as documented, management and external auditors 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. It may need to include a review, at an appropriate level of precision, of key information about noncash transactions, foreign currency impacts, items that are required to be reported gross, and more. Without more detailed WCGWs related to the preparation and review of the statement of cash flows, we may not identify the right controls or, if management’s review is the only control, we may not be testing the design appropriately to determine whether the review addresses all relevant WCGWs.

[5.2.80] While the main objective of a walkthrough is to help management and external auditors understand the flow of transactions and to allow them to identify appropriate WCGWs, selection of controls over the WCGWs is closely related to the risk assessment process and often occurs concurrently with the identification of WCGWs. See chapters 6, 7, and 8 of the ICOFR Reference Guide for discussion on selecting and testing controls.
Key takeaways:

Identifying the What Could Go Wrongs (WCGWs)

1. **Look for the conditions that could lead to a misstatement.** A WCGW is not simply a risk that the data could be misstated. Rather, a WCGW represents a condition that could allow a misstatement to enter the system or could allow the data to lose its integrity.

2. **Look for WCGWs related to each meaningful activity within the IT system.** There may be a WCGW with respect to the completeness and accuracy of data whenever data is entered into an IT system, moves within the IT system, and exits the IT system (either to enter another IT system or in the form of information produced by the entity (IPE), such as a system-generated report). There also may be WCGWs with respect to the accuracy of calculations or other data manipulation performed by the IT system.

3. **Document the identified WCGWs.** Part of the risk assessment process is to understand the financial reporting risks. Documenting only the flow of information and the related controls is insufficient to demonstrate that management and external auditors understand the WCGWs and have selected the appropriate controls.

4. **Document relevant WCGWs in sufficient detail** to allow a reviewer to understand the specific condition that would allow for a material misstatement to occur within the financial statements. **Link each identified WCGW to a relevant financial statement assertion.**
5.3 IT Considerations When Understanding the Process Activities

IT-Related Risks

[5.3.10] When performing walkthroughs of business processes, consider risks arising from both manual and IT systems. The SEC Staff, the COSO Framework, and the PCAOB auditing standards all state clearly that identifying risks and controls related to IT is not a separate evaluation or audit step.7

[5.3.20] IT considerations in risk assessment 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.

Overall IT Environment

[5.3.30] The topic of understanding the overall IT environment is further discussed in chapter 8 of the ICOFR Reference Guide, General IT Controls. It is important to understand the overall IT environment in order 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 controls management has in place to address the risks, including completeness and accuracy of relevant data elements flowing through the process.

[5.3.40] An understanding of the workings of IT systems utilized by the entity, including how information flows into, through, and out of the relevant IT systems, may be facilitated by the use of IT System Diagrams (ISDs).

[5.3.50] 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. 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 also a framework by which management and external auditors can ensure they understand IT adequately when they walk through a business process to identify relevant WCGWs.

---

7 See SEC Release 33-8810, p. 19; COSO Framework, p. 98; and PCAOB Auditing Standard No. 5 par. 35.
Illustration 5.11: Example of an ISD that describes the sales and sales returns process of a retailer

HO/O2: IT System Overview Diagram for Sales and Sales Returns

[5.3.60] In the Illustration above, the ISD considers the application as well as the database that stores data and the underlying operating systems, including IT components. There may be additional components relevant to the ICOFR assessment, such as scripts, interfaces, and customized application programming interfaces. Each aspect of the ISD is important to an adequate understanding of the business processes that rely on IT, help management and external auditors identify relevant WCGWs, and inform their judgment when it comes to identifying the relevant general IT controls (GITCs) that support the automated controls which are relied upon in the ICOFR assessment to mitigate risks identified within each business process.

IT Risks at the Process Level

[5.3.70] 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 WCGWs in the process at the assertion level where there is a reasonable possibility that these WCGWs could result in or contribute to a material misstatement. This includes the WCGWs 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.

[5.3.80] Walkthroughs and other procedures can provide an understanding of how IT affects the entity’s flow of information and allow management and external auditors to consider IT risks (WCGW with the data as it flows through the IT system) when identifying likely sources of misstatement. There is a potential WCGW related to the completeness and accuracy of data whenever data enters the system, when it is stored and can be accessed in the system or database, when it moves from one system to another, and when the data is summarized, accumulated, or subjected to calculations.
When performing walkthroughs, it is not required 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. However, because there is often complexity involved with IT infrastructure, both management and 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.

Illustration for the audit:
Should IRM be invited to participate in the walkthrough? Probably, but it depends.

<table>
<thead>
<tr>
<th>Scenario 1 – IRM resources familiar with ERP:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assume an entity’s purchase-to-pay process relies on IT. The extent of IT reliance is high but the inherent risk of the accounts associated with the process and the relevant assertions are not significant. The IT application is a large, well-known Enterprise Resource Planning (ERP) system; the audit team and the IRM resources are familiar with the ERP system from prior audits.</td>
</tr>
<tr>
<td>We may choose not to invite IRM to participate in the purchase-to-pay process walkthrough this year but instead <strong>ask IRM to perform a desktop review</strong> of the preliminary process documentation and identification of WCGWs. This would increase the likelihood that we invite IRM to participate in the audit next year. After reviewing the narrative and/or flowchart, IRM provides a series of review comments for follow-up by those who performed the walkthrough.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scenario 2 – ERP has been upgraded in a specific area:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assume the same fact set as above with one change: the ERP system was upgraded to augment the process during the current year. The upgrade focused narrowly on reporting from the ERP system that helped end users review expenditures before authorizing disbursements.</td>
</tr>
<tr>
<td>We may invite IRM to participate in the <strong>whole</strong> walkthrough or in the <strong>portion</strong> of the walkthrough where information flows into the upgraded end-user reporting.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scenario 3 – ERP has been significantly upgraded:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assume the same fact set as above with this change: the ERP system was significantly upgraded during the current year to expand functionality and improve efficiency.</td>
</tr>
<tr>
<td>We may invite IRM to participate in the <strong>entire purchase-to-pay process walkthrough</strong> and request the IRM professionals to document portions of the process that rely heavily on IT. Further, the IRM manager may review purchase-to-pay process walkthrough documentation.</td>
</tr>
</tbody>
</table>
General IT Controls

[5.3.100] The effectiveness of GITCs may have a pervasive impact on automated controls and manual controls with automated components at the process and transaction level, at a higher level, and within entity-level controls. Because of this, it is important to consider GITCs when assessing IT risks.

[5.3.110] Since GITCs do not directly address the relevant financial statement assertions, there is no requirement to walk through processes that pertain to GITCs alone. However, it is necessary to obtain and document a sufficient understanding of the business process, relevant WCGWs within the process, and the related application controls to determine which GITCs to test. For purposes of the ICOFR assessment, GITCs are evaluated to the extent they support consistent effective operation of automated controls (or manual controls with an automated component) relied upon in financial reporting. Performing a walkthrough of relevant business processes helps management and external auditors achieve the necessary understanding and meet the objectives of paragraph 34 of PCAOB AS No. 5, as described earlier in this chapter. Furthermore, linking relevant automated controls and manual controls with an automated component to the supporting GITCs helps management demonstrate the entity’s compliance with Principle 11 of the COSO Framework, which requires that management understand and determine the dependency and linkage between business processes, automated control activities, and technology general controls (GITCs). For further discussion on GITCs, see chapter 8 of the ICOFR Reference Guide – General IT Controls.

Scenario 4 – Entity relies on Excel spreadsheets:
Assume an entity relies on a series of Excel spreadsheets that transcribe information obtained from various IT systems as part of determining whether long-lived assets are impaired. The inherent risk related to valuing long-lived assets is significant and there are numerous asset groupings.

— **We may invite IRM to participate** in the walkthrough of the entire impairment review process. Alternatively, we may invite IRM to participate in the **portion** of the walkthrough where valuation of long-lived assets is addressed. IRM can help identify WCGWs related to the transfer of information from the IT systems to the spreadsheets and end-user computing, and evaluate whether the identified controls are sufficient to address the end-user computing WCGWs.
Key takeaways:

IT Considerations When Understanding the Process Activities

1. **Consider IT risks and manual risks to be part of a single process.** Remember that identifying risks and controls within IT is not a separate evaluation.

2. **Consider using an IT System Diagram.** An ISD may help you understand the various layers of IT embedded in a process to identify all relevant WCGWs.

3. **Consider whether it is necessary to involve someone with specialized IT skills to understand a business process and assess risks.** IT specialists may help you better understand IT within the process, including WCGWs and controls within the IT systems.
5.4 Documentation Considerations

[5.4.10] Documentation includes describing the flow of information through the process. The form and extent of the documentation developed either during or after walkthrough procedures will vary depending on the nature and complexity of the process. Documentation may take the form of a narrative or a flowchart, or a combination of the two.

[5.4.20] Generally, flowcharting is the most effective manner to document understanding of business processes, the flow of transactions, and the relevant risks. Flowchart diagrams, or flowcharts supplemented by a brief narrative, can substantially reduce or even eliminate the need for long, detailed process descriptions. They can also enhance management’s and external auditors’ understanding of the entity’s processes, IT systems, and controls and help the entity comply with the objectives of Principles 7 and 10 of the COSO Framework.

[5.4.30] A flowchart graphically depicts steps or activities that constitute a wide-ranging process, including key inputs, processes, and outputs. The purpose of a flowchart is to help identify the WCGWs and the controls in place to address them. It does not need to be overly complex; professional judgment is required to determine how much detail is necessary. For more information and guidance, refer to the Better Understanding the Process through Flowcharting – an Implementation Guide publication included at Appendix 5.1.

[5.4.40] A flowchart documents the flow of information through an entity’s process and also serves as a tool that helps management and external auditors execute the following steps in the ICOFR assessment process:

— Identify portions of the entity’s processes that have not been adequately understood as part of the walkthroughs (i.e., gaps in the understanding of the flow of information through the entity’s process);

— Identify all relevant WCGWs associated with a particular process;

— Identify all relevant controls associated with a particular process;

— Identify WCGWs where controls have not been identified or selected to address the WCGW; and

— Identify relevant IT systems through use of the flowchart or an ISD and understand the flow of information through IT.

[5.4.50] Walkthrough documentation includes at a minimum:

— Dates the walkthrough occurred;

— Interviewers;

— Interviewees;

— Transactions traced, including identifying characteristics of the transactions;

— Documents reviewed, including identifying characteristics of the documents; and

— Probing follow-up questions asked by the interviewers of the interviewees, and any notable responses.
Appendix 5.1: Better Understanding the Process through Flowcharting – An Implementation Guide
Chapter 6
Control activities
The SEC Staff is of the view that after management identifies the relevant financial reporting risks, it should then evaluate whether it has controls to “adequately address the entity’s financial reporting risks.”

The COSO Framework articulates a similar concept in Principle 10: The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives.

This chapter primarily focuses on the design and implementation of control activities that directly address financial reporting risks. Chapters 7 and 8 of the ICOFR Reference Guide also address parts of the control activities component. Chapter 7 speaks to Management Review Controls, a particularly challenging type of control activity. Chapter 8 discusses general IT controls, which are also discussed general IT controls, which are also challenging control activities that deserve special attention. Additionally, Chapter 10 of the ICOFR Reference Guide provides considerations for management when monitoring whether the controls are functioning.

Control activities operate in an integrated manner with the other COSO components; for instance, an effective risk assessment is needed to properly design and implement control activities, monitoring is necessary to determine that the controls are operating as intended, appropriate levels of information and communication provide control operators with the information they need to operate controls properly, and a robust control environment lays the foundation for an effective system of internal controls.

2  Internal Control – Integrated Framework published by COSO on May 14, 2013, p.88
6.1 Principles of Effective Control Activities

[6.1.10] After identifying the relevant reporting risks, “management should evaluate whether it has controls placed in operation (that is, in use) that adequately address the entity’s financial reporting risks. The determination of whether an individual control, or combination of controls, adequately addresses a financial reporting risk involves judgments about whether the controls, if operating properly, can effectively prevent or detect misstatements that could result in material misstatements in the financial statements.”

[6.1.20] This directive is consistent with the COSO Framework, which establishes three principles necessary for effective control activities within ICOFR:

<table>
<thead>
<tr>
<th>Principles of the Control Activities Component</th>
<th>Principle 10: The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 11:</td>
<td>The organization selects and develops general control activities over technology to support the achievement of objectives.</td>
</tr>
<tr>
<td>Principle 12:</td>
<td>The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.</td>
</tr>
</tbody>
</table>

[6.1.30] This chapter primarily focuses on Principles 10 and 12, while chapter 8 of the ICOFR Reference Guide discusses the general IT controls described in Principle 11.

---


4 Internal Control – Integrated Framework published by COSO on May 14, 2013, p.87
6.2 Selecting, Developing, and Deploying – Control Activities

**Identifying Controls**

[6.2.10] The controls we are interested in identifying are the manual or automated procedures the entity uses to prevent, or detect and correct, errors or fraud that could directly result in material misstatements of the financial statements. These controls may include higher-level or process-level controls. Examples of manual and automated controls include:

- **Manual controls**: authorization, management review, reconciliation, safeguarding and segregation of duties.
- **Automated controls**: system configuration/account mapping, exception/edit report, interface, authorization, segregation of duties and system access.

[6.2.20] Control activities may be preventive or detective, and organizations usually employ a mix of the two. The major difference between the two types of controls is the relative occurrence of the control activity. A preventive control is designed to avoid an unintended event or result at the time of initial occurrence (e.g., upon initially recording a financial transaction or upon initiating a manufacturing process). A detective control is designed to discover an unintended event or result after the initial processing has occurred but before the ultimate objective has concluded (e.g., issuing financial reports or completing a manufacturing process).

**Distinguishing the control from the process**

[6.2.30] Controls, to be effective, must always be independent of the process. Management and external auditors may sometimes fall into the trap of blurring the distinction between a process and the controls designed to prevent or detect unauthorized transactions or errors, particularly in areas of significant judgment. This distinction is important because management is required to establish and evaluate the controls over financial reporting, not just understanding the process.

[6.2.40] A process is defined by Merriam-Webster’s Dictionary as a series of actions that produce something or that lead to a particular result. Processes and the related actions are separate from the controls. Actions within the financial reporting processes may introduce intentional or unintentional errors into the financial statements.

[6.2.50] A control is designed to prevent or detect the potential errors in the financial reporting process, but does not itself introduce errors into the financial statements. Because of this, Principle 5 of the Risk Assessment component of internal control requires an understanding of the process and identification of “what could go wrongs” (or WCGWs) prior to selecting the controls.

[6.2.60] Particularly when dealing with Management Review Controls over complex estimates or transactions, the lines between the process and the control can be blurred. Even when the control operates continuously (as opposed to occurring at a distinct point in time), it is important to distinguish between the process (e.g., who determines the proposed reserve amount) and the control (e.g., who reviews and approves the proposed reserve amount). Management and auditors are required by SOX to test the controls, not the process, when evaluating control activities.

---

5 Internal Control – Integrated Framework published by COSO on May 14, 2013 refers to process-level controls as “transaction controls.”

6 The descriptions in paragraphs 6.2.10 through 6.2.20 are consistent with those described in footnote 27 of the 17 CFR Part 241 (Release 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. The Internal Control – Integrated Framework published by COSO on May 14, 2013 also provides similar examples of types of process control activities. Those examples include: authorizations and approvals, verifications, physical controls, controls over standing data, reconciliations, and supervisory controls.
To help determine whether the process has been separated from the control, evaluate whether the control operator is a different individual and independent from the process owner.

When processes and controls are not sufficiently distinct, management and external auditors will find it difficult to evaluate whether a control is designed and/or operating effectively.

An effective risk assessment, including understanding the flow of a transaction from initiation to recording in the financial statements, is important to properly distinguish between the process activities and the controls. See chapter 5 of the ICOFR Reference Guide – Risk Assessment for further discussion.

Illustration 6.1:
Distinguishing between a process and a control

Example of a process:
On a quarterly basis, the Tax Director and his team prepare a tax package to support the uncertain tax positions. The tax package includes a memo on new tax positions and tax positions that may need to be reevaluated based on activity that occurred during the period (e.g. tax return filings, tax audits, settlements, etc.). The memo is further supported with summary and detailed roll-forwards of the uncertain tax positions, along with detailed calculations of the liability, interest and penalties, and supporting documents such as legal/tax opinions, tax returns, and relevant court rulings, where appropriate.

Example of a control:
On a quarterly basis, the Tax Vice President reviews the uncertain tax positions liability for existence, completeness, accuracy, and valuation. As part of the management review control, he reviews the tax package prepared by the Tax Director and his team.

Controls are identified to address WCGWS

Entities may have one control that addresses one WCGW, a suite of controls that address one WCGW, or one control that addresses multiple WCGWs within a process.

Generally, management has a greater need for precision and redundancy (i.e., more controls that meet the same objective) than do external auditors. External auditors are focused on materiality, while management is focused on accurate books and records requiring a higher degree of accuracy. Because of this, management may have financial reporting controls that external auditors will not test.
A retailer’s sales process begins with data being entered into the point-of-sale (POS) system at retail stores. Sales data accumulates within the POS system and is eventually transferred electronically and maintained at the corporate level (corporate database).

Management identifies WCGWs within the sales process related to the data as it enters and is accumulated within the POS system.

Management also identifies a WCGW related to the interface between POS and corporate database.

The retailer has application controls to address these WCGWs.

However, the retailer has a control whereby the information that is electronically transferred to corporate database from the POS system is reconciled to bank statements showing daily cash deposits by store. If designed appropriately, this reconciliation control may sufficiently address all of the relevant WCGWs identified within the sales process. In other words, the WCGWs related to the POS system all relate to the completeness and accuracy of the sales data making its way into corporate database and ultimately the financial statements. The reconciliation control provides evidence (i.e., existence, completeness and accuracy) that the sales data was properly captured within POS and that it was transferred to corporate database.

A POS system could process other data, such as capturing the relief of inventory and recognizing the cost of sale when a sales transaction occurs. The scope of this example control has been limited to address the impact on the sales process (i.e., it does not address how controls related to POS system might impact other processes such as inventory or cost of sales).

Illustration 6.2: When can a “downstream” control address multiple WCGWs?

[6.2.120] Use caution when selecting controls that purport to address multiple WCGWs, to avoid inadvertent reliance on untested controls.
Illustration 6.3:
Consider whether WCGWs within other processes impact the selection of controls

In the example above, selecting the reconciliation control may be appropriate related to the sales process. However, the retailer may use the data from the POS system in an impairment analysis because it needs a breakdown of sales by SKU, information found within POS but not within the corporate database. In this case, the reconciliation control is unlikely to provide sufficient evidence about the completeness and accuracy of the SKU data. The reconciliation control only provides evidence about the sales data in total.

Also the reconciliation control, generally, does not provide evidence about controls over financial statement account assertions concerning cost of goods sold.

Design and Implementation of Controls

When selecting controls, consideration should be given to whether they are appropriately designed and implemented to mitigate the identified financial reporting risks.

Evaluating the design of a control involves considering whether the control, individually or in combination with other controls, can effectively prevent, or detect and correct, material misstatements. It is often helpful to refer to the definition of a material weakness. PCAOB Auditing Standard (AS) No. 5 defines a material weakness as 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 the entity’s annual or interim financial statements will not be prevented or detected on a timely basis.

Evaluating the implementation of the control involves confirming that it exists and that the entity is using it. The design and implementation evaluation are generally performed together, often as part of a process walkthrough. While there is no requirement for management to perform a walkthrough, doing so is often the best way to obtain the appropriate understanding of processes and identify the WCGWs. Generally, the determination of the design and implementation is performed before the testing of operating effectiveness—there is no point testing a poorly designed or implemented control.

The main consideration when assessing the design of a control is its precision. Consider whether the control is designed to operate at a “would” level—meaning that the control, if operating effectively, would prevent, or detect and correct, a material misstatement. A “would” threshold means that there is only a remote chance that the control or controls would not prevent, or detect and correct, a management review control (MRC) material misstatement. Understanding the appropriateness of the precision threshold may be difficult when evaluating the design of a MRC. Determining the precision of controls at the assertion level, including MRCs, for each assertion they are intended to address, is key to their efficacy. See chapter 7 of the ICOFR Guide – Management Review Controls for more discussion on MRCs.

Precision for each control may be very different. Precision does not equal materiality; rather, the precision at which each control operates should be considered in the context of whether all controls, operating as a system, would prevent or detect a material misstatement individually or in the aggregate. Precision is also the expectation relative to the design of the control given the risk it is intended to address.
Illustration 6.4:
Consider precision when selecting controls to test as part of the audit

Example:
An entity’s materiality for the current year is assessed as $2 million. In response to a WCGW, the entity has a control in which the purchasing manager reviews and approves all purchases over $1 million to ascertain existence and accuracy of payable and related asset or expense accounts and safeguard the entity’s assets. As part of design assessment, management notes a significant volume of purchases, the vast majority of which are below $1 million.

In this case, the control may not be sufficiently precise to detect a material misstatement because there is a more than remote chance that a material misstatement exists, in the aggregate, in the population of purchases not reviewed.

Contrasting Example:
The entity begins using an automated check to compare prices on all purchase orders to the price master file. This check produces a report of every extended variance over $50. A purchasing supervisor reviews this variance report and investigates all differences noted.

In this case, the control would likely be precise enough to address relevant assertions for all transactions.

[6.2.180] Along with the overriding concern which is whether the control is designed to operate at a “would” level, other considerations come into play when selecting controls to test including:

— Is the control likely to be effective?
— Is the person monitoring (management, internal audit and/or external audit) likely to be able to obtain sufficient evidence to conclude on the operating effectiveness?

Considerations Related to Fraud

[6.2.190] As discussed in chapter 5, we should consider the risk of fraud when assessing WCGWs. Specifically:

— Assessing incentives and pressures that may exist at the entity;
— Assessing opportunities for unauthorized acquisition, use, or disposal of assets, altering of entity’s reporting records, or committing other inappropriate acts;
— Assessing attitudes and rationalization (i.e., consider inappropriate acts might occur or be justified); and
— Determining how incentives and pressures, opportunities, and attitudes and rationalization (including bias) create opportunities for fraud.

[6.2.200] Based on the WCGW assessment, management and the external auditor alike, would identify controls that are designed and operate with expectation of mitigating fraud risks.
[6.2.210] Consideration also should be given to the need for controls over:

— Journal entries and adjustments made in the period-end reporting process;
— Significant unusual transactions;
— Related party transactions; and
— Significant management estimates (management bias)—see chapter 7 of the ICOFR Reference Guide – Management Review Controls.

[6.2.220] Controls that are designed to detect, prevent or deter fraud often need a different level of testing than other controls. Management and external auditors should consider the nature, timing and extent of evidence obtained to support the design and operating effectiveness of anti-fraud controls.

Illustration 6.5:
Consider precision of controls designed specifically to prevent or detect fraud

**Example:**
An entity’s materiality for the current year is assessed as $30 million. However, the entity considers that there is a risk of fraud related to management creating fictitious sales. Management has incentive to create the fictitious sales because a significant portion of its bonuses depend on whether they meet certain revenue targets.

Controls have been designed and implemented to mitigate this risk including segregation of duties such that no member of management can post journal entries, create a sales order or generate an invoice. In addition, all journal entries related to revenue are reviewed specifically by someone whose bonus does not depend on the achievement of those revenue targets.

When considering precision, all of the segregation of duties controls have a zero tolerance—that is, the control is tested to confirm that each member of management whose bonus depends on the achievement of the revenue targets does not have conflicting duties and any deviation is not tolerated. Further, when determining the precision for the journal entry review control, even though management has determined that an error of $30 million may not be material, it would consider a misstatement caused by a fictitious journal entry to revenue of a much lower amount to be material. Therefore, while there is a second review of all journal entries with a dollar amount of $5 million or more, the second review of revenue journal entries has a precision of $50 thousand.
Considering Segregation of Duties as Part of the Design of the Control

[6.2.230] Consideration is given to segregation of duties when assessing the design and operating effectiveness of controls. The COSO Framework states, “When selecting and developing control activities management should consider whether duties are divided or segregated among different people to reduce the risk of error or inappropriate or fraudulent actions.”

[6.2.240] Segregation of duties reduces the opportunities for one person to be in a position to both perpetrate and conceal errors or fraud in the normal course of their duties. Segregation of duties is achieved by assigning different people to authorize transactions, record transactions and maintain custody of assets, and/or perform the related controls.

[6.2.250] Segregation of duties can address important risks relating to management override and safeguarding of assets. Management override circumvents existing controls and is a common way of committing fraud. The segregation of duties is fundamental to mitigating fraud risks because it reduces (but can’t absolutely prevent) the possibility of one person acting alone.

Controls Needed for the Proper Functioning of Selected Controls

[6.2.260] Often “selected” controls rely on the effective design and operation of “other” controls. For example:

— Certain controls, including management review controls, may use information produced by the entity (IPE). The controls that are in place to determine the completeness and accuracy of that information are therefore important to the effective operation of the management review control.

— General IT controls are necessary for application controls to function as designed.

[6.2.270] The “other” control’s design (and operating effectiveness) should be tested to conclude on the design (and operating effectiveness) of the “selected” control. For more information about controls over IPE and general IT controls, see chapters 7 and 8 of the ICOFR Reference Guide respectively.

Illustration 6.6: Completeness and Accuracy of Information Used in the Operation of a Control

The accounting manager reviews the legal contingency liability for existence, completeness, accuracy, and valuation. As part of that review, the manager obtains an internal summary of all open legal matters and discusses them with legal counsel. The effective design and operation of this control depends, in part, on the complete and accurate population of all open legal matters. Controls over the completeness of the population are important to the design and operation of the accounting manager’s review control. Such a control might be a reconciliation by the legal department of the internal summary of all open legal matters provided to the accounting manager, to letters returned from outside legal counsel listing open legal matters. The entity sends letters to their outside legal counsel requesting a list of open legal matters quarterly.

---

7 Internal Control – Integrated Framework published by COSO on May 14, 2013, p. 95
Controls over Safeguarding of Assets

[6.2.280] As discussed in chapter 5, the objective of ICOFR as established by the SEC includes controls over the safeguarding of assets—that is, controls management has implemented to prevent or detect the unauthorized acquisition, use, or disposition of assets that could result in a material misstatement to the financial statements. Safeguarding controls do not refer to the physical protection of assets or controls over making bad business decisions.

[6.2.290] Where a WCGW exists related to unauthorized acquisition, use or disposition of the entity’s assets that could result in a material misstatement in the financial statements, controls should be identified and tested to provide reasonable assurance against such WCGWs. These controls are commonly referred to as “safeguarding controls.”

[6.2.300] When implementing controls to prevent unauthorized acquisition, use or disposition of assets, segregation of duties is often an important safeguarding control. Other common safeguarding controls may include:

- Periodically comparing the results of cash, security and inventory counts with accounting records;
- Requiring appropriate management approval before an employee enters into a contract that binds the entity to certain obligations; and
- Requiring appropriate authorization for access to computer programs and data files.

Illustration 6.7:
Only certain types of safeguarding controls are relevant to ICOFR

The entity may identify WCGWs related to the unauthorized disposition (theft) of inventory. As a result, the entity has security measures to prevent theft, such as locks on the warehouse and cameras to monitor the inventory. This may be advisable, but these types of security controls are generally outside the scope of ICOFR. From an ICOFR perspective, the relevant safeguarding controls related to the risk of theft include timely inventory counts and reconciling the reported inventory balance to the physical inventory counts. Relevant safeguarding controls also may include a control to determine that material losses are appropriately disclosed in the financial statements, where required, even if the losses are appropriately recorded in the financial statements.
Significant Unusual Transactions

[6.2.310] An entity may enter into significant, unusual transactions (SUTs) during the fiscal year. Management must have controls to identify SUTs timely, understand the business purpose for the SUT, understand the financial reporting risks that arise because of the SUT, and design and execute controls to address those risks. The processes and controls for an individual SUT are not typically 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 controls will remain dormant and there will be no instance to evaluate the operating effectiveness of the controls.

Illustration 6.8:
What types of SUTs might the entity enter into?

<table>
<thead>
<tr>
<th>Examples of SUTs:</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Business combinations executed by an entity that is not regularly acquisitive;</td>
</tr>
<tr>
<td>— Issuance of debt, or refinancing of existing debt under a new vehicle or agreement with terms not typical to the entity;</td>
</tr>
<tr>
<td>— A long-lived asset impairment trigger within an entity that does not regularly have triggers;</td>
</tr>
<tr>
<td>— Restructuring charges; and</td>
</tr>
<tr>
<td>— Unusual sales transactions.</td>
</tr>
</tbody>
</table>
Factors management and external auditors should consider when evaluating SUTs, include:

- Understanding whether there are controls to identify SUTs;
- Understanding the business purpose for the SUT (i.e., to assist with the identification of the SUT WCGWs);
- Understanding the SUTs flow of transactions related to the relevant assertions, including how these transactions are initiated, authorized, processed, and recorded;
- Determining the relevant SUTs WCGWs in the process;
- Identifying the SUTs controls implemented to address the SUTs WCGWs;
- Identifying the controls implemented over the prevention or timely detection of unauthorized acquisition, use, or disposition of the entity’s assets that could result in a material misstatement in the financial statements; and
- Selecting and evaluating SUTs controls as appropriate.

**Illustration 6.9:**
What if a SUT occurs, or is identified, after completion of the risk assessment?

**Scenario:**
An entity has a calendar year-end. During July and August, management and external auditor completed and documented their walkthroughs. As a result of these July/August walkthroughs, the parties understand the flow of information, and identify relevant WCGWs and the controls that address them. Then, on December 15, the entity consummates a material business combination.

**What to be aware of:**
Risk assessment is never “completed.” It is iterative. The entity excludes the controls at the acquired business from its ICOFR evaluation, as permitted by the SEC. However, management and the external auditor still should consider controls at the entity related to the proper recording and disclosure of the business combination. This includes the determination of the fair values of assets acquired and liabilities assumed.

The business combination occurred late in the year, after management and external auditor had conducted walkthroughs. Controls over accounting for the business combination are different from controls already evaluated and financial reporting risks already identified. Management and the external auditor should understand the process management went through to record the assets acquired and liabilities assumed, identify the relevant WCGWs and then identify relevant controls. **Importantly, management and external auditor cannot infer the design and operating effectiveness of the controls based on the fact that no audit differences were identified in the accounting for the business combination.**
**Illustration 6.10:**
How should management evaluate a deficiency related to a component of an acquired business that is excluded from management’s ICOFR assessment?

**Scenario:**
An entity has a calendar year-end and completed the acquisition of Business A in August of the current year. Consistent with the SEC’s guidance, management does not intend on testing ICOFR at the Business A level as part of its current year ICOFR assessment.

Prior to the end of the year, management identified two matters with respect to the acquisition:

1. A misstatement and a related deficiency at Business A.
2. Significant changes to the purchase price allocation accounting recorded as of the date of acquisition.

**What to consider:**
Regarding the first matter, because the entity has decided not to include Business A in the current year scope of ICOFR, the deficiency that was discovered at the Business A level as a result of the identified misstatement does not need to be considered when determining whether the entity has effective ICOFR. The entity should consult its legal counsel to determine whether the deficiencies identified at the Business A level are important to users of the entity’s financial statements and therefore, should be disclosed.

Regarding the second matter, while ICOFR of Business A may be excluded from management’s assessment of ICOFR in the year of acquisition, the controls over the purchase price allocation accounting for the business combination operate at the entity level, and therefore, are subject to the entity’s ICOFR testing and assessment, even in the year of acquisition. In determining whether significant changes to the allocation of the purchase price are indicative of a deficiency in ICOFR at the entity level, the following questions may be considered:

— Were the changes to the preliminary purchase price allocation the result of management continuing to execute its processes and controls over the purchase accounting or were they discovered in some other manner? If they were discovered in some other manner, would management have detected the same issue upon execution of the controls over the allocation of the purchase price?

— Were the changes made prior to management finalizing the allocation of the purchase price and is management’s assertion that the acquisition accounting for the acquired assets and liabilities affected by the misstatement were preliminary supportable and consistent with other evidence (i.e., disclosures within the latest SEC filing such as the Form 10-Q)? In the event management identified an error as it completed its process and operated its controls in the course of finalizing the purchase price allocation, it is likely that a change to an account balance would not constitute a deficiency in ICOFR at the entity level.
Illustration 6.11:
A significant unusual revenue transaction is identified

As management and the external auditor perform more work investigating a SUT, they realize it has gone through a process different from the one that they walked through. In considering what to do from an ICOFR perspective, these questions should be considered:

- What controls did management have to detect that an unusual transaction occurred? Have those controls been evaluated? Was this transaction identified because of those controls? If not, why not and could there be similar transactions?
- What was the business purpose for the SUT? What process did the unusual transaction go through? What are the WCGWs in that process? What are the relevant controls?

To the extent that the WCGWs and controls are similar to those of normal recurring transactions, additional control work may not be necessary. But for the part of the process that is different, additional control evaluation is necessary.

Deployment of Control Activities

[6.2.330] Entities should deploy control activities through policies that establish what is expected and through procedures that put these policies into action. According to the COSO Framework, the policies and procedures should assign clear responsibility for the performance of controls, tell the control operators how frequently and when the control activities should be executed, and explain what corrective actions should be taken in response to matters identified in the execution of a control. The policies also should establish competence requirements for the control operators. And, established policies and procedures should be periodically reviewed to ensure their continued relevance.

[6.2.340] Often an entity’s ICOFR policies and procedures are established separately from its business operating policies and procedures. As entities document their understanding of each relevant business process and identify risks and related controls within each process, there will likely be more integration between the entities’ operating procedures and ICOFR procedures. Control activities established in response to the identified risks should be built into the everyday job responsibilities of management and employees at various levels within the organization. They should guide everyday execution of the established controls, specifying who should perform the controls, and when and how the controls should be performed. Control activities should also include the use of knowledge and tools to support effective execution of the controls.

---

8 The description in paragraph 6.2.330 is consistent with the points of focus of Principle 12 described in Internal Control – Integrated Framework published by COSO on May 14, 2013, p. 101.
The control policies and procedures should be documented in writing for each relevant business process and applied consistently across the organization and at all levels. The COSO Framework is very specific about the need for written documentation of control policies and procedures. It acknowledges that policies and procedures are often communicated orally or implied through management’s actions and decisions, but when an entity’s ICOFR is subject to external party review (such as an ICOFR audit), then “policies and procedures would be expected to be formally documented.”

The emphasis on written documentation of control policies and procedures is clear in the COSO Internal Control over External Financial Reporting: a Compendium of Approaches and Examples (Compendium). The first approach suggested by COSO in the Compendium addresses all the points of focus of Principle 12; this approach refers to the documentation of policies and procedures in the form of flowcharts, narratives and control matrices. Whatever documentation format is employed, the example documents referenced in the Compendium clearly define the purpose of the policy and its applicability, the key roles and responsibilities related to the control activities, and escalation procedures for identified exceptions. The example policy documents also specify the frequency with which the policy should be reviewed for its continued relevance.

---

9 Internal Control – Integrated Framework published by COSO on May 14, 2013, p. 102
Control activities are only one component of an effective ICOFR. For example, the control activities of the entity:

— Are affected by and responsive to the control environment in which they operate;
— Are designed based upon the risk assessment of the entity, which includes consideration of external and internal factors, including fraud risk. The risk assessment is performed at the entity level and the process level;
— Rely upon effective information and communication; and
— May need to be adjusted based upon the results of monitoring.

As evidence about the design of control activities is obtained, management and auditors evaluate whether assessments of other components continue to remain appropriate.

Illustration 6.12:
When evidence is obtained about the design of control activities, evaluate this evidence to either support or contradict preliminary assessments about other components

When the design of controls was being evaluated, the following was noted:

— Some controls are performed by people without the appropriate skills to effectively operate the control. This may indicate a deficiency in the control environment, which requires an entity to hire, develop and retain competent personnel. Additionally, if this was not detected by the entity, it may indicate a deficiency in the monitoring process, which should be designed to identify issues with respect to the operating effectiveness of control activities.

— Some controls needed to be redesigned because of changes in the business, but they were not. This may indicate a deficiency in risk assessment, which should identify such changes. It may also indicate a deficiency in the information and communications component, which should communicate identified risks to the appropriate personnel so that changes to control activities can be made.
Key takeaways:

Control Activities

1. **Separate the process from the control.** When processes and controls are not sufficiently distinct, we are challenged to evaluate whether a control structure meets the requirements imposed by COSO Framework.

2. **Select controls that address all relevant WCGWs, including WCGWs related to fraud and safeguarding of assets.** When selecting controls to test, determine if the controls identified appropriately address each relevant WCGW identified in the Risk Assessment process.

3. Remember: **Controls should operate at a “would” not a “could” level.** Precision is an important element in evaluating the design of a control and takes into consideration materiality and risk assessment. Controls should be designed to operate individually or in combination at the “would” level. Precision is not a synonym for materiality.

4. **Consider whether the controls selected are dependent upon other controls.** Often the controls selected for testing rely on the effective design and operation of other controls (e.g., general IT controls and controls over IPE). Test the design and operating effectiveness of those controls as well.

5. Remember a proper ICOFR assessment requires consideration of the design and effectiveness of controls around the identification and accounting for SUTs.
Chapter 7
Management review controls
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 impacting 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 can be process-level or higher-level controls. Process-level controls are generally controls that operate over one or more relevant assertions within a single process whereas higher-level controls typically operate over multiple processes.

While management review controls, particularly those that involve judgment, are an important part of control activities, they likely do not fully and effectively address business process risks without other process-level controls (see the COSO Framework, page 951). The COSO Framework refers to process-level controls as “transaction controls.”

It is often more difficult to obtain sufficiently persuasive evidence about the design and operating effectiveness of MRCs compared to other types of controls because they tend to be more complex controls, often with a high degree of judgment. When evaluating an MRC, the evaluator should place himself in the role of the control operator to assess the appropriateness of the design and operating effectiveness of the MRC.

Management and external audit teams are encouraged to assess the design and operating effectiveness of MRCs early in the ICOFR assessment process. This will provide management with enough time to respond to potential deficiencies and enable both management and external auditors to obtain sufficient evidence to show if the remediated MRC is designed and operating effectively.

1 Internal Control – Integrated Framework published by COSO on May 14, 2013
7.1 Identification and Classification of Management Review Controls (MRCs)

“Management review controls, in particular, are an important element of [management’s ability to successfully transition to the new revenue standard], which is not surprising given the important role that some of these controls play and the amount of judgment that they may involve. I believe the implementation of the new revenue standard provides an opportunity to be proactive and improve the design and operation of management review controls that may exist within a company’s revenue recognition process, including with reference to the various estimates and judgments that the new revenue standard may require. Therefore, as you evaluate your contracts with customers, it would be appropriate to take a fresh look not only at your historical accounting policies and how they may need to change but also at the design of the related controls (both existing and new) to ensure they are designed to operate in a manner that is sufficiently sensitive or precise to prevent or detect a material misstatement in the financial statements.”

– James Schnurr, SEC Chief Accountant

Why is the proper evaluation of MRCs important?
[7.1.10] MRCs are an important part of control activities, particularly for those areas of the financial statements that are subject to significant judgment and subjectivity. However, it is often more difficult to obtain sufficient evidence about the design and operating effectiveness of MRCs compared to other controls because of that level of management’s inherent judgment and subjectivity. Additionally, because MRCs often are used in more judgmental and complex areas that have the potential for a higher risk of material misstatement, the persuasiveness of the evidence required to demonstrate the design and operating effectiveness of the control increases.3

[7.1.20] When designing and evaluating MRCs, management and the external auditor determine whether the control is designed to operate at a level of precision such that it would prevent or detect and correct a material misstatement in a timely manner with respect to the relevant financial statement assertions the control is intended to address. 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. If an MRC is not designed to operate at a sufficient level of precision, or cannot be determined to operate effectively at a sufficient level of precision, the control does not provide evidence necessary to address potential sources of misstatement in the process.

[7.1.30] The adequacy of documentation and evaluation of MRCs has been under significant regulatory scrutiny in recent years. The SEC Staff has stated that these controls might be designed to operate at an appropriate level of precision; however, 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.4 The PCAOB has also highlighted significant auditing practice issues identified in its inspections of external audit firms in this area, specifically as it relates to assessing precision.5 As discussed earlier in this guide, the SEC Staff has stated that the ICOFR issues identified by the PCAOB may not be only a problem of audit execution, but may be indicative of deficiencies in management’s controls and assessments.6

Precision is discussed in greater detail in Section 7.2 of this Chapter.

What are the categories of MRCs?
[7.1.40] Not all MRCs present the same risks and challenges when it comes to evaluation of their design and operation. Accordingly, an entity’s controls may require different approaches to addressing those risks and challenges. While not required by the SEC or the COSO Framework, it may be useful to classify MRCs into one of the following three categories to assist in tailoring the nature, timing and extent of evidence needed to evaluate MRCs appropriately. The higher the category of an MRC, the greater the evidence needed to support the design and operating effectiveness of the MRC.

2 James V. Schnurr, SEC Chief Accountant. Remarks before the 12th Annual Life Sciences Accounting and Reporting Congress, Philadelphia, PA (March 2016)
5 PCAOB Staff Audit Practice Alert No. 11 – Considerations for Audits of Internal Control Over Financial Reporting (October 2013)
6 James V. Schnurr, SEC Chief Accountant. Remarks Before the UCI Audit Committee Summit, Newport Beach, CA (October 2015)
[7.1.50] It is important to draw the distinction between the MRC category and the precision at which the MRC operates. The MRC category and the precision at which the MRC operates are not necessarily correlated. The level of precision is dependent on the objective of the control and many times a category 1 MRC will operate at a very high level of precision as compared to a category 3 MRC as a result of how the controls are designed and the risks of misstatement they are intended to address.

**MRC Category 1**
1. Degree of judgment involved in execution of the control is low
2. Control is generally found within the process and, if it serves as a monitoring control, the MRC is not used to reduce or eliminate reliance on other process-level controls

**MRC Category 2**
1. Degree of judgment involved in the execution of the control is other than low
2. If the control is designed to monitor the effectiveness of other controls, it aims to reduce or eliminate reliance on and testing of other process-level controls or GITCs

**MRC Category 3**
1. Degree of judgment involved in execution of control is significant
2. Control is associated with a relevant assertion that requires significant judgment
3. Generally, other process-level controls are insufficient without this MRC given the degree of judgment involved with respect to the relevant assertions
Examples of MRC that are in category 1:

Management’s review of a bank reconciliation to ascertain the completeness, existence and accuracy of cash is an example of a Category 1 MRC in a situation where the bank reconciliation itself serves as a control rather than part of the process to determine the period-end balance of cash (this may not always be the case; in certain situations, a bank reconciliation may be a key step in the process to determine the period-end cash balance rather than a control). In this situation, there are two controls in place: the bank reconciliation itself and management’s review of the bank reconciliation. The bank reconciliation control is not an MRC, but the review of the bank reconciliation is an MRC that requires only a little judgment. In fact, if reliance is placed on both controls, the review of the bank reconciliation acts as a monitoring control, as contemplated by Principle 16 of the COSO Framework, rather than a control activity.

Another example is a review of a three-way match exception report (control designed to address the existence and accuracy of accounts payable and the related expense and asset accounts) where it takes little judgment to determine whether an exception exists or how to address it. This MRC operates at the process level and does not require significant judgment.

A review control related to a goodwill impairment test might be considered either an MRC 1 or an MRC 3. If there is significant headroom between the fair value of a reporting unit and its carrying value in Step 0 or – in some circumstances – Step 1 of the test, goodwill impairment may not be considered a significant risk of material misstatement of the entity’s financial statements that requires special consideration (significant risk). The degree of judgment required of the control operator to reach the correct conclusion related to the goodwill impairment test is rather limited. Therefore, in such a situation, it is likely that the review control over the goodwill impairment test would be considered to be an MRC 1. Alternatively, the more significant the risk that the estimate presents to reasonably stated financial statements (e.g., when Step 2 of the impairment assessment is necessary or when concluding on Step 1 requires significant judgment), the more likely the related review control would be evaluated to be an MRC 3.
A review control over the allowance for doubtful accounts (control designed to address the valuation of accounts receivable) might be an MRC 1, 2 or 3. Some companies operate in a stable business, have no significant changes in customer base, and there may not be other economic conditions that would suggest history is not a good indicator of current uncollectible accounts. Further, the historical write-offs may be consistent year after year and the total allowance may be less than or only slightly above materiality with little risk of significant understatement. Because of those conditions, the evaluator might conclude that the review control is an MRC 1. At the same time, consistent with all controls, it also is important that management has an effective control in place to monitor changes in the business or the economy to make an informed risk assessment regarding the allowance (this might be an Information and Communication control related to management’s identification, use and communication of relevant quality information to support the functioning of control activities in accordance with Principles 13 and 14 of the COSO Framework). As any of those internal or external factors change, there is a need to consider revising the assessment of the level of judgment required to effectively execute the control over the allowance for doubtful accounts in a manner that would prevent or detect a material misstatement. That, in turn, could result in a change in the classification of the MRC as either category 1, 2, or 3. For example, as the variability of the historical write-offs increases, or when there are significant portions of the allowance that are more judgmental and less based on historical write-offs, the level of subjectivity and judgment involved in the execution of the control increases and the related MRC would more likely fall into either category 2 or 3.

Regardless of the conclusion as to the MRC level, evidence should demonstrate the control is designed to operate at an appropriate level of precision in response to the identified risks (WCGWs) consistent with the guidance contained in this chapter. An MRC 1, because of the lower level of judgment and subjectivity involved in its execution when compared with a level 2 or 3 MRC, would generally require less evidence to demonstrate it is effectively designed. However, the considerations around precision should nonetheless be addressed.

Example of MRC that is not in category 1:
Management’s review of historical product return rates to determine what return rates to use in the sales return reserve (control designed to address the valuation of the sales return reserve), where the sales return reserve is a significant estimate. While this MRC operates at the process level, considerable judgment is involved, and therefore it would most likely fall into MRC category 3.
Examples of MRCs that are in category 2:

Management’s review of depreciation expense to ascertain its completeness, existence and accuracy where process level controls are not tested and relied upon. In entities with a stable asset base, this control may not require significant judgment, and it may be relied upon instead of other process-level controls because the MRC is designed to address all relevant risks in the process (risks at the process level are also referred to as “what could go wrongs” or WCGWs throughout this chapter of the Guide; see guidance beginning at paragraph 7.1.130 for additional discussion about the importance of identifying appropriate WCGWs).

The Chief Financial Officer’s (CFO’s) review of the income statement designed to address completeness and accuracy of expenses. This control operates in a monitoring capacity, as contemplated by Principle 16 of the COSO Framework, and there is likely at least a moderate level of judgment involved. Even though it is a monitoring control, management may design and operate the MRC such that it also operates as a control activity for certain relevant assertions over a significant account. In other words, for certain relevant significant account assertions (most likely those assertions with lower assessed risk), the MRC may be designed at a level of precision that it would prevent or detect a material misstatement in a timely manner.

For example, in the CFO’s review of the income statement, the MRC may operate as a control activity over the accuracy of amortization expense associated with an intangible asset because the low level of judgment required in execution of the control with respect to that assertion allows it to operate at an appropriate level of precision that it would identify a material misstatement. However, the MRC would operate as a monitoring control for the existence of sales because the precision of the control is not sufficient that it would prevent or detect a material misstatement with respect to that assertion.

In such a situation, the MRC would have to address all relevant WCGWs in the process related to the relevant assertions over the significant accounts. An MRC, such as the CFO income statement review described in this example, most often requires other process-level controls to be in place and operating effectively in order for the MRC to operate at the “would” level of precision. Paragraph 7.1.80 includes discussion on the concept of a “suite” of controls that generally would be needed to support the effective operation of an MRC. See paragraph 7.2.110 for a more detailed discussion of the “would” level and precision.

On occasion, these types of controls are used as compensating controls when process-level controls are deficient. An MRC in category 2 or 3 needs to be evaluated with the rigor described in this chapter of the ICOFR Reference Guide when it is identified as a compensating control that mitigates deficiencies in other process-level controls. Refer to further discussion in Chapter 11 of this guide on evaluation of control deficiencies.

Example of MRC that is not in category 2:

Management’s review of the warranty accrual, a significant estimate, to ascertain its reasonable valuation. Because the MRC relates to a significant estimate in the financial statements and because of a high degree of judgment required in execution of the control, this control likely would fall into MRC category 3.
Examples of MRCs that are in category 3:
Management’s review of components of accounting estimates such as the allowance for loan and lease losses, fair value estimate in a goodwill impairment test, and valuation of hard-to-value securities. There is significant judgment involved in operating the control, it is associated with an accounting estimate, and other process-level controls cannot replace it because of the level of judgment involved.

Examples of MRCs that are not in category 3:
Management’s review of an account, or multiple accounts, that are not considered significant estimates. This control would likely fall into MRC category 1 or 2.

Comparison by the controller of the security portfolio prices obtained by the entity from its pricing vendor for financial reporting purposes to an average of prices obtained by the controller from three independent pricing sources. All securities with prices that differ from the average of the three independent pricing sources by more than 5 percent are flagged and sent for investigation by the pricing vendor and revised by the controller based on their findings. The pricing vendor investigates the differences and notifies the controller of any required revisions to the pricing of securities in the entity's records. The controller updates the recorded security prices based on the information provided by the pricing vendor. Even though the control is performed by a member of management and addresses valuation of investment securities, a potentially complex area that may require a significant amount of judgment, the control, as designed, is not an MRC in category 3. The control requires little judgment from the control operator who simply flags certain securities for further investigation by a third party based on an objective threshold. Furthermore, the control, as designed, may not be sufficient to address relevant WCGWs related to the valuation of the entity’s investment securities. The example control could become an MRC in category 3 and better address the relevant WCGWs if its design were expanded to include additional steps such as an independent valuation of the identified outlier securities by the controller, a review by the controller of the outlier securities for attributes which may drive the identified pricing differences, or a review by the controller of the entire investment portfolio for securities which did not meet the 5 percent variance threshold but may still require follow-up or investigation due to their similarity to the outlier securities. These additional steps would likely introduce a significant degree of judgment into the operation of the control.

Illustration 7.3:
Understanding Category 3 MRCs

While the categorization framework described above is a useful way to think about management review controls and will be applied throughout the remainder of this guide, it is important to keep in mind that determination of the nature of each MRC, evaluation of the appropriateness of its design and the extent of evidence needed to demonstrate the control’s operating effectiveness remain a matter of professional judgment. Professional judgment is exercised by both management (when they design and assess the operating effectiveness of controls) and external auditors (when they test MRCs in connection with their audit of internal control over financial reporting). Further, the assessed category of an MRC does not impact the need to understand and evaluate whether the control is designed at an appropriate level of precision to achieve the objective of the control.
Digging Deeper Into the Classification of MRCs

[7.1.70] Once the control objective is understood (i.e., the process, the WCGWs, and the manner in which the control is intended to address the WCGWs), it will be easier to properly categorize the MRC. Additionally, GITCs and entity-level controls are not controls that have a direct impact on the financial statement assertions, and therefore generally do not need to be categorized using the MRC 1, 2 or 3 framework.

[7.1.80] It may be difficult to design a single, broad MRC to address multiple WCGWs. Broad MRCs generally should be disaggregated into individual controls that together function as a suite of controls to address the relevant WCGWs.

[7.1.90] When an MRC is broken down into individual, or “mini-controls,” consisting of a suite of controls over the WCGWs associated with a relevant assertion, it is easier to identify where there is subjectivity in the execution of the MRC and which WCGWs within a process the MRC is capable of addressing.

[7.1.100] Breaking an MRC down into “mini-controls” can be particularly useful in the case of MRCs that address accounting estimates. Such estimates typically are based on a number of significant inputs and assumptions. An MRC associated with the estimate needs to address, either by itself or in combination with other process-level controls, the completeness and accuracy of each one of these significant inputs and assumptions. In such situations, it may be most effective to “disaggregate” the accounting estimate into individual inputs and assumptions and then identify the specific “mini-controls,” representing subsets of the MRC identified at the estimate level, and other process-level controls over those disaggregated elements of the estimate.
Illustration 7.4: 
Breaking down the MRC – Understanding the MRC and the WCGWs that it addresses

Scenario:
Management has identified a key control related to impairment of long-lived assets. The control is described as “management’s review of long-lived assets for impairment.”

On its own, this review control as documented is likely too broad to effectively address all relevant WCGWs associated with the impairment analysis. There are many things that this review control should include to be effective, including determining whether any triggering events require further analysis and analysis of recoverability of the current book value of the long-lived assets using projected future cash flows. Within each of those elements of the impairment analysis, there would most likely be multiple inputs and assumptions with varying degrees of significance, sensitivity and subjectivity.

Breaking down the MRC into different aspects of the long-lived assets impairment process—for example, by which WCGW it addresses—may be helpful.

In this case, reviewing the analysis that led to determining that a triggering event occurred may be (depending on the circumstances) largely objective and fall into a category 1 MRC. But the review of the cash flow projections used in the impairment assessment may be highly subjective and can be identified as a separate MRC 3 from the triggering event identification control. In fact, the review of the cash flow projections may be further broken down into different aspects of that review (e.g., the review controls over projected sales and projected costs may require a different level of judgment depending on the line of business). Management should have sufficiently precise “mini-controls” over each aspect of the estimate and the assessment of each control should focus on whether it is designed to address the related WCGWs.

[7.1.110] Failure to disaggregate MRCs to the appropriate level will often lead to a control that is not capable of effectively addressing all relevant WCGWs. This includes identifying and testing controls over the completeness and accuracy of the information used in the MRC. See section 7.3 for additional guidance related to controls over the completeness and accuracy of information used in the execution of management review controls.

MRC Considerations
[7.1.120] Distinguishing a control from a process is a critical step in the determination of the proper design and operating effectiveness of any control. This distinction may be particularly difficult in areas requiring significant judgment which is where many management review controls in category 2 and 3 operate. Processes, and the related activities, are separate from the controls. Similarly, control operators should be independent from the process owners who initiate, process and eventually record transactions in the financial statements. This is why Principle 10 of the COSO Framework requires an understanding of the process and identification of WCGWs within the process prior to selecting controls. It is the activities within the process that may introduce errors in the financial statements. Controls are established to prevent or detect those errors.
[7.1.130] There are certain things to understand about every control, not just MRCs, to be able to evaluate the design and effective operation of the control. The SEC Staff has stated that in order to determine whether the operation of a control is effective, management should consider factors such as:7

— How the control is applied;
— The consistency with which the controls are applied; and
— Whether the person performing the control possesses the necessary authority and competence to perform the control effectively.

[7.1.140] Consideration of factors such as how the control is performed and whether it is applied consistently requires understanding of the metrics, thresholds or other criteria used in the execution of the control to identify outliers and exceptions and how such outliers and exceptions are followed up on and resolved. See section 7.2 for a more detailed analysis of the importance of metrics, thresholds and other criteria used in the execution of management review controls.

[7.1.150] The SEC Staff has stated that when evaluating a control and the evidential matter supporting the appropriate design and operating effectiveness of the control, we consider the nature of the relevant assertions over the significant accounts and disclosures that the control is supposed to address, including the extent to which such accounts and disclosures:

— Involve judgment in determining the recorded amounts;
— Are susceptible to fraud;
— Have complex accounting requirements;
— Experience change in the nature or volume of the underlying transactions; or
— Are sensitive to changes in environmental factors, such as technological and/or economic developments.

[7.1.160] Those evaluating an MRC should place themselves in the role of the control operator to understand the factors discussed in paragraph 7.2.190 and how they may impact the design and operation of the control. For routine, process-level controls, including controls classified in MRC category 1, the documentation and testing of the design and operating effectiveness of a control may be relatively brief compared to more complex controls. By contrast, controls that fall into MRC categories 2 and 3 may require more robust documentation and testing.

[7.1.170] As discussed earlier in this chapter, when determining the level of documentation and test work necessary for any control, consider whether the persuasiveness of the evidence supporting the design and operation of the control is commensurate with the level of risk that the control is intended to address, and whether an experienced accountant would be able to understand the design and operating effectiveness of the control based on what has been documented. As the level of assessed risk of material misstatement increases, the persuasiveness of evidence necessary to demonstrate effective design and operation of controls increases.

---

Illustration 7.5:
Evidence and documentation should be commensurate with the level of risk

MRC Category 1:
When describing the design of management’s review of a bank reconciliation when the bank reconciliation itself serves as a control which is also being relied upon, the documentation may not need to be overly detailed for an experienced accountant to understand the criteria used in the execution of the review control (whether the book balance fully reconciles to the bank statement) and what constitutes an outlier (e.g., reconciling items outstanding for longer than one month and over a certain $ amount).

MRC Category 3:
When evaluating the design of a control that entails a review of projected financial information used in an intangible asset impairment assessment, the approach to evaluate the MRC must be tailored to provide sufficient evidence commensurate with the WCGWs and the higher level of risk that the projected financial information review is designed to address. Additionally, the documentation likely would be more thorough, including robust discussion on the criteria applied by the control operator and the outliers, to provide an experienced accountant with sufficient information to be able to reach a conclusion about the design of the control.

The Importance of Process-Level Controls in the Design of MRCs

[7.1.180] According to the guidance provided by the COSO Framework for Principle 10, when selecting and designing control activities, it is important to understand what a particular control is designed to accomplish, i.e., what specific risk (or WCGW) within a business process it is supposed to mitigate.

[7.1.190] The specificity and clarity with which an identified risk (WCGW) is defined are key to management’s ability to design a control that is appropriately responsive to that particular risk. A properly defined risk is also critical to management’s and external auditors’ effective evaluation of the control. A WCGW is not simply the risk that an account or disclosure could be misstated. It is also not merely the absence of a control. Rather, a well-defined WCGW focuses on the conditions that could allow misstatements to enter the system or the data to lose its integrity. (See chapter 5 of the ICOFR Reference Guide – Risk Assessment – Understanding WCGWs for further discussion).

[7.1.200] To successfully identify relevant WCGWs and their related process-level controls, it is necessary to have a sufficient understanding of the business process and the flow of information through the system (this is true for both routine processes, such as sales or procurement, as well as for significant unusual transactions, such as business combinations or impairment of goodwill). Flowcharting may be an effective way to obtain and document this understanding. (See chapter 5 of the ICOFR Reference Guide – Risk Assessment – Understanding WCGWs for further discussion).
The responsibility to obtain a proper understanding of the business process, the flow of information, and the risks (WCGWs) within the process starts with management. It should not be assigned solely to 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 and documentation are missing or deficient. In this respect, the SEC Staff has stated that management should identify those risks of misstatement that could, individually or in combination with others, result in a material misstatement of the financial statements. Management should use its knowledge and understanding of the business, and its organization, operations, and processes, to consider the sources and potential likelihood of misstatements in financial reporting elements; otherwise a deficiency exists in the risk assessment component of management’s internal control over financial reporting.

Thorough analysis and understanding of a business process usually results in the identification of multiple WCGWs within the process. There may be situations where an MRC alone is sufficient to address all relevant WCGWs within a process and prevent or detect a material misstatement, but those situations are rare. In most cases, an MRC sufficiently addresses only some of the WCGWs within a process, and there need to be other process-level controls identified that will address the remaining risks, including controls over the completeness and accuracy of the information used by the MRC. See section 7.3 for additional guidance related to controls over the completeness and accuracy of information used in the execution of management review controls.

With respect to an MRC in category 3, the MRC is necessary because other process-level controls are unlikely to adequately address the risk of a material misstatement given the amount of judgment required by the subject matter of the review control. However, that does not mean that the evaluation of controls for a particular business process should be limited to that MRC 3. To the contrary: it is likely necessary to identify and evaluate other process-level controls in addition to the MRC 3, including controls over the completeness and accuracy of the information used by the MRC. Often, for an MRC 3 to operate effectively, one or more additional process-level controls also need to be in place and operating effectively. Consistent with the guidance in section 7.1.80, these process-level controls are part of the suite of controls that are necessary to address all WCGWs. Without considering this suite of controls, the MRC in and of itself may not reach the required would level of precision. This is consistent with the COSO Framework, which states that while management review controls “are important in the mix of control activities, it is difficult to fully and efficiently address business process risks without transaction (process-level) controls.”
Illustration 7.6:
Considerations when selecting process-level or Management Review Controls

MRC Category 2:
If the CFO's review of the income statement for completeness and accuracy of expenses is considered to be designed appropriately and with sufficient precision and the entity has documentation that provides sufficient evidence of the review control's design and operating effectiveness, it still may be appropriate to test process-level controls. Process-level controls, such as controls over the coding of expenses to the appropriate general ledger account and controls over allocating certain expenses among income statement accounts, provide additional persuasive evidence that is often difficult to obtain by solely relying on the MRC. As stated previously, the combination of the MRC and the process-level controls provides more persuasive evidence than the MRC alone, and may allow the MRC to function in a monitoring capacity.

MRC Category 3:
For example, the review of the warranty accrual to ascertain its appropriate valuation is likely to require controls over the completeness and accuracy of return data by product, the number of units sold, or other metrics and measurements (see section 7.3 for a discussion of controls over the information used in the execution of management review controls). It also may be necessary to identify controls related to the build-up of the warranty accrual, including controls over key decisions made throughout the process. The extent and precision of controls over key decisions made throughout the process may result in the MRC being designed and executed as a less precise, redundant or monitoring control.
Key takeaways:

Identification and Classification of MRCs

1. **Understand the process** within which an MRC operates and the risks (WCGWs) within the process before evaluating the MRC.

2. **Distinguish a process from a control.** Remember that it is the process activities that may introduce misstatements to the financial statements. Controls are established to prevent or detect misstatements.

3. There may be situations where an MRC alone is **sufficient** to address all WCGWs within a process and prevent or detect a material misstatement, but those situations are rare.

4. Consider identifying and testing the operating effectiveness of other **process level controls** that will address some of the WCGWs within the process in addition to or in lieu of a Category 2 or 3 MRC.

5. To guide in determining the nature, timing and extent of evidence needed to conclude on the design and effectiveness of an MRC, **classify each MRC** that is expected to be relied upon into one of the three categories **based on its level of risk.**

6. **By breaking an MRC down into “mini-controls,”** it may be easier to understand where there is subjectivity and determine whether the MRC addresses all relevant WCGWs within the process. Some WCGWs may need to be addressed by other controls.
The Importance of Establishing Criteria

[7.2.10] It is important to establish defined and objective criteria for investigation to be used in the execution of MRCs. The established criteria for investigation determine the level of precision with which a given control is designed to operate. Precision of a control frequently can be understood as the magnitude of a potential misstatement that could be accepted based on the control’s design and operation.

[7.2.20] Establishing criteria for investigation in the design of the control sets the parameters for the MRC as to the characteristics within the information or data being reviewed that will trigger additional action on the part of the control operator to validate appropriateness – otherwise known as an “outlier.” The identification of an outlier does not necessarily represent a misstatement that needs to be corrected. Rather, an outlier is a characteristic of the information being reviewed, as established in the design of the control, which requires further investigation by the control operator. That investigation may either confirm the appropriateness of the outlier, determine the outlier is an error which requires correction, or determine that further information or activities are necessary in order to resolve the matter. An MRC’s criteria for investigation determine its level of precision and whether the MRC is capable of addressing the WCGWs it is intended to address.

[7.2.30] Without establishing defined and objective criteria for investigation, understanding whether the MRC is designed to consistently operate at an appropriate level of precision to achieve the objective of the control (i.e., operate at the would level), becomes challenging.

[7.2.40] When establishing or evaluating the criteria to be used in the execution of MRCs, management and external auditors consider a number of factors in assessing the precision of the control which are discussed in more detail beginning at paragraph 7.2.220.

Illustration 7.7:
Metrics, thresholds and criteria vs. the level of a control’s precision

An entity’s ERP system performs an automated three-way match control as part of the purchasing process and identifies discrepancies between the vendor invoice, the related purchase order, and the receiving documentation. At the end of each day, an accountant in the Accounts Payable department generates a report from the system showing all discrepancies on the purchase transactions processed during the day. Each day, a control operator reviews the report and investigates any discrepancies in excess of $10. The $10 threshold represents the criteria for investigation in this review control and the level of precision at which the review control is designed to operate. Based on the control’s design, a potential error in the entity’s accounts payable and the cost of the acquired assets or services of up to $10 in each individual purchase transaction has been determined to be acceptable by management.

Determining whether the $10 criteria for investigation allows the control to operate at the right level of precision depends on the objective of the control. While the $10 precision level may seem low, the three-way match operates hundreds or thousands of times in any reporting period. The $10 differences that may be acceptable in individual transactions might eventually add up to a number that becomes significant to the entity’s financial statements.
When evaluating the threshold for investigation established in the three-way match review control, it is also important to consider the objective of the control (existence and accuracy of payables and related asset or expense accounts and safeguarding of the entity’s resources) and the nature of transactions to which the control is applied (routine purchases of goods and services at objectively determinable prices). Taking into account these two important considerations, if the threshold for investigation of discrepancies identified through the three-way match were established at, for example, $20,000, this would raise obvious questions about the effectiveness of design of the control, including the risk of bias on the part of the person who established the high threshold for investigation.

Similarly, in management’s review of a bank reconciliation, the threshold for investigation of reconciling items would likely be established at a relatively low level regardless of the size of the entity’s balance sheet or scale of its operations. The design of the control should take into account the objective of the control (completeness, existence, accuracy and safeguarding of the entity’s cash balances) and the nonjudgmental and easily verifiable nature of transactions that typically flow through the cash accounts.

On the other hand, the criteria for investigation in management’s review of a more subjective area of the financial statements, such as a warranty accrual may be established at a relatively higher level considering the objective of the control (reasonable valuation—not absolute accuracy—of the accrual and the nature of the significant account over which the review is performed (complex, judgmental, based on a number of variables). Establishing the criteria for investigation at a relatively higher level may also be justified in certain MRCs by the existence of more precise process-level controls over related data elements and WCGWs of the account balance.

See guidance beginning at paragraph 7.2.150 regarding precision of controls as compared with materiality and the established risk tolerances.

[72.50] Establishing criteria for investigation to be used in the execution of controls is important for all types of control activities. However, it is particularly important that management articulates—and external auditors understand—the established criteria for MRCs in category 2 and 3 which typically involve a significant degree of judgment and have a tendency to be performed informally, “in the minds of management,” and “based on the knowledge and experience” of the control operator with the matter being reviewed. Because of this, effective documentation of management’s criteria for investigation when executing an MRC is important to provide evidential matter that it is consistently performed at an appropriate level of precision.

Why it is important to understand the established criteria for MRCs

— The criteria are likely not readily discernible based on the description of the control.

— Without established criteria, it is difficult to determine whether the control is precise enough to detect or prevent a material misstatement.

— Without established criteria, it is difficult to determine whether the control is performed consistently.

— Without established criteria, it is difficult to determine if the MRC appropriately addresses the identified WCGW(s).
When evaluating whether, based on the established criteria, the MRC operates at a sufficient level of precision, it is important to understand what the control operator is supposed to do, how often they are supposed to do it, and what they are specifically considering when executing the control. In essence, the evaluator of the control should be able to place himself in the position of the control operator.

Additionally, many times criteria for investigation in an MRC are established to investigate instances where actual amounts or balances differ from planned or period balances in excess of a certain threshold. For example, in the case of a review control, actual financial results are compared to a budget and differences in excess of a specified threshold are investigated by the control operator. It is important to evaluate whether that criteria for investigation allows the control to operate at a sufficient level of precision. However, control evaluators also need to consider whether the design of the control would effectively identify for investigation balances that did not change in excess of the defined threshold, but should have. If the criteria for investigation are not capable of identifying such instances, the criteria may not be appropriate such that the MRC is likely not designed to consistently operate at the would level.

Level of Evidence Obtained from the Entity’s ICOFR Procedures

The SEC does not provide a lot of guidance on required specificity of management’s control design and operation documentation. The SEC Staff has stated® that the nature and extent of evidence should increase as the risk related to the control increases. MRCs generally address higher risks to the financial statements and, therefore, management should have robust evidence surrounding the design and operating effectiveness of these controls.

What the SEC and COSO have said about MRCs

The SEC has stated on pages 44-45 of its 2007 interpretative guidance:

— “In contrast (to management), the auditor is responsible for conducting an independent audit that includes appropriate professional skepticism. Moreover, the audit of ICFR is integrated with the audit of the entity’s financial statements. While there is a close relationship between the work performed by management and its auditor, the ICFR audit will not necessarily be limited to the nature and extent of procedures management has already performed as part of its evaluation of ICFR. There will be differences in the approaches used by management and the auditor because the auditor does not have the same information and understanding as management and because the auditor will need to integrate its tests of ICFR with the financial statement audit.

— We agree with those commentators that suggested coordination between management and auditors on their respective efforts will ensure that both the evaluation by management and the independent audit are completed in an efficient and effective manner.”

The COSO Framework states on page 30 that controls which require a significant degree of judgment (which is the case with many MRCs) cannot be performed entirely in the minds of senior management without some documentation of management’s thought process and analyses. The Framework also emphasizes that in cases where management asserts to regulators (such as the SEC) on the design and operating effectiveness of its system of internal control, management has a higher degree of responsibility with reference to evidence supporting their assertion. The Framework says:

— “In considering the nature and extent of documentation needed, management should remember that the documentation to support the assertion will likely be used by the external auditor as part of his or her audit evidence, including the sufficiency of such documentation for those assertions. Management would also need to document significant judgments, how such decisions were considered, and how the final decisions were reached.”

In Principle 12, the COSO Framework points out additional advantages of properly documenting in writing the design of control procedures, including MRCs which are some of the most challenging controls to both design and execute. It states, among other benefits, that written documentation of how, when and by whom controls should be executed increases accountability of the control operators, makes the established control procedures more difficult to circumvent, and facilitates transfer of ownership of controls in case of personnel turnover.9

[72.90] When documenting the design and operation of an MRC, management should consider whether the level of documentation is sufficient for both its purposes and from an external audit perspective. Management should guard against limiting its documentation because of its familiarity with the control and the related business process and consider the needs of external auditors who are required to gather sufficient appropriate evidence of the MRC’s design and operating effectiveness under relevant professional standards. Concluding on the design and operating effectiveness of MRCs from an audit perspective becomes increasingly difficult when the control operator does not maintain sufficiently detailed documentation—even when the documentation maintained might be viewed as being sufficient for management’s own assessment.

[72.100] KPMG has developed the Design of a Review Control by Management, the Review Control Execution Documentation, to facilitate management’s analysis and documentation of the design and effective operation of MRCs in category 2 and 3. The templates are included as Appendix 7.1 and Appendix 7.2 to this chapter of the ICOFR Reference Guide. KPMG has also developed the Evaluation of a Review Control by Management template to assist internal auditors and others working under the direction of management in their evaluation of the design and operating effectiveness of MRCs in category 2 and 3 and the appropriateness and sufficiency of documentation supporting these controls. That template is included as Appendix 7.3 to this chapter of the ICOFR Reference Guide.

[72.110] As stated in Illustration 7.2, category 2 and 3 MRCs, and MRCs identified as compensating controls that mitigate deficiencies in other process-level controls should be documented with the rigor described in this chapter of the ICOFR Reference Guide. Known control deficiencies place an extra burden of proof on compensating controls and the evidence needed to conclude that they mitigate the risks exposed by the control deficiencies to an appropriately low level.

[72.120] It may be beneficial for management to coordinate evaluation of MRCs with external auditors. Evaluation of MRCs by external auditors early in the audit process will provide management with enough time to respond to identified deficiencies and enable both management and the external auditors to obtain sufficient evidence of the appropriate design and operating effectiveness of the remediated controls.

9 COSO Framework, p. 102.
Determining Whether the Design Achieves the Objective of the MRC

The evaluation of the design of an MRC should be considered in terms of each WCGW the control is designed to address and upon which reliance will be placed. In particular, when testing the MRC, the evaluator should place himself in the position of the control operator when executing and evaluating the MRC based on the defined criteria, outliers, etc. For all MRCs, but particularly for category 2 and 3 MRCs, determining whether the design achieves the objective of the MRC includes understanding the significant assumptions and whether the control operator’s review is designed to determine the appropriateness of those assumptions. Consider for example the following:

<table>
<thead>
<tr>
<th>Considerations when evaluating the design of the MRC</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>The criteria are appropriate and address the objective of the control</td>
<td>For example, an MRC is designed to review fluctuations in income statement accounts greater than $100K. Consider whether the MRC is designed to address the WCGW (irrespective of the precision of the control). In this case, the WCGW relates to the completeness and accuracy of certain income statement accounts. Note that the MRC addresses fluctuations greater than established tolerance. However, the MRC, as designed, is not effective at detecting items that should have fluctuated but did not. In this case, the MRC may not effectively address all WCGWs, and reliance on process-level controls in lieu of or in addition to the MRC may be necessary.</td>
</tr>
<tr>
<td>Similarly, an MRC designed to identify for further investigation investment securities whose prices changed by more than 5 percent as compared with the previous period would not address the risk that prices of certain securities should have changed but did not. To address that risk, depending on the specific circumstances of the entity and the characteristics of its investment portfolio, it may be necessary to design a separate control whose criteria for identifying items for further investigation may need to be defined as fluctuations in prices of less than 5 percent.</td>
<td></td>
</tr>
<tr>
<td>Likewise, an MRC designed to identify for further investigation securities whose price fluctuations during a period deviated from the movement in the corresponding yield curve by more than 5 percentage points would not address the risk that prices of certain securities should not have followed the overall market trend due to circumstances specific to these securities or their issuers. This WCGW would again need to be addressed by other controls separate from the MRC or the MRC itself would need to be modified to address the additional WCGW.</td>
<td></td>
</tr>
</tbody>
</table>
### Considerations when evaluating the design of the MRC

<table>
<thead>
<tr>
<th>The control operator considers or should consider additional information to identify outliers</th>
<th>For example, when evaluating the control, the evaluator places himself in the role of the control operator, and may determine that the control operator considers much more than the entity has described in its documentation. Or, in evaluating the MRC with respect to the valuation of accounts receivable, the evaluator may determine that the design of the MRC, which consists primarily of the control operator’s review of the A/R aging, is insufficient without additional information such as the receivables aged by geographic location or by customer. In both cases, the MRC documentation should be supplemented to better document the control’s design. The above-mentioned Design of a Review Control by Management template attached as Appendix 7.1 to this chapter of the ICOFR Reference Guide may assist in proper documentation of the relevant design considerations.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The defined outliers are appropriate given the control’s objective.</td>
<td>An MRC over the valuation of accounts receivable may define outliers as any amount past due more than 120 days (the age of an outstanding balance of more than 120 days represents the threshold for investigation of this review control). However, as the evaluator places himself in the role of the control operator, he may determine, based on write-off history, that once a receivable is past due for 90 days, there is a high likelihood it is uncollectible. In this case, he might feel that the defined outliers and the related threshold for investigation that only include receivables greater than 120 days may not be appropriate given the control objective. Instead, the control operator may need to review all receivables from customers with significant past due amounts, including those that are 90+ days overdue.</td>
</tr>
</tbody>
</table>

---

**Precision, Materiality and the Would Level**

[7.2.140] Precision and the established criteria for investigation are inextricably linked. When considering if an MRC is precise enough, place yourself in the role of the control operator. Determine if the operator is considering the appropriate control characteristics and objectives and, based on the established metrics, if the control operator’s expectations are set at a level that would prevent, or detect and correct a material misstatement every time the control operates.
When considering precision, evaluate whether the control is designed to operate at a \textit{would} level—meaning the control, if operating effectively, \textit{would} prevent, or detect and correct a material misstatement. \textit{Would} represents a “probable” level of assurance, meaning there is only a less than reasonable possibility of a material misstatement in the relevant assertion(s) from the WCGW addressed by the control over a significant account or disclosure addressed by the control. While this threshold is a consideration for the design of all controls, it is particularly important when evaluating the design of management review controls.

Determining whether the control is precise enough such that it \textit{would} prevent or detect and correct a material misstatement requires judgment, particularly for category 2 and 3 MRCs.

Guidance provided for Principle 10 in the COSO Framework states that \textit{precision of controls should be considered in the context of the organization’s risk tolerance} for a particular objective. The tighter the risk tolerance, the more precise the actions to mitigate the risk and the related control activities need to be.\(^\text{10}\)

The COSO Framework defines risk tolerance as “the acceptable level of variation in performance relative to the achievement of objectives”\(^\text{11}\), with “variation in performance” understood as uncorrected misstatements and “objectives” defined as relevant assertions (completeness, existence, accuracy, valuation, obligations and rights, and presentation) over significant accounts and disclosures in an entity’s financial statements. Risk tolerance for individual financial statement accounts and disclosures is established quantitatively at a level that is lower than materiality for the financial statements as a whole. This is to reduce to an appropriately low level the probability that the aggregate of uncorrected misstatements in individual accounts or disclosures will become material to the financial statements taken as a whole.

The fact that precision of controls is considered in the context of risk tolerance established for the related significant accounts or disclosures does not mean that each control’s precision should be set at the level equal to the risk tolerance. To the contrary: \textit{precision of individual controls may need to be set at a level much lower than the established risk tolerance} to account for the risk that errors in individual transactions subjected to a particular control may aggregate to a value that exceeds the established risk tolerance for the related significant account or disclosure. On the other hand, due to the level of imprecision inherent in certain significant accounting estimates, it may be impossible for management to design review controls over these estimates with precision that falls within the established quantitative measure of risk tolerance. In such situations, an MRC alone may not be sufficient to prevent or detect and correct a material misstatement in the significant accounting estimate and other controls may need to be identified to achieve that objective, such as controls that address the risk of management bias.

\(^{10}\) COSO Framework, p. 93.
\(^{11}\) COSO Framework, p. 61.
Evaluating precision in terms of risk tolerance
The following should be considered when evaluating the precision of MRCs:

— **As the control becomes less precise** (i.e., as the designed precision of the control approaches the established risk tolerance), the ability of that control to function at the would level becomes less likely and skepticism about its ability to function at the would level increases. This generally means that it is necessary to gather more persuasive evidence about the control’s design and effectiveness.

— The inherent uncertainty surrounding certain estimates may exceed the established quantitative measure of risk tolerance for the estimate. This may be the case in particular for significant accounting estimates, such as the Allowance for Loan and Lease Losses (ALLL) for banks, insurance reserves, goodwill impairment, business valuations, legal contingencies, and the warranty reserves. The MRC cannot operate more precisely than the inherent imprecision of the estimate; however, in such circumstances, the **MRC should not operate less precisely than the inherent imprecision.** Moreover, additional controls (other than the MRC) may need to be identified to appropriately address the risk of a material misstatement in the estimate. They may include controls that address the risk of management bias including controls over consistent application of the methodology used to determine the estimate, controls over the placement of the estimate within a range of reasonable results, and others.

— For all MRCs, especially those in category 3, be aware of the **risk of bias in the design (including precision) and execution of the controls.** That risk increases significantly in the case of controls such as those described above where inherent uncertainty surrounding the estimate exceeds the established risk tolerance. Separate controls may need to be identified to address the risk of bias in estimates. See discussion beginning at paragraph 7.2.250 for additional considerations related to the impact of bias on management review controls.

**Illustration 7.8:**
Inherent imprecision greater than risk tolerance

An entity recently completed a business acquisition and is in the process of performing the purchase price allocation and accounting for the transaction. In the run-up to the acquisition, the entity designed and documented a process to account for the transaction, analyzed the flow of relevant information, and identified the key risks (WCGWs) within the process and controls to address those risks. One of the identified controls is a review by the controller of the reasonableness of projected sales information to be used in the valuation of a trade name acquired by the entity as part of the transaction. Sales revenue attributable to the trade name is projected by the entity’s Financial Planning and Analysis (FP&A) Department which is separate from the controller’s office.
In designing the review, the controller notes that materiality determined by management for purposes of its ICOFR assessment is $5 million and the risk tolerance established for valuation of intangible assets is $3 million. The estimated fair value of the trade name (based on the projected sales information submitted for the controller’s review) is $300 million. There are no observable market prices for the trade name. The controller’s review will consist primarily of comparing the projected growth in sales revenue over the next five years to the historical average calculated over the same period of time because management determined historical sales levels represent a relevant metric to assess projected sales based on the nature of the business. The controller will also compare the projected sales growth to industry expectations obtained from a trade publication.

In contemplating the criteria to be used to identify unusual year-over-year changes in the projected sales revenue, the controller notes that a 0.5 percentage point change in the projected revenue growth rate from either the historical average or the industry expectation would change the estimated fair value of the trade name by about $5 million. This exceeds the established risk tolerance but represents only 1.7 percent of the estimated fair value of the trade name. The controller considers the amount and the significance of assumptions made by FP&A personnel in developing the projected sales information. The controller also recognizes that establishing criteria for identification of outliers at or below the risk tolerance level would not be practical as it would likely identify all annual changes in the projected sales for investigation and be at a level of precision beyond what we would reasonably expect the control to operate. In other words, the projection itself is inherently imprecise and it cannot become more precise if the control operates at a level that would investigate smaller differences.

Taking this into account, the controller considers relevant GAAP guidance for determining the fair value of assets for which no observable market prices are available. The controller notes that in such situations GAAP requires that valuation methods incorporate assumptions that marketplace participants would use in their estimates of fair value whenever that information is available without undue cost and effort.

Considering the GAAP guidance, the controller defines the threshold for investigation as a deviation of the projected annual sales growth of 2 percentage points or more from either the historical average or the industry expectations. In making that determination, the controller considers his experience in the industry, the historical volatility of the entity’s sales, questions raised by market analysts when the entity’s sales deviate from the market consensus, and other relevant factors. The controller concludes that the 2-percentage-point threshold for identification of outliers will ensure that the projected growth in sales attributable to the trade name is well within the marketplace participants’ expectations and thus reasonable. Perhaps most important, the controller has determined that the 2-percentage-point threshold is as precise as the control can reasonably operate, even though it is above the established risk tolerance. This is appropriate only when the inherent imprecision of the estimate exceeds the established risk tolerance. The controller documents the design of the review control and his rationale for the selected criteria. Further, because of the size of the estimate fair value of the trade name and the significant amount of judgment involved in estimating that fair value, there is likely a higher risk of misstatement in this area of the financial statements. As previously discussed in this Guide, as the level of misstatement risk increases, so too does the level of evidence necessary to demonstrate the effective design and operation of controls.
The design of the review control discussed in this Illustration takes into account the inherent imprecision of the estimate addressed by the control (valuation of the acquired trade name) and considers relevant GAAP guidance applicable to the estimate. While the selected threshold for identification of outliers allows for a degree of variability in the fair value of the trade name that exceeds the established risk tolerance, it ensures that the review control does not operate less precisely than the inherent imprecision of the estimate defined by the reasonable expectations of marketplace participants. As stated in paragraph 7.2.160, given the significant imprecision inherent in the estimated fair value of the acquired trade name, separate controls may need to be identified to sufficiently address remaining risks, such as management bias in the estimate.

The outliers identified through the operation of an MRC may indicate whether the established precision and the criteria used by the control operator to identify items for follow-up and investigation are set at an appropriately low level.

The criteria established by the control operator may need to be dynamic in order to operate at the would level. They may need to be adjusted in response to changes in various external and internal factors, including the nature of the subject matter of the review control. Management should have controls in place to monitor such changes and respond to them on a timely basis, including through adjustments to the existing system of internal controls, in accordance with the Risk Assessment principles of the COSO Framework. See paragraph 74.90 for an illustration of these concepts.

Factors to Consider with Respect to Precision

As stated earlier, the precision of a control frequently can be understood to be the size of a potential misstatement the control would prevent, or detect and correct, if the control operates effectively (or—taken from a different perspective—the maximum size of a potential misstatement that could be accepted based on the control’s design and operation).

In general, an individual control should be designed such that its precision is at an appropriately low level that potential misstatements that might result from the operation of all controls across the organization would not aggregate to a reasonable possibility of a material misstatement of the entity’s financial statements, after factoring in the inherent probability of an error occurring.

The level of precision of a control is affected by a number of factors. The PCAOB addressed the factors that affect the level of precision of an MRC. A well-documented MRC would include consideration of each of the following factors regarding its designed precision level:

— The objective of the review

A procedure that functions to prevent or detect misstatements generally is more precise than a procedure that merely identifies and explains the difference.

12 PCAOB Staff Audit Practice Alert No. 11 – Considerations for Audits of Internal Control Over Financial Reporting (October 2013) pages 19-21
For example, a CFO’s review of the financial statements may be an important monitoring control, but may not be designed to be a control activity that would consistently prevent or detect a material misstatement—this is similar to how external auditors use final analytical procedures. There typically are other effective process-level controls in place to prevent or detect and correct a material misstatement. In this case, management and external auditors may test and rely on the CFO’s review control as a monitoring control, but such reliance would not eliminate the need to test and place reliance on the process-level controls. The evidence of the appropriate design and effective operation of those process-level controls constitutes the primary ICOFR evidence for both management and external auditors.

The SEC states\(^\text{13}\) that, with respect to monitoring controls such as the CFO review in the example noted above, “it is unlikely that management will identify only this type of entity-level control as adequately addressing a financial reporting risk.”

The SEC Staff further notes\(^\text{14}\) that “the more indirect the relationship to a financial reporting element, the less effective a control may be in preventing or detecting a misstatement.” This is why it is important to understand how such controls address each WCGW related to relevant assertions.

For example, an MRC is designed to identify and investigate variances over a certain threshold from the prior year. But in understanding a WCGW that the MRC is designed to address, it may be determined that investigating variances from the prior year may not identify all outliers that should be investigated. This may lead to a conclusion that the MRC is not designed properly to operate at the \textit{would} level. This failure to identify all outliers also explains why it often is insufficient to use an MRC as the only control to address the WCGWs related to relevant assertions.

— **The level of aggregation**

A control that is performed at a more granular level generally is 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 company revenue. An analysis of components of cost of sales, such as cost of sales by region or location, or other disaggregated data is more precise than a consolidated gross margin analysis, all else being equal. The greater ability of the analysis of the disaggregated components of costs to identify misstatements generally should be reflected in the design of the review control in the form of more precise criteria used to identify outliers that may require investigation.

— **The consistency of performance**

A control performed routinely and consistently generally is more precise than one performed sporadically. MRCs need not only operate at a level of precision where they \textit{would} prevent or detect a material misstatement, individually or when aggregated; they also must consistently operate at that level every time they are executed.

\(^{13}\) SEC Release No. 33-8810 p. 18

\(^{14}\) SEC Release No. 33-8810 p. 18
— **Correlation to relevant assertions**

A control that is indirectly related to an assertion normally is less likely to prevent or detect misstatements in the assertion than a control that is directly related to an assertion. For example, a control designed to detect errors in the recorded amounts of accounts receivable might not operate with a sufficient level of precision to detect errors in the valuation of delinquent receivables. Conversely, a control that is properly designed to be directly related to the relevant financial statement assertion, such as an aging analysis review by the controller, might operate at a higher level of precision as it relates to valuation of receivables.

— **Predictability of expectations**

Some entity-level controls are designed to detect misstatements by using key performance indicators or other information to develop expectations about reported amounts ("detective controls"). The precision of those controls depends on the ability to develop sufficiently precise expectations to highlight potentially material misstatements. For example, GDP growth likely is not a KPI that would help management set a sufficiently precise expectation about revenue growth.

A control performed on an account that is predictable would be expected to be designed with a greater level of precision than one performed on an account that is unpredictable.

For example, in situations involving reliance on both process-level controls and an MRC in category 2, a highly predictable account may lend itself to placing more reliance on the MRC and less on process-level controls. Alternatively, with a less predictable account, it may be necessary to place more reliance on process-level controls and less on the MRC.

— **Criteria for investigation**

For detective controls, the threshold for investigating deviations or differences from expectations relative to materiality is an indication of a control's precision. For example, a control that investigates items that are near the threshold for financial statement materiality has less precision and greater risk of failing to prevent or detect misstatements that could be material than a control with a lower threshold for investigation.

[7.2.250] The PCAOB provided the following guidance when testing the design of MRCs\(^\text{15}\), which is consistent with the guidance throughout this section of the Chapter:

> “Auditing Standard No. 5 provides that the auditor should test the design effectiveness of controls by determining whether the company’s controls, if they are operated as prescribed by persons possessing the necessary authority and competence, satisfy the company’s control objectives and can effectively prevent or detect errors or fraud that could result in material misstatement of the financial statements.

\(^{15}\) PCAOB Staff Audit Practice Alert No. 11, Considerations for Audits of Internal Control Over Financial Reporting (October 2013), pages 21-22.
Evaluating whether a management review control is capable of preventing or detecting potential material misstatements generally involves obtaining an understanding of and evaluating the following:

a. Whether the control satisfies the corresponding control objective, including whether it addresses the risks of material misstatement to the relevant assertion of the significant account or disclosure;

b. The factors affecting the precision of the review, including the objective of the review and appropriateness of the expectations, level of aggregation, and criteria for investigation for identifying potentially material misstatements;

c. The steps involved in identifying, investigating, and resolving significant differences from expectations;

d. The person(s) who performs the control including the competence and authority of the person(s);

f. The frequency of performance of the control, that is, whether the review occurs often enough to prevent or detect material misstatements before they have a material effect on the financial statements; and

f. The information used in the review, for example, whether the review uses system-generated data or reports, as discussed later in this alert.

The evaluation of design may be performed in conjunction with obtaining an understanding of internal control over financial reporting and performing procedures to achieve the objectives of paragraph 34 of Auditing Standard No. 5. For example, to assess whether a control is effectively designed, it is important to identify the risk of material misstatement to the relevant assertion of the significant account or disclosure that the control is intended to address. 

[7.2.260] When misstatements are identified during the audit, there is an implication on controls that were intended to addresses risks in the area of the financial statements the misstatement occurred. The review control that failed to prevent, or detect and correct, the misstatement cannot be more precise than the size of the misstatement itself as the known misstatement went undetected. Many times, the potential misstatement is higher, and often significantly higher, than the known misstatement. This should be taken into account when evaluating precision of an MRC. Additional guidance on assessing the severity of a control deficiency is included in Chapter 11, Identifying and Evaluating Deficiencies. 

[7.2.270] Generally, the more frequently a control is executed, the greater the level of precision with which the control would be expected to be designed.

For example, in the case of a CFO’s review of the completeness, existence and accuracy of marketing expenses which operates just once at the end of the year, it may be appropriate to set the precision of that review equal to the risk tolerance established for the marketing expense account because the maximum error in the marketing expenses that the control might “miss,” if effectively designed and executed, would be limited to the risk tolerance. 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 may have been more appropriate for the CFO’s quarterly review to involve a level of precision that is one quarter of the established risk tolerance.
There are some MRCs that are designed to be a complete reperformance of the related activity. For example, an entity may have a process (separate from the control!) whereby a department determines the projected financial information (PFI) to be used in the valuation of an intangible asset, and a control (separate from the process!) in which the control operator reviews all of the assumptions and decisions made by those who initially determined the PFI. In such situations, the review control is designed to appropriately reevaluate all assumptions and decisions. The criteria used in the operation of the control are the same as those used in the process of determining the PFI.

MRCs designed to be a complete reperformance of the related activity are difficult to evaluate as to their design and operating effectiveness. Management and external auditors should coordinate closely ahead of the execution of these controls to determine what sort of evidence of the controls’ design and execution can be maintained and provided for purposes of the ICOFR assessment and external audit.

Considerations of External and Internal Factors

It is important to consider how external and internal factors influence the design and operating effectiveness of the MRC. Often with MRCs, the assertions being addressed relate to significant estimates. Those estimates, in order to be stated in accordance with GAAP, need to take into account changes to the business, industry or environment. Principle 9 of the COSO Framework says that “early warning systems” should be in place to identify information signaling new risks that can have a significant impact on the entity. Therefore, an appropriately designed system of ICOFR includes a risk assessment control or controls to identify changes in various external and internal factors and assess the effect those changes may have on the entity and its ICOFR, particularly the controls around estimates.

Illustration 7.9:
How internal and external factors influence the design and operating effectiveness of MRCs

The controller’s review of the allowance for doubtful accounts to ascertain its appropriate valuation is a relevant MRC. The entity significantly increased its sales in a geographic region where the risk of not collecting receivables is significantly greater than in regions where the entity traditionally has operated. As part of evaluating the MRC, consider whether the MRC itself or other controls would identify the effect this operational risk has on the valuation assertion related to the allowance for doubtful accounts and respond accordingly.

Controls over Management Bias

For controls related to significant estimates and other areas of judgment, it is important to consider how they address management bias.
Considerations of management’s bias for MRCs in Category 3

An entity may have to make many significant accounting estimates in the process of producing financial statements. The greater the inherent uncertainty in those estimates, the more important it is that there are controls over management bias in the estimates. Such controls may include analysis and review of current estimates compared to historical estimates, including not just whether the estimates fall within a reasonable range but also whether they consistently fall within the same portion of the range. Depending on the level of uncertainty and the significance of the risk, the control may include oversight of such analysis by the audit committee or others charged with governance.

For example, one entity has many estimates. The audit committee receives an analysis of each estimate, including the range of reasonableness of each estimate, how that range was determined, how the range compares to prior periods, and where within the range management’s estimate fell this period compared to prior periods. It also receives an analysis of how the estimates as a whole impacted earnings.

In this case, the review of each estimate by the audit committee serves as a control designed to mitigate the risk of management bias in the estimates. Bias may be evident in changes made by management to how the range of reasonable results is determined, where within that range (at the lower end, in the middle, or at the higher end) the estimate developed by management falls and how that relative placement of the point estimate changed period over period.

18 COSO Framework, p. 79
Key takeaways:

Test of Design

1. Remember: a properly designed MRC includes establishing **criteria for investigation (as well as related controls over that criteria)** to determine how the control is intended to operate and at what precision.

2. Consider whether **the criteria appropriately address the objective of the control**, whether there is **additional information** that the control operator should consider, and whether the **definition of outliers is appropriate**.

3. Consider **precision in terms of the risk tolerance** established for the related account or disclosure. Precision of an individual control should be **set at an appropriately low level** such that potential misstatements that might result from the operation of all controls across the organization, or multiple smaller misstatements that might go undetected by the control, would not aggregate to a material misstatement of the entity’s financial statements, after factoring in the inherent probability of an error occurring.

4. Consider whether the **design of the control** was or should have been **impacted by external and internal factors**.

5. Particularly for MRCs in category 3, consider whether management’s review control appropriately **responds to the potential for bias** and whether there are other controls that mitigate the risk of management bias inherent in the execution of the MRC.

6. **Complete the Design of a Review Control by Management template** (Appendix 7.1) to document in detail the design of each MRC in category 2 and 3.
The COSO Framework stresses the importance of having controls over the completeness and accuracy (C&A) of information used to support other components of internal control. In the COSO Framework, one of the five components essential to an effective system of internal controls is Information and Communication. The COSO Framework states:

“The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.”

The COSO Framework emphasizes that:

“Maintaining quality of information is necessary to an effective internal control system, particularly with today’s volume of data and dependence on sophisticated, automated information systems. The ability to generate quality information begins with the data sourced. Inaccurate or incomplete data, and the information derived from such data, could result in potentially erroneous judgments, estimates, or other management decisions.

“The quality of information depends on whether it is:

- Accessible – The information is easy to obtain by those who need it. Users know what information is available and where in the information system the information is accessible.
- Correct – The underlying data is accurate and complete. Information systems include validation checks that address accuracy and completeness, including necessary exception resolution procedures.
- Current – The data gathered is from current sources and is gathered at the frequency needed.
- Protected – Access to sensitive information is restricted to authorized personnel. Data categorization (e.g., confidential and top secret) supports information protection.
- Retained – Information is available over an extended period of time to support inquiries and inspections by external parties.
- Sufficient – There is enough information at the right level of detail relevant to information requirements. Extraneous data is eliminated to avoid inefficiency, misuse, or misinterpretation.
- Timely – The information is available from the information system when needed. Timely information helps with early identification of events, trends, and issues.
- Valid – Information is obtained from authorized sources, gathered according to prescribed procedures, and represents events that actually occurred.
- Verifiable – Information is supported by evidence from the source. Management established information management policies with clear responsibility and accountability for the quality of information.”

17 COSO Framework, p. 111
In summary, the COSO Framework requires management to design, implement and operate effective controls over the completeness and accuracy of information produced by the entity (IPE) that is used to operate controls. This is particularly important for management review controls which, by their nature, include representatives of management or another employee reviewing information contained in underlying documents, reports or other information produced by the entity. The effectiveness of management review controls depends to a large extent on the quality of the information being reviewed.

Illustration 7.11:
Reliance of an MRC on IPE

Scenario:
The controller reviews a listing of securities whose period-end prices have been determined “in-house” (the “manually priced securities report”) and captured in the investment management system to facilitate the period-end financial close process. The controller verifies the reasonableness of each security’s pricing by comparing it to supporting documentation. The controller then investigates any differences between the price per the manually priced securities report and the applicable supporting documentation of 3 percent or more.

In this control, there are two distinct pieces of IPE that the controller relies upon in his review. The first is represented by the manually priced securities report generated from the investment management system. The second relates to the “supporting documentation” against which the controller verifies the pricing of securities. If the objective of the controller’s review is defined as the appropriate valuation of the manually priced securities, the effectiveness of the control in achieving that objective is dependent on the following key considerations:

- Independence of the pricing information on the manually priced securities report from the applicable “supporting documentation;” without the independence of the two sets of data, the control would only address the accuracy (not proper valuation) of the pricing information reflected in the investment management system against the supporting documentation and would likely be a simple process-level control.

- Completeness and accuracy of the information in the manually priced securities report as well as in the supporting documentation. The entity should have controls in place to ensure the C&A of both pieces of IPE used in the execution of the MRC. That includes C&A controls over the listing of securities from the investment management system and over any calculations embedded in the supporting documentation, data used in these calculations and appropriateness of methodology underlying the calculations. These controls may be either manual or automated in nature and may include MRCs separate from the review control performed by the controller, as described above.
Identifying Relevant Data Elements

IPE is generally in the form of financial or nonfinancial information presented in reports used by management in the operation of the MRC. When considering the completeness and accuracy of information used in the operation of an MRC, the evaluator is not necessarily concerned about the report as a whole, but rather is interested in the individual relevant data elements.
Illustration 7.12:
What data elements are considered relevant to the design and operating effectiveness of MRCs?

Relevant data elements include all data elements that are important to the operation of the control.

— For example, within a report about the allowance for loan and lease losses, there may be data that, if incomplete or inaccurate, may lead management to make an incorrect assessment. That data may include items such as loan grade, collateral type, last payment date, and loan type. If the report contains data elements irrelevant to the operation of the control such as information about credit card products currently being used by the borrower, there is no need to identify and evaluate controls over those items.

— Likewise, within a report about the warranty accrual for an auto manufacturer, relevant data elements may include vehicle type, repair rates, and warranty period. But the report also may contain data not important to the operation of the control and ultimately the assertion being tested, such as demographic information about the individual car owner, and there would be no need to identify and evaluate controls over those items.

— Similarly, within the documentation supporting valuation of manually priced securities, there may be data elements which are key to the proper valuation of these securities, such as quoted prices for similar assets in active markets, applicable interest rates or yield curves, relevant volatility or credit spread information. On the other hand, the supporting documentation may include other data elements which are not relevant to the valuation of the subject-matter securities, such as information about the major holders of these securities, and there would be no need to identify and evaluate controls over the completeness and accuracy of such data.

[7.3.50] When evaluating the design and operating effectiveness of an MRC, also consider whether the IPE that the control operator uses in the execution of the MRC is the most relevant data available. In other words, determine what information is used by the control operator and what elements of the IPE are relevant to the MRC before identifying and testing controls over the completeness and accuracy of that IPE.

[7.3.60] Because of the importance of financial and nonfinancial information to the operation of an MRC, failure to demonstrate the appropriate design and effective operation of controls over the completeness and accuracy of the information used by the MRC generally renders the MRC ineffective. Those controls can be either manual or automated in nature. However, with today’s volume of data and dependence on information technology systems, controls over the C&A of IPE are often automated.
Understanding the Flow of Each Data Element

[7.3.70] Understanding how each relevant data element flows through the financial information system to the final report which is then used in the operation of a control is a critical first step in evaluating controls over the completeness and accuracy of IPE. **It is insufficient to focus only on the controls over the generation of the report without understanding the source of the data elements and the risks (WCGWs) to which the data elements have been exposed during their flow through the financial information system.** This is because generating the report only addresses the completeness and accuracy of the data going from the system to the report. It does not address the completeness and accuracy of the data elements from initiation and through the system before they are accumulated and presented in the report. Additionally, this does not address the completeness and accuracy of the data elements (or the report itself) after the report has been generated if subjected to further manipulation (e.g., a report is imported into a spreadsheet that is subject to modification before it is utilized in the execution of a control).

[7.3.80] Often, the understanding obtained about the flow of transactions through the process is a good starting point for determining the flow of each data element, from initiation to inclusion in the report. In fact, the flow of some of the data elements may be partially or wholly consistent with the flow of the related transactions.

**Obtaining an understanding of the flow of transactions for each relevant data element**

Determine the flow of each relevant data element, from initiation to inclusion in the report, the related WCGWs and relevant controls by performing the following:

— Obtain an understanding of how the relevant data elements are initiated, processed, generated, extracted, and manipulated as part of the IPE used in the MRC;
— Identify the relevant WCGWs regarding the completeness and accuracy of the relevant data elements in the IPE; and
— Identify and evaluate controls to address the WCGWs.

Evaluating the Controls over the Generation of the Report

[7.3.90] The ability to rely on controls over the completeness and accuracy of IPE generated from an IT system depends on the results of the evaluation of relevant application controls and general information technology controls (GITCs) that support those application controls. Because it is important for IPE to be complete and accurate, and because an MRC uses the IPE to operate the control, ineffective GITCs that support the automated controls over the C&A of IPE generally also render the MRC ineffective.

[7.3.100] How often should controls over the completeness and accuracy of the IPE be tested? In many situations, management takes the view that its IT system produces canned reports and that the underlying source code has not been modified since the IT system was implemented. Consequently, the amount of testing over the completeness and accuracy of the IPE may be very limited in timing and scope. This may be the case when management asserts that:

— It has system application controls over the completeness and accuracy of its system-generated reports (example WCGW – report pulls incomplete or inaccurate data);
— Those application controls were tested at one point and determined to be operating effectively (e.g., when the system was first implemented);

— GITCs such as change management controls are operating effectively and provide management with evidence that the system-generated reports continue to produce complete and accurate information (example WCGW – unauthorized or incorrect change made to a report); and

— It has process level controls over the input of the relevant data elements within the report.

Collectively, these represent management’s controls over the IPE.

[7.3.110] However, established information systems and related controls (including automated application controls and the GITCs supporting those controls) rarely remain unchanged for extended periods of time. Therefore, Principle 16 of the COSO Framework requires that management consider the rate of change in the entity’s business processes and periodically reestablish baseline understanding of the design and current state of internal controls (Example WCGW – change that should be made to a report was not made). This is consistent with the benchmarking strategy often employed by external auditors to test IT application controls. Under that strategy, the evaluator may conclude that the automated application control continues to be effective without repeating the prior year’s specific tests in every assessment period. However, the specific tests are reperformed on a periodic basis to reestablish the baseline understanding of the automated application control. This strategy is appropriate provided the relevant GITCs are effective and the evaluator has obtained sufficient evidence that the automated application control is unchanged. Ordinarily, the time period between specific tests performed to reestablish the baseline understanding of an automated application control would not exceed three years.

[7.3.120] Distinguishing between risk assessment, management’s controls and management’s assessment (testing) of relevant controls is important. In general, we would expect that management and auditors would both identify similar WCGWs and control activities. However, management and the auditor’s testing approaches may differ. The SEC allows for these differences in testing approaches, including testing of controls over IPE. The SEC’s 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 (SEC’s Management Guidance) states:

— The nature of evidential matter may vary based on the assessed level of ICOFR risk of the underlying controls and other circumstances. Reasonable support for an assessment would include the basis for management’s assessment, including documentation of the methods and procedures it uses to gather and evaluation evidence.

20 SEC Release No. 33-8810 p. 31-32
If management determines that the evidential matter within the company’s books and records is sufficient to provide reasonable support of its assessment, it may determine that it is not necessary to separately maintain copies of the evidence it evaluates. However, in these instances management should consider whether reasonable support for its assessment would include documentation of how its interaction provided it with sufficient evidence.

Further, in determining the nature of supporting evidential matter, management should also consider the degree of complexity of the control, the level of judgment required to operate the control, and the risk of misstatement in the financial reporting element that could result in a material misstatement of the financial statements. As these factors increase, management may determine that evidential matter supporting the assessment should be separately maintained.

[7.3.130] In smaller companies, for example, management’s daily interaction with its controls may provide it with sufficient knowledge about their operation to evaluate the operation of ICOFR. Knowledge from daily interaction with the controls provides information obtained by on-going direct involvement with and direct supervision of the execution of the control that may allow the control operator to determine whether there is a material issue with the completeness or accuracy of the information.21 This type of familiarity with the information does not extend to the auditor, who might apply audit procedures to the account once a year.

[7.3.135] Conversely, daily interaction in companies with multiple management reporting layers or operating segments would generally not provide sufficient evidence because those responsible for assessing the effectiveness of ICOFR would not ordinarily be sufficiently knowledgeable about the operation of the controls. In these situations, management would ordinarily utilize direct testing or ongoing monitoring-type evaluation procedures to obtain reasonable support for the assessment.

[7.3.140] Regardless of the approach taken by management to assess the effectiveness of ICOFR, management’s documentation under COSO is required to support the assertion that components and relevant principles are present and functioning, and to evidence to external auditors that its system of internal control is properly designed and operating effectively.22

---

21 SEC Release No. 33-8810 p. 30
22 COSO Framework, p. 29-30
Illustration 7.13: Acceptable differences between management’s approach and the auditor’s approach

Background:
The collections manager is responsible for determining the allowance for bad debts. As part of his job, he runs the accounts receivable aging every day to determine which past due accounts require follow up. His knowledge of past due accounts and historical write offs are the basis for his determination of the allowance.

The controller is the control operator and reviews the collection manager’s determination of the allowance. As part of the review, the controller separately runs the accounts receivable aging directly from the system (which constitutes IPE) and reviews it with the collections manager.

In this situation, both management and the auditor are likely to identify the same WCGWs and control activities:

— WCGWs include that the manner in which the accounts receivable aging is configured to run will not yield a complete or accurate accounts receivable aging. [For purposes of this example, assume that the entity has appropriate controls and testing approach relative to WCGWs around the input of relevant data elements into the system.]

The relevant controls to address WCGWs associated with C&A of the accounts receivable aging include the configuration of the report and the related GITCs. Both management and the auditors identify these as relevant controls. The following scenarios present different testing strategies for purposes of evaluating the effectiveness of the controls around C&A.

Scenario 1:
Facts:

— the allowance is 1/3 of materiality, and it has been approximately 1/3 of materiality for the past several years
— the balance of the allowance account has remained consistent in recent periods
— there have been no identified deteriorations in the business environment that might cause a change in the collectability of receivables
— general IT access and change controls are effective
Management testing approach:
Management may determine that the combination of the GITC testing and the testing of the manual review control may provide them sufficient evidence that the report is still configured appropriately. That is because the general change and access controls are effective and the fact that part of the control requires the control operator to discuss the A/R aging with the collections manager. If the accounts receivable aging used by the control operator in the review was incomplete or inaccurate, it would be detected in discussions with the collections manager who runs an accounts receivable aging every day and calls customers constantly (note also that both the collections manager and the controller, as part of this control, agree the listing of totals to the general ledger to address completeness). If the accounts receivable aging were inappropriately configured, the collections manager would know because he would be calling debtors for collection and they would indicate that it is not past due, and/or he would notice significant shifts between categories. Management determined this test approach provides sufficient evidence to conclude that the configuration is appropriate.

Auditor testing approach:
Given the facts in this scenario, the auditor may determine that management’s testing approach is appropriate to provide the auditors with sufficient evidence as well. As a result, the auditors continue to test the relevant GITCs in conjunction with the overall approach to audit automated controls, but also make sure that as they test the review control, they determine that it is performed and documented in a way that demonstrates the configuration yielded a materially complete and accurate aging. The configuration of the report is not deemed a relevant control to test because the auditor did not identify a risk of material misstatement associated with improper configuration.

Scenario 2:
Same facts as scenario 1, with the following differences:

— The allowance is two times materiality
— There has been significant activity in the allowance, such that the receivables being provided for are largely different quarter to quarter

Management testing approach is the same as in scenario 1.

Auditor testing approach:
The auditor determined that they would need to test the both the system configuration and GITCs to conclude that the configuration is appropriate.
The difference in testing approaches may be appropriate in this circumstance, given all that management knows from its daily interaction with the controls. However, as noted in 7.3.120 above, management should consider whether reasonable support for its assessment would include documentation of how its interaction provided it with sufficient evidence to determine the effectiveness of the relevant controls. As the risk of misstatement increases, the more likely it would be that management’s and the auditor’s testing approaches would be aligned. In other words, as the risk increases, management may have to obtain more evidence that the report is configured appropriately. Further, any difference in approaches between auditor and management does not represent a difference in the identification of the WCGWs or the relevant controls, but simply a difference in testing strategies.

**Scenario 3:**
Same fact pattern as scenario 2, but the control operator does not engage in meaningful conversation with the collections manager and instead relies on his or her own analytical review, which is largely dependent on the accounts receivable aging being complete and accurate.

In such a scenario, management’s approach to testing the configuration will need to include testing both the GITC and the configuration of the report (in addition to testing an additional control around determining that the report used in the review used the correct parameters), because the control does not function in a manner that would allow management to determine whether the accounts receivable aging is complete and accurate.

**Commentary:**
— The key to determining the appropriate testing strategy is to take a step back from the process level WCGWs and determine whether the risk that the report is incomplete or inaccurate, and that such inaccuracies could lead to a material misstatement, has been mitigated. This analysis would include a careful consideration of the nature of the process and the control, as well as the risk of a material misstatement at the assertion level. If the allowance for bad debt fluctuates considerably and/or is a multiple of materiality, it is more likely that a separate control would need to be identified and tested to mitigate the risk of material misstatement, and the reliance on daily interaction would be inappropriate. It is essential that management and auditors each document their testing approaches, considering the specific WCGWs, the controls designed to address these risks, and how the testing approach presents sufficient evidence to conclude on effectiveness.

[7.3.150] Benchmarking may be an effective strategy for management to periodically verify the accuracy of assertions made with reference to controls over the completeness and accuracy of information used in their review controls, as listed in paragraph 7.3.90 above. It is also consistent with the above-referenced requirements of Principle 16 of the COSO Framework. However, this strategy is generally appropriate provided that management has designed, implemented, and evaluated relevant GITCs and found them to be effective, and provided that management has obtained sufficient evidence that the automated application control is unchanged.
When employing a benchmarking strategy, consider the following:

— On a periodic basis (considering the assessed risk and the rate of change in the related business process), the baseline of an automated application control operation should be reestablished; and

— Obtaining evidence to demonstrate that a baseline approach is acceptable is often more cumbersome than testing the specific controls supporting completeness and accuracy.

Regardless of the testing strategy employed by management, the specific WCGWs and controls should be appropriately identified and tested by both management and the auditors. If the testing strategy of management and the auditors differs, both parties consider whether management’s approach is reasonable under the circumstances. If management’s approach is not appropriate, but the auditors test the controls and find them to be operating effectively, there is still likely a deficiency in the monitoring component of COSO.

Evaluating Controls Associated with the Generation of a Report

When a report or other information is downloaded from the entity’s IT system and subjected to further refinement or manipulation, including exporting information into Excel, the information has the potential to be altered. In these circumstances, management should have appropriate controls over the completeness and accuracy of the refined or manipulated information. Protecting the spreadsheet via a password or similar measures may be important, depending on the process, but it is not sufficient in and of itself and also does not provide sufficient evidence of controls over the further refinement or manipulation. Management should have controls over the integrity of the data that are commensurate with the risk.

Considering the Impact That Deficiencies in Controls over Completeness and Accuracy of the IPE Have on the MRC

When controls over the completeness and accuracy of IPE are deficient, the evaluator of an MRC should consider the impact of those deficiencies on the evaluated MRC. There may be either manual or automated compensating controls that mitigate the effect of the deficiency. However, exercise caution when assessing the compensating effect. Manual controls often are not designed to fully address deficiencies in the application control related to the C&A of the information. Therefore, caution should be exercised when attempting to rely on manual compensating controls over the C&A of IPE. It also is necessary to obtain persuasive evidence to support the assertion that such manual compensating controls would detect information that is not materially complete and accurate.
Key takeaways:

Information Produced by the Entity that is used in Management Review Controls

1. Evaluate the design and operating effectiveness of the controls over the completeness and accuracy of IPE used in the operation of the control as required by the COSO Framework and SEC guidance.

2. Determine the flow of each relevant data element (from initiation to inclusion in the report), identify the related WCGWs (including risks over data integrity, report extraction and the potential for manipulation of data), and test the related controls over completeness and accuracy of IPE (including relevant application controls and GITCs).

3. Remember: Failure to have effective controls over the completeness and accuracy of the IPE generally renders the MRC ineffective.

4. Remember: Ineffective GITCs generally render the MRC ineffective.
In evaluating the operating effectiveness of a management review control, the same concepts discussed in section 7.2 with respect to the design of the control apply. When evaluating the design, it is necessary to determine if the control is designed to prevent or detect and correct a material misstatement. When evaluating the operating effectiveness, it is necessary to consider all of the same concepts about design and determine whether the control was executed in a manner consistent with its design. As mentioned in paragraph 7.2.100, KPMG has developed the Review Control Execution Documentation template (included in Appendix 7.2 to this chapter of the ICOFR Reference Guide) which is designed to facilitate documentation of the control operator’s consistent execution of each MRC in category 2 and 3 in accordance with its documented design. The control operator should document the operation of each MRC in category 2 and 3 to enable subsequent evaluation of the operating effectiveness of the control both by management (represented, for example, by internal auditors or others under the direction of management) and external auditors. Internal auditors or others working under the direction of management use the Evaluation of a Review Control by Management template (included in Appendix 7.3 to this chapter of the ICOFR Reference Guide) to document their assessment of the design and consistent execution of MRCs in category 2 and 3 and to evaluate the adequacy of documentation assembled by the control operator to support the appropriate design and operating effectiveness of the MRCs.

The PCAOB provided the following guidance when testing the operating effectiveness of MRCs:

“Auditing Standard No. 5 provides that the auditor should test the operating effectiveness of a control by determining whether the control is operating as designed and whether the person performing the control has the necessary authority and competence to perform the control effectively. The auditing standard also provides that the evidence necessary to persuade the auditor that a control is effective depends upon the risk associated with the control.

Testing the operating effectiveness of a management review control involves performing procedures to evaluate whether the control is working as designed to prevent or detect potentially material misstatements. Testing typically involves, for selected operations of the control, obtaining and evaluating evidence about:

a. The steps performed to identify and investigate significant differences; and

b. The conclusions reached in the reviewer’s investigation, including whether potential misstatements were appropriately investigated and whether corrective actions were taken as needed.

The nature, timing, and extent of testing should be commensurate with the risk associated with the controls. Higher risk controls warrant more testing.

The auditor also should take into account other relevant evidence in the audit when evaluating the effectiveness of a control, such as identified misstatements that were not prevented or detected by the control.”

21 PCAOB Staff Audit Practice Alert No. 11, Considerations for Audits of Internal Control Over Financial Reporting (October 2013), page 23.
Management and external auditors are reminded that according to the auditing standards, the effectiveness of a control (including management review controls) cannot be inferred from the absence of misstatements detected by substantive audit procedures. In an audit of internal control over financial reporting, separate evaluation of the operating effectiveness of each relevant control is necessary regardless of the results of substantive testwork performed on the account or disclosure addressed by the control.

There are a few additional items to consider when evaluating the operating effectiveness of MRCs, and they are addressed in this section.

The Importance of Identifying Outliers

It is important that an MRC, when operated in accordance with its design, identifies outliers. Without outliers, it is difficult to obtain evidence that shows the MRC is designed and operating effectively. Remember, an MRC (particularly one in category 2 or 3) is a control that requires judgment in its performance and, therefore, outliers are likely to be identified during the performance of the control. How these outliers are addressed can demonstrate if the design of the control is sufficient and if the control operator is using appropriate judgment in the operation of the control.

When an MRC (particularly one in category 2 or 3) is performed and reveals no outliers, this may suggest that the MRC is not operating with sufficient precision, or that the MRC is acting as a monitoring control. In that case, the evaluation may need to focus on the process-level controls because they provide the primary source of ICOFR evidence for the related account or disclosure.

On the other hand, when an MRC is performed and reveals a large number of outliers, this may suggest that other controls in the process are either missing or are inappropriately designed, or are not operating effectively. This might put undue pressure on the MRC and compromise its effectiveness, for example by affecting the diligence with which the numerous identified outliers are followed up on and resolved.

What Constitutes an Outlier and How to Test for Outliers

An outlier is an item that falls outside the criteria for investigation established for the review. An outlier may occur frequently or infrequently depending on the nature of the control.

Outliers are not necessarily misstatements, but outliers are a necessary part of supporting the precision of the control and showing that it operates effectively, as designed. However, if a misstatement is identified as a result of following up on and investigating an outlier, we consider whether the misstatement may be indicative of other issues in the subject matter of the review control, including in items that did not meet the originally defined criteria used by the MRC to identify outliers.

The number of outliers required to conclude on the operating effectiveness of an MRC is a matter of judgment, but is influenced by, among other things, the sufficiency of evidence obtained from process-level controls and the degree of judgment involved in the control. However, in general, identifying one outlier may not be sufficient. When an MRC addresses relevant assertions for multiple significant accounts, generally the control should identify outliers for each relevant assertion.
Management has a significant securities investment portfolio consisting primarily of Level 1 and Level 2 securities. Management performs an MRC related to the valuation of investment securities. Part of the MRC includes management investigating any of the prices provided by two independent third-party service providers that vary by 2 percent (i.e., the threshold is to review any variance greater than 2 percent and an outlier is anything that falls outside of that threshold).

There are several items to consider. For example, what does history indicate is a normal variation between the prices of the two service providers?

- For Level 1 securities, the differences are likely to be nonexistent. The 2 percent threshold, then, is not likely to produce any outliers, and given the relatively high threshold compared to the expectation, this indicates that the threshold is not appropriate for Level 1 securities.

- For Level 2 securities, variation between the third-party service providers may vary considerably by type of instrument. The number of outliers at the 2 percent threshold is such that for some types of securities, many of them would exceed the 2 percent and for other types of securities, none of them would exceed the 2 percent threshold. This indicates that a 2 percent threshold across all types of securities is not appropriate.

The appropriateness of thresholds and the number of outliers they identify also may change over time in response to changes in various external and internal factors. The 2 percent threshold may appear high and identify no outliers for certain highly liquid securities at a time when securities markets are stable and predictable. However, at times of significant market uncertainty, the same 2 percent threshold may become too narrow and identify a number of outliers that is unreasonable considering the inherent uncertainty embedded in the valuation of securities which should be well understood by the users of the entity’s financial statements.

There is no specified way to determine whether the number of outliers provides sufficient evidence or indicates that the threshold is appropriate. The determination may depend on careful evaluation of the design of the metrics, thresholds and other criteria used in the execution of the control as well as the resolution of the identified outliers:

- If the prices from both third-party pricing services are the same for all Level 1 securities, there are no outliers. This does not mean that the MRC is ineffective because little to no differences is expected in the estimated prices.

- If there are only two outliers related to a particular type of security classified as Level 2, that may or may not provide sufficient evidence.
  - When both of the outliers were investigated, an adjustment needed to be made, and there are several more similar securities whose price variations are just below the threshold used to identify outliers. In this case, the threshold may need to be adjusted downward.
If neither outlier resulted in an adjustment and the remaining similar securities did not have variances close to the threshold, two outliers may be sufficient.

For situations in between these two examples, judgment is used to determine whether the control is operating at a sufficient level of precision to detect or prevent a material misstatement.

As stated in paragraph 7.2.180, given the dynamic nature of the environment in which companies operate, management should have controls in place to monitor the continuing appropriateness of the criteria for investigation used in the execution of management review controls. These controls should include periodic reevaluation of the degree of uncertainty inherent in the subject matter of the MRC, especially when it comes to significant accounting estimates. The changing number of outliers identified by an MRC from period to period may be an indicator of the need for an adjustment to the design of the MRC.

Techniques used to evaluate the operating effectiveness of MRCs

To determine whether an MRC is operating effectively (and possibly identify outliers), one of the following two evaluation strategies (or a combination of the strategies) may be applied: (1) Reperform the control, and (2) Perform inquiry and inspection or observation procedures.

— **Reperformance** may include using the control operator’s metrics, thresholds, or criteria independently to identify outliers or exceptions and then evaluating the control operator’s follow-up on these items. Whenever we reperform a control, there should still be sufficient documentary evidence showing that the control was in fact performed. This relates in particular to the evidence of follow-up actions taken by the control operator and the operator’s resolution of all identified outliers.

— **Inquiry** may include asking the person responsible for performing the control to determine what they look for when performing it and what actions they take to address exceptions. It may also involve 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. Whenever inquiry is used, it should not be used as the sole procedure.

— **Inspection** may include inspecting documents used by the operator in performing the control to obtain evidence to corroborate those inquiries, and evaluate the effectiveness of the control as implemented by the control operator.

— **Observation** refers to looking at a process or procedure being performed by others, for example, observation of key meetings, or the performance of control activities.
Key takeaways:

Other considerations when Testing the Design and Operating Effectiveness of MRCs

1. **Without outliers, it is difficult to obtain audit evidence** that the MRC is designed and operating effectively.

2. When an MRC is performed and **there are no outliers, this may suggest that the MRC is not designed with sufficient precision**, or that the MRC is a monitoring control and the evaluation should focus on the process-level controls because those controls provide the primary source of ICOFR evidence for the related account or disclosure.

3. An outlier may occur frequently or infrequently depending on the nature of the control. **Outliers do not have to lead to misstatements**, but they are a necessary component in assessing the precision of the control.

4. When an MRC addresses multiple relevant assertions for one or more significant accounts, generally **outliers should be identified for each relevant assertion**.

5. **Complete the Review Control Execution Documentation template** (Appendix 7.2) each time an MRC in category 2 and 3 is performed to document the consistent execution of the control in accordance with its design and facilitate subsequent evaluation of the control’s operating effectiveness by management and external auditors.

6. Evaluation of the design and operating effectiveness of category 2 and 3 MRCs requires more evidence than simply observing a signature and asking questions. The persuasiveness of the evidence should be **commensurate with the risk addressed** by the MRC. The evaluator **places himself in the position of the control operator**, and obtains sufficient, appropriate evidence regarding the MRC’s effectiveness in both detecting and resolving outliers based on the control’s design. **Complete the Evaluation of a Review Control by Management template** (Appendix 7.3) to document evaluation of the operating effectiveness of each MRC in category 2 and 3.

7. When assessing the operating effectiveness of a management review control, the evaluator should verify that **all the outliers or exceptions that should have been identified were, in fact, identified by the control operator**. The evaluator should also ensure that all the outliers or exceptions were adequately followed up on and resolved.
Chapter 8
Understanding and responding to information technology (IT) risks
In an ever-evolving technologically driven business environment, recognition of the important relationship between automated control activities and Chapter 8: Understanding and Responding to Information Technology (IT) Risks is an essential consideration for any properly designed system of ICOFR.

As described in Chapters 5 – Risk Assessment—Understanding WCGWs and 6 – Control Activities, a proper risk assessment includes understanding business processes, how IT affects the entity’s flow of information, and where those risks are likely to manifest themselves in the form of misstatements. Many of the What Could Go Wrongs (WCGWs) identified during risk assessment relate to IT, and therefore the control activities selected to address those IT-related WCGWs are automated or have an automated component (referred to hereafter as process-level “automated” or “application” controls, regardless of whether they are fully automated or the automation is only part of the control). COSO requires that entities evaluate the design, implementation and effectiveness of general IT controls relevant to the effective operation of the process level automated control activities. These General IT Controls, referred to hereafter as GITCs, may relate to many application controls, IT applications and apply to mainframes, client server systems, file servers or a combination thereof.

Many organizations approach the design and testing of GITCs without consideration of the relevant process-level automated controls. In general, this approach is not consistent with the requirements of Principle #11 of the COSO Framework. The design and operating effectiveness of GITCs should only be considered for those GITCs (both automated and manual) that support the consistent operation of automated controls (or controls with an automated component). In COSO’s words, a proper determination of which GITCs are relevant starts with understanding “the dependency and linkage between business processes, automated control activities and technology general controls.” Without the linkage between automated controls and GITCs, the likelihood of not selecting the appropriate GITCs to test, or not obtaining sufficient evidence of the effectiveness of relevant GITCs, increases.

This chapter builds upon the concepts described in Chapters 5 and 6 with respect to IT-related WCGWs and the related process-level automated controls. This chapter also focuses on the GITCs that are important to the effective operation of those automated controls. This chapter should be read in conjunction with Chapters 5 and 6 of this Guide.
8.1 IT Considerations in Planning

[8.1.10] This section focuses on obtaining an understanding of the IT environment. It also provides illustrations of how to document that understanding. Subsequent sections of this chapter elaborate upon key concepts related to understanding process-level activities and related WCGWs (including IT risks); what to do when IT risks are identified; and how to identify the process-level automated controls and the relevant GITCs that support their consistent operation. Because of the nature of automated controls, information on IT-related WCGWs and automated control activities is provided in this chapter. WCGWs, Control activities (including IT-related WCGWs and automated controls), and the selection of controls to test are further discussed in Chapters 5 and 6 of this Guide.

[8.1.20] The COSO Framework describes the three principles in Control Activities and relevant IT aspects as follows:

| Principles of the Control Activities Component | 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 procedures that put policies into action. |

[8.1.30] Process-level automated controls (further discussed in section 8.3 and also referred to as simply “automated controls”) are control activities which address Principles 10 and 12 of the COSO Framework. GITCs (further discussed in section 8.4) address Principle 11 and “help ensure that automated controls work properly when first developed and implemented [and] continue to function properly after they are implemented.”1 Management and the auditor are responsible for understanding how the process-level automated controls within a business process are linked to the respective GITCs.

IT Resource Considerations

[8.1.40] An entity’s use of IT has a significant impact on ICOFR. While generally benefiting an entity’s internal control, use of IT also presents risks to the entity’s financial reporting. IT impacts the nature, timing, and extent of effort needed to assess risk, design controls, and monitor the effectiveness of those controls.

[8.1.50] Management should consider whether it has the appropriate IT resources involved in the design of internal controls around IT as well as in the ICOFR assessment. External auditors consider whether management has the right IT resources as part of its evaluation of management’s control environment, as well as whether they (the external auditors) have the right IT resources on their own team as they execute the audit. IT resources are likely needed to assist in:

— Performing relevant IT ICOFR assessment activities;
— Helping understand and document the flow of information through the business processes and IT systems;
— Identifying IT-related WCGWs;
— Designing IT controls;
— Monitoring the effectiveness of IT controls; and
— Evaluating the impact of IT deficiencies.

1 COSO 2013 Framework, p. 97
Illustration 8.1:
Common Question: Do IT resources need to participate in the walk-through?

Answer:
It may be helpful to have IT resources participate in walk-throughs of highly IT-dependent processes. They can help identify WCGWs related to IT and the process-level automated controls that may address them. Identification of relevant WCGWs and automated controls requires a robust understanding of how IT processes and maintains financially relevant information. Relevant WCGWs and automated controls may exist at the database and operating system levels, and may not be readily apparent without IT resource involvement.

A practice to avoid:
The internal and external auditors walk through highly IT-dependent business processes without IT resources. After the walk-through, the auditors ask their respective IT resources to review the results of the walk-through and document the relevant GITCs that support the consistent operation of the identified automated controls. This practice frequently results in failure to identify relevant WCGWs and automated controls because the IT professionals are not involved in the walk-through of the business process and are not, therefore, in a position to comment about whether all relevant WCGWs and automated controls have been identified.
Understanding of the IT Environment

[8.1.60] In order to understand the IT risks and controls at the process level, it is important to understand the operations of the entity, including the entity’s IT environments relevant to the audit. This understanding:

— Begins with an understanding of the flow of information through the financial business process and related IT systems and environments;
— Relates IT to these relevant financial business processes; and
— Identifies the relevant technical components of IT (applications, databases, operating systems, and networks, and relevant IT locations).

[8.1.70] A documented understanding of the entity’s IT environment may take various forms (e.g., narratives and/or IT system diagrams). As part of obtaining an understanding of the entity’s IT environments, or when performing other risk assessment procedures, significant risks or financial statement-level risks related to IT are likely to be identified. Following are example narratives and IT system diagrams:

Illustration 8.2:
Documenting Our Understanding of IT – Multiple Environments

Example: Documenting an understanding of IT
Key elements of understanding of the IT environment:

Daisy Inc. uses Hyperion for financial reporting, Oracle Financials for financial accounting and Oracle HR for HR/payroll. All the applications are hosted in a data center located in Short Hills, NJ. Both the financial accounting and HR/payroll applications are part of a distributed environment as depicted on the following page and supported by the local IT group in Short Hills, NJ. The financial reporting application is running on a Windows environment and is supported by the IT group located in Daisy Inc.’s corporate office in New York, NY.

Daisy Inc. has a standard set of policies and procedures to help ensure that controls over each of the applications have been implemented consistently across the multiple groups supporting the IT environment.

The financial reporting application, Hyperion, was upgraded from Hyperion Enterprise to Hyperion Financial Management (HFM) in February of the current year. This was a major upgrade, which required replacing hardware, converting data, and installing and configuring new servers including upgrading the operating systems to Windows 2003 and upgrading the databases to SQL Server 2000.

The IT environment and its relationship to the accounting activities is shown below at a high level. It is used for planning purposes and is not meant to be a detailed, activity-based flowchart at the process level.
The understanding of the IT environment may be simple enough that one illustration, such as that shown in illustration 8.2, is sufficient. But other IT environments are more complex, and the understanding of various IT layers should be done at the process level. Most process-level flowcharts document only the process activities at the application layer, and perhaps at the database level. But a proper evaluation of ICOFR considers all relevant layers or components of IT, including operating systems, active directories, and networks, that present risks and need to be controlled in order for the application to function properly.

<table>
<thead>
<tr>
<th>Key takeaways:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IT Considerations in Planning</strong></td>
<td></td>
</tr>
<tr>
<td><strong>1. Involve IT resources appropriately.</strong> IT resources are helpful in understanding the IT environment and the source and flow of information and WCGWs in an integrated way. They also help identify relevant IT risks and controls.</td>
<td></td>
</tr>
<tr>
<td><strong>2. Obtain a proper understanding of how IT is used by the entity.</strong> This understanding is the basis for properly identifying IT risks and the controls needed to address those risks.</td>
<td></td>
</tr>
<tr>
<td><strong>3. Be aware of the various layers of IT.</strong> Most process flowcharts depict the activities at the application layer. Understanding the IT environment is critical to understanding risks at all layers of IT.</td>
<td></td>
</tr>
</tbody>
</table>
8.2 Understanding Process-Level Activities and Related Risks

[8.2.10] Chapter 5, Risk Assessment—Understanding WCgWs, discusses the need to understand the flow of the transaction through the process from initiation to reporting. This understanding includes understanding IT-related WCgWs, beginning when data enters a system, the manipulation of data within the system, the movement of data from one system to another, and its transformation from the system to a report.

[8.2.20] Understanding and addressing IT risks is not optional and is not an evaluation that is separate from the risk assessment discussed in Chapter 5. The entity must identify and document the relevant WCgWs in the process at the assertion level where there is a reasonable possibility that these WCgWs could result in or contribute to a material misstatement. This includes the WCgWs related to IT. Failure to sufficiently understand risks including those that arise from the use of IT in a process, is a deficiency that needs to be evaluated for severity and could result in a material weakness.

Illustration 8.3:
Recap of IT-Related Points in Chapter 5

Understanding of the process-level activities includes knowing:
— How specific data elements of interest are captured and flow through the information system to the financial statements;
— How manual and IT processes work to avoid process gaps and address WCgWs;
— Relevant activities within IT systems, not just inputs and outputs; and
— Whether IT system components (such as modules, scripts and report writers) reveal specific risks (i.e., risks within individual system components).

In identifying WCgWs arising from IT:
— Consider the IT-related WCgWs as part of the overall assessment of WCgWs related to financial statement assertions, not as a separate exercise
— Consider the broad set of IT risks that may have a process-level impact at the assertion level, including privileged users, access at the various IT layers, etc.

[8.2.30] Our understanding of the business processes can be documented in a variety of forms (e.g., narratives and/or flow charts). The following examples illustrate how an entity might document its understanding of a business process and identify the related IT WCgWs in the process:
Illustration 8.4:
Identifying IT Risks in Cosmic Car Sales Process

This illustration describes how an inbound EDI transmission from a customer initiates a sales order. **This example only provides excerpts of the process** to stress IT considerations. Other relevant parts of the process are omitted from this example. For a more detailed example of a process flowchart, see the appendices to Chapter 5.

Activities at each circled number:
1. The information in the EDI transmission from the customer is converted to an IDoc suitable for SAP applications. The ORDER IDoc is transferred to a posting program, SAP SD, and a sales order is created with the following information: customer name and address, model, vintage year, options, extended warranty, and shipping address. The information in the ORDERS IDoc for Cosmic Car is compared against the inbound EDI transmission, and the transfer of the information in the IDoc to the sales order document is noted.

2. After the order is created, the sales order amount is compared against the customer’s existing credit limits (calculated by order amount plus outstanding receivables on the customer’s account) to ensure that the sale is within the credit parameters established for that customer.

3. Once the credit limit has been verified, the order is released for fulfillment. The shipping department prepares the car for shipment, and once the car is shipped, an invoice is generated in the system and revenue is recognized.

4. On a weekly basis, the credit supervisor reviews a report of all open receivables greater than 90 days based on invoice due date. The credit supervisor investigates each receivable that is more than 90 days old to check that it is valid and decide what actions need to be taken to collect.

Example IT-related WCGWs identified (For purposes of this example, not all WCGWs and relevant controls have been identified.)
Process-Level WCGWs

- EDI is not configured appropriately such that the customer PO is not appropriately received (inappropriate quantity and/or item);
- The system is not appropriately configured to stop all orders where the credit limit has been exceeded (note that, as is the case with most IT-related WCGWs, there are other WCGWs as well—e.g., approval of credit limits, access to change credit limits, etc.);
- Access to mark a car as shipped is inappropriate;
- Job scheduler is not appropriately configured to record the sales in the appropriate period;
- The report of all open receivables more than 90 days old is incomplete or inaccurate.

Note: This example is continued later in this chapter, as a part of a discussion of process-level automated controls that address the WCGWs, along with the GITCs that support their consistent operation.

[8.2.40] As discussed in Chapter 5, walk-throughs follow information as it flows into, through, and out of relevant IT systems. It is important to trace the financially relevant data through the IT systems—not around them. There is completeness and accuracy risk when data is entered into an IT system, when data is subject to change within the IT system (by aggregation or other calculation), and when data exits the IT system—either to enter another IT system, or as information produced by the entity (IPE) such as a system-generated or management-prepared report.
Key takeaways:

Understanding Processes-Level Activities and Related Risks

1. **Understand process-level activities and risks related to IT.** We should understand how specific data elements are captured, and how those data elements flow through the information system to the financial statements. We also should understand how manual and IT processes work to **avoid process gaps**. IT is an **integral** part of the process and should be considered as part of the overall assessment of risk, not in a separate evaluation. We should consider risks revealed in individual system components (such as modules, scripts and report writers) **not just major applications**.

2. **Involve IT resources appropriately.** IT resources can help us obtain an understanding of process activities—particularly in highly IT-dependent processes—by helping identify relevant WCGWIs and automated controls.
8.3 What are Process-Level Automated Controls and How are They Relevant to ICOFR?

[8.3.10] As discussed in Chapter 6, Control Activities, once relevant WCGWs are identified, control activities are designed and implemented to mitigate those risks. To the extent that the WCGWs are IT-related, the risks are generally mitigated by automated controls.

[8.3.20] Process-level automated controls and GITCs are interrelated, and both are important. Their functions are different, however, and so they need to be considered separately.

[8.3.30] Process-level automated controls, which are described in further detail below, are the process-level controls that are often needed to address WCGWs. GITCs, on the other hand, are the general controls that are needed to “help ensure that automated controls work properly when first developed and implemented [and] continue to function properly after they are implemented.” As previously indicated, both automated controls and GITCs may be fully automated or may be manual controls with an automated component.

[8.3.40] We consider both the process-level automated controls and the related GITCs that support the consistent operation of those automated controls. The SEC Staff stated that, “While IT general controls alone ordinarily do not adequately address financial reporting risks, the proper and consistent operation of automated controls or IT functionality often depends upon effective IT general controls.” We discuss GITCs in more detail in section 8.4.

[8.3.50] This section describes process-level automated controls in detail and provides illustrations of how to select them for testing. Identifying and selecting controls to test is often performed concurrent with identifying the risks discussed in the previous section. Selecting automated controls to test is often more effective and efficient than testing manual controls in an environment with effective GITCs.

[8.3.60] Process-level automated controls may be programmed into software, databases, and other system components to perform business logic on data—i.e., logic that governs the input, processing, integrity, and output of data. Examples of automated controls include:

- System access, including enforcing segregation of duties (SODs);
- Edit checks;
- Exception reports;
- Interface controls; and
- Configuration of system calculations.
Illustration 8.5:  
Identifying Process-Level Automated Controls in Cosmic Car Sales Process

Note: For purposes of this example, process-level automated controls have only been identified for a subset of the WCGWs identified in Illustration 8.3. In Illustration 8.3 (above), the engagement team performed a walk-through of the sales process and identified certain WCGWs related to IT. Two of those WCGWs relate to the system’s check to make sure the order will not exceed the credit limit. Specifically:

— The system is not appropriately configured to stop all orders where the credit limit has been exceeded; or
— Credit limits are changed inappropriately.

Control 1  
*Basic description:* SAP is configured to compare the open receivables from the customer plus the purchase order amount to the credit limit. If the amount exceeds the credit limit, the purchase order is not processed. A report is generated for a customer service representative to contact the customer to discuss options (e.g., apply for an increased credit limit, pay down the outstanding receivable balance, etc.).

Control 2  
*Basic description:* Access to change credit limits is granted only to those in the credit department, and those in the credit department do not have access to create a PO or ship confirm an order.

Control 3  
There is also a manual control with an automated component; namely, that all changes to credit limits are reviewed by the credit supervisor to determine the appropriateness. A report is generated that shows all changes to the credit limits. There need to be controls around the completeness and accuracy of that report.

Illustration 8.6:  
Additional Examples of Process-Level Automated Controls

**Initial capture of data relevant to financial reporting in a system**  
*Example:* Capture of inventory purchases (existence of inventory)

— **System access control** (Relevant WCGW=Those who can enter receipt of inventory are segregated from those who can enter and pay invoices and from those who can add or change POs)

— **Configuration control and exception report related to three-way match** (Relevant WCGW=The system is configured inappropriately such that differences between the PO, inventory received, and the invoice are not flagged for further review)
Key calculations relevant to financial reporting

Example: Calculation of interest income (accuracy of interest income)

— **System access control** (Relevant WCGW=Database access is not restricted and therefore unauthorized updates to the master rate tables is possible).

— **Configuration control and exception report related to rate changes** (Relevant WCGW=Management has a control to review all rate changes to determine that they were authorized. The report to capture all rate changes may be inappropriately configured).

— **Configuration control related to the system calculation of interest income** (Relevant WCGW=the system configuration is inappropriate and does not accurately capture interest income for the period).

The movement of data from one system to another

Example: Nightly transfer of sales transactions data from SAP into the sales data warehouse (completeness, accuracy and existence of sales)

— **Configuration control related to the job scheduler** (Relevant WCGW=the job scheduler is not appropriately configured to capture all relevant data once and only once)

— **Configuration control to ensure that the batch was transferred into data warehouse appropriately** (Relevant WCGW=The system configuration is such that an error code is not generated when it should be (e.g., when the number and dollar amount of sales transactions from the originating file does not equal the same information in the sales data warehouse)

The storage and maintenance of data

Example: The storage of inventory data in Oracle (completeness, accuracy, and existence of inventory)

— **System access control related to database access** (Relevant WCGW=Inappropriate access to the database, which may lead to inappropriate change to data)

System generated reports and other Information Produced by the Entity (IPE)

Example: The generation of an Accounts Receivable aging report (existence of sales and A/R, valuation of A/R)

— **Configuration control related to the job scheduler, which is configured to compare the total balances of the data written to the report to the total balances of the originating file.** (Relevant WCGW=A/R aging report is not complete or accurate)

Note: With respect to controls over reports and other IPE, it is important to consider the controls from the point of initiation through reporting; relevant controls should exist that ensure the completeness and accuracy of the data used as input to the report.
When routine business transactions are subject to highly automated processing with little or no manual intervention, it may be difficult to identify and test manual controls that, by themselves, effectively address WCCWs. Because of the routine nature of the transactions, process-level automated controls that address WCGWs should be tested instead, along with the GITCs that support their consistent operation. If a significant amount of an entity’s information is initiated, authorized, recorded, processed, or reported only in electronic form, consider the following:

- If evidence needed to assess ICOFR is electronic, the sufficiency and appropriateness of that evidence usually depends on the effectiveness of controls over its accuracy and completeness.
- If appropriate automated controls that address these risks are not operating effectively, information may be improperly entered or changed.

In the following sample scenarios, it may be difficult to select and test manual controls that, by themselves, provide sufficient evidence that management’s system of internal control would detect a material misstatement because of the volume of transactions that flow through the system. In these scenarios, process-level automated controls are likely to be needed to appropriately address the WCGWs:

- **Scenario 1:** An entity initiates orders for purchase and delivery of goods using automated processes, based on predetermined rules (e.g., maintaining minimum quantities on-hand). It also pays the related Accounts Payable using automated processes tied to system-generated decisions initiated when goods are delivered and payment terms are determined. The entity produces no manual documentation of any part of these transactions.
- **Scenario 2:** An entity provides services to customers via electronic media. (For example, the entity is an Internet service provider or a telecommunications company.) This entity uses IT to log the services provided, initiate and process its billings, and automatically record these amounts in electronic accounting records that are part of the system used to produce financial statements.
Illustration 8.7:
Common Pitfall: I don’t need to consider process-level automated controls because the entity has strong manual controls.

Scenario:
An online provider of education services uses information system A to manage and deliver course content. Information system A also tracks course start dates and student attendance data that are subsequently transferred to information system B, which uses this information to compute and record revenue. The course start dates and student attendance is critical information to record revenue appropriately.

The company tested a system configuration control related to calculating and recognizing revenue and refunds in information system B, along with relevant GITCs that supported the consistent operation of the system configuration control. The system configuration control and related GITCs were designed and operating effectively.

However, the company determined that it was not necessary to perform testwork related to system A because management reviews revenue in detail both from an operational standpoint and as part of a financial statement review. Observations:

Observations:
— The effective operation of the revenue review control was dependent upon accurate enrollment information that came from system A.
— As discussed in more detail in Chapter 7, Management Review Controls, these types of analytical reviews generally do not operate at a precision that is sufficient to prevent or detect a material misstatement.
— Management should have identified and tested the entity’s controls over the accuracy and completeness of course start date and attendance data generated in information system A that was ultimately used to calculate revenue.
— Management should also have tested controls over the transfer of key data e.g., course start date and attendance data) from information system A to information system B.

Information Produced by the Entity or System-Generated Reports
Management-prepared or system-generated reports are often used in Management Review Controls. This information is commonly referred to as Information Produced by the Entity or IPE. Testing controls over management prepared or system-generated reports does not provide evidence that the information contained within an entity's information system is complete and accurate. Rather, controls over management-prepared or system-generated reports ensure the complete and accurate reporting of the information that resides within an entity’s information system. It is essential that management ensures there are controls over the completeness and accuracy of the IPE. These controls are necessary to ensure the broader process-level controls are operating effectively. Keep in mind, controls over management-prepared or system-generated reports, to the extent automated, should be supported by relevant GITCs. In the case that GITCs are not effective, see the section below, Considerations when a GITC Deficiency is Identified.
1. When relying on a report used by management as part of a control, should controls over the completeness and accuracy (C&A) of the report be tested?

   **Answer:** Yes. When the report is used by management as a basis of a control, we should identify and test controls over C&A of the report. See further discussion on testing C&A of reports included in Chapter 7 of this Guide.

2. When testing Management Review Controls that include use of the report, should controls over C&A of the report be tested?

   **Answer:** Yes. When testing Management Review Controls that make use of a system-generated report, we document and test management’s controls over C&A of the system-generated report. It is also necessary to test the controls over the origination and processing of the data up to the point that a system-generated report is created.

3. If data is imported to a data warehouse or reporting tool used to prepare financial reports, should controls over C&A of the import process be tested?

   **Answer:** Yes. We develop an understanding of the source and flow of information from initiation of the transaction to reporting; we consider the WCGWs, including the risk that relevant financial data may be moved from system to system in an incomplete or inaccurate fashion. An interface control at the point where relevant data enters the data warehouse may address an important WCGW; if so, this control is subject to testing. We consider this along with the other controls addressing the important WCGWs we have identified.
<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. If an application or reporting tool is used to obtain data that will be analyzed to determine a significant estimate (e.g., Loan Loss Reserve), should controls over C&amp;A of that data be tested?</td>
<td>Yes. In addition to testing controls that address risks relevant to incomplete or inaccurate data from initiation of the transaction until it resides in the database, the controls around the generation of the report (to determine that the data is pulled completely and accurately from the database) as well as end-user computing controls need to be tested.</td>
</tr>
<tr>
<td>5. What is an acceptable approach to test controls over C&amp;A of spreadsheets in an end user computing environment?</td>
<td>Often, there are no systematically enforced controls over spreadsheets. In these cases, we treat the spreadsheet as a manually generated report. See discussion below regarding End-User Computing.</td>
</tr>
<tr>
<td>6. When the external auditor uses the work of others, including Internal Audit, should procedures for testing the C&amp;A of a report used by IA, or controls over C&amp;A of reports used in controls tested by IA, be documented?</td>
<td>Yes. Management’s testing of the C&amp;A of relevant data from the reports needs to be documented. Documentation should explain how IA or management tested and how they concluded on the C&amp;A of reports they relied on for their control testing.</td>
</tr>
<tr>
<td>7. Are process-level system access controls over the ability to change parameters of a configured control required to be tested, or can we rely solely on GITC access controls?</td>
<td>GITCs do not directly address the WCGWs related to a relevant assertion. Rather, GITCs are designed to address the ongoing effectiveness of process-level automated controls, which in turn directly address relevant assertions. If the process-level system access controls over the ability to change parameters address the WCGWs related to a relevant assertion, relying solely on a GITC is insufficient.</td>
</tr>
<tr>
<td>8. Are procedures to test the C&amp;A of reports different for reports that are considered &quot;standard&quot; or &quot;canned&quot; reports?</td>
<td>The objectives of testing for C&amp;A are no different for “standard” or “canned” reports. However, the WCGWs may be different. As a result, we may identify different controls for “standard” or “canned” reports from other reports. <strong>Example:</strong> In a report that is hard-coded in a well-known ERP system, a relevant WCGW may be “inappropriate changes to the parameters of the report.”  <strong>Contrasting Example:</strong> In a home-grown system, a relevant WCGW may be “inappropriate changes to the programming code in the report logic.” <strong>Note:</strong> These are illustrations. Management should consider the WCGWs based on their facts and circumstances and then design controls to mitigate the risk of incomplete and inaccurate reports.</td>
</tr>
</tbody>
</table>
**Testing Process-Level Automated Controls**

[8.3.120] To evaluate the design and implementation of an automated control and test its operating effectiveness, we gather evidence to show how the control works, how it addresses the WCGW(s), and whether or not it does so effectively. To properly test the automated control, we must understand its key attributes. These attributes may include:

— The specific data elements used as input into the operation of the control, and where those data elements reside;

— The logic of the control and how it handles various conditions; and

— The implementation of the control in the system (e.g., is it implemented as a set of configurations or as programmed logic?).

[8.3.130] In a typical scenario where an automated control is applied to every transaction, inspecting the IT application system setting (a system query) may be the most appropriate testing technique. To perform this test, it is generally appropriate to use at least one query as a test for each relevant attribute of an automated control. This test assumes that the relevant GITCs have been tested and are operating effectively. In this case, we test the relevant GITCs to confirm that the automated control operated effectively throughout the period subject to audit. See Illustrations 8.8 and 8.9 below.

[8.3.140] In certain instances (e.g., where we can’t use a system query, or additional evidence is needed based on the relative risk the control addresses), we may choose to perform other procedures such as running test data through the system and comparing the results to actual data or to expected results based on established business rules. But be cautious: without understanding the technical aspects of how the system performs a control at a detailed level, this comparison may not sufficiently test the design of the automated control.

[8.3.150] Running insufficient test data through the system can render the testing of a process-level automated control deficient. For example, when testing whether an Accounts Receivable aging report correctly categorizes invoices into appropriate aging categories (i.e., current, and days past due categories of 0-30, 31-60, 61-90, 91-120 and over 120), it would be inappropriate to only select current invoices and test whether these invoices are properly categorized in the “current” aging category. This limited test data would not identify an error in the logic of the automated control whereby more significantly aged invoices were categorized into an incorrect aging category.

[8.3.160] When running test data through the system, select data from the beginning of the process you’re testing, address all significant transaction types, including transactions initiated from multiple sources (e.g., multiple master files, interfaces with other systems), and include unusual data combinations (e.g., negative/zero quantities, excess quantities, and override capabilities).

[8.3.170] The following illustrations 8.8 and 8.9 are examples of effective approaches to testing process-level automated controls. The nature, timing, and extent of procedures performed are determined by the significance of the automated control to the financial statement assertions they address and, therefore, how persuasive the audit evidence needs to be. (The discussion in the next section addresses how we link automated controls to GITCs that support their consistent operation.)
Illustration 8.8:
Example Testing Approaches for Process-Level Automated Controls (excluding the linking and testing of GITCs that support their consistent operation)

Illustration A:
Management and the external auditor identify an automated three-way match control that determines whether to route a purchase-to-pay transaction (e.g., the vendor’s invoice) to the computerized payment process or to the Accounts Payable clerk for further analysis. The automated three-way match control compares the vendor name, the description of the goods, the price, and the quantity of goods received, to the terms of the authorized purchase order, and to the terms of the vendor invoice. If the three quantities and extended prices are within 0.5 percent of each other, the invoice is paid. If the three quantities and extended prices exceed 0.5 percent of each other, the invoice is routed to an Accounts Payable clerk for investigation.

In this circumstance, management and the external auditors need to learn the source of data elements subject to the control, and where data resides in the IT system before they are used by the control. They may also inspect the configuration of the control, noting that the business rules are properly implemented as intended. After obtaining this evidence about the design and implementation, they address whether information routing and comparison is operating effectively. To do so, they select items from the specific data sets used to operate the control and then may reperform the logic for all attributes reflected in the business rules for routing.

Illustration B:
Management and external auditors identify an automated control that passes or fails a transaction based on certain business rules. Specifically, this is an automated control over Accounts Payable where payments up to $10,000 are automatically approved, but payments over $10,000 require authorization by the controller.

In this situation, management and the external auditor inspect the system settings for both a pass and a fail (not just a pass), to determine that the system configuration supports the business rules. Management and the external auditor determine that payments up to $10,000 are automatically approved, and that the system rejects payments over $10,000 unless already authorized by the controller.

Illustration C:
Management and external auditors note that an AR aging report is generated automatically. They inspect the settings over each aging category (e.g. 0-30 days past due, 31-60 days past due, 61-90 days, etc.) to determine that the system is configured to follow the established business rules.
Because IT processing is highly automated, we may obtain evidence about the design appropriateness and effective implementation of a process-level automated control by observing its configuration during a single walk-through. This procedure, as well as other procedures we perform to understand the flow of information through the financial processes and IT systems may provide substantial audit evidence about the operating effectiveness of the automated control. Only inquiring about process-level automated controls does not provide sufficient evidence regarding their operating effectiveness; we combine inquiry with other monitoring/testing procedures such as observation or inspection. As noted later in this chapter, evidence regarding the design and implementation of automated controls should be considered in conjunction with audit evidence that supports the design and operating effectiveness of related GITCs (in particular, change controls and access controls).

**Illustration 8.9:**
Common Question: Which controls do I test first, Automated Controls or GITCs?

**Consider efficiency and risk factors**
Most often, we first test the controls that are most likely to fail. This approach prevents us from wasting time by testing controls we may not be able to rely on.

- For example, if GITC(s) are found to be ineffective and impact the continued operation of the automated controls it supports, we will need to test alternative manual controls that do not rely on the deficient GITC(s). In this case, any testing of automated controls impacted by the GITC deficiency would be unnecessary.

- Conversely, if automated controls are found to be ineffective, then any testing of the GITCs that support the continued operation of those automated controls also would be unnecessary.
Key takeaways:

How are Automated Controls Relevant to the Audit?

1. **Automated controls are important.** Avoid the common pitfall of assuming that you don’t need to test automated controls because the entity has strong manual controls. Verify that automated controls that address the WCGWs related to IT have been identified and tested. Remember that we are often more efficient and effective when we test automated controls.

2. **Test controls over the completeness and accuracy of IPE.**

3. **Plan proper tests of automated controls.** Inquiring about automated controls does not, in itself, provide sufficient audit evidence regarding their operating effectiveness. We combine inquiry with other testing procedures such as observation or inspection. When running test data through the system to test an automated control, ensure the test data is sufficient by covering all transaction types. When performing a system query to test an automated control, make sure the query addresses all attributes of the control.

4. **Manual controls often have an automated component.** It is important to consider whether manual controls have an automated component. For example, the manual review of an AR aging report relies on automated control over generating the AR aging report. We must make sure we test those automated controls.
Identifying, Linking, and Testing GITCs

[8.4.10] Once we have identified the relevant process-level automated controls, we identify GITCs that support them. The COSO Framework highlights the importance of determining the dependency between automated controls and GITCs by including this concept as a point of focus, “Determines Dependency between the Use of Technology in Business Processes and Technology General Controls,” to principle 11.4. In other words, we only test GITCs to the extent that they are important to the design and operation of the relevant automated controls.

[8.4.20] Failure to establish proper linkage between the automated control and the GITC may result in one or more of three problems. First, we may be testing GITCs that aren’t relevant to ICOFR: this is inefficient. Second, we may not identify the GITCs that are truly relevant to ICOFR: this is more likely when an automated control relates to system-generated or management-prepared reports used in the financial reporting process, particularly in Management Review Controls (i.e., GITC testing did not extend to information or applications that generated these reports). Third, we either may not obtain sufficiently persuasive evidence about the functioning of the GITC after considering this linkage and its importance to the audit or, alternatively, we may obtain more persuasive evidence than necessary.

[8.4.30] Included in Appendix 8.1 to this chapter is a working paper, Identification of GITCs – Linking GITCs to Automated Controls, designed to assist in identifying the relevant GITCs for testing. It will help management and auditors link between the automated controls and the relevant GITCs that are important to their effective operation.

Illustration 8.10:
Common Pitfall: What happens when we don’t properly link GITCs to automated controls?

Scenario: GITC deficiency is identified
A provider of benefits management services to the healthcare industry used an information system to house key revenue and rebate applications. Users had unrestricted administrative access to the revenue and rebate applications. In response, compensating process-level controls (including reconciliation controls, automated data processing controls, and Management Review Controls) were identified and tested.

The Management Review Controls operated at a disaggregated level and management’s review identified account fluctuations at a sufficient level to detect a material misstatement (see Chapter 7 or further discussion on designing an appropriate MRC).

Deficiencies in the approach:
There were likely to be automated controls over the completeness and accuracy of information used in the Management Review Control and the relevant process-level system access control(s). If those relevant controls end up being linked to the GITC that was determined to be deficient, management and the auditors would have quickly realized that these controls over the completeness and accuracy of information used in the Management Review Control could not be relied upon. As a result, they would ultimately have determined that the Management Review Control could not be relied upon because of the GITC deficiency.

The parties should have also evaluated the system access by the individuals who performed the various compensating process-level controls to determine that they did not have inappropriate administrative privileges to the revenue and rebate applications.

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 588628
[8.4.40] In order to properly link GITCs to process-level automated controls, it is helpful to understand what they are and how they operate. GITCs maintain the integrity of information and security of data. GITCs are policies and procedures that relate to many IT applications and support the effective functioning of automated controls by helping ensure the effective operation of information systems. GITCs apply to mainframes, client server systems, file servers, or combinations thereof.

[8.4.50] When information-processing functions are outsourced to third parties, the process-level automated controls and GITCs that support their consistent operation are typically described in Service Organization Control (SOC) reports. In some cases, service organizations provide separate SOC reports for the automated controls in their applications and the GITCs that address them. Therefore, you may need to obtain more than one SOC report to understand the full population of GITCs that impact the effective operation of the automated controls, and how those GITCs were tested.

[8.4.60] IT resources may need to be involved in the identification and testing of GITCs important to the effective operation of automated controls. They may need to participate in walk-throughs or similar procedures, and help identify both the relevant automated controls and the related GITCs.

[8.4.70] Identifying access-related GITCs that are important to the effective operation of automated controls can be challenging. Illustrations of how to identify these GITCs are provided in the continuation of the Cosmic Car Illustration:

Illustration 8.11:
Identifying Relevant GITCs in Cosmic Car Sales Process

Note: The GITCs identified here may be incomplete; additional GITCs may be linked to the process-level automated controls based on entity-specific facts and circumstances.

After identifying automated controls in the sales process (illustration 8.5), management and auditors need to identify the relevant GITCs that are needed to make sure each automated control continues to function as intended. This illustration considers the first of the automated controls identified in illustration 8.5:

Control 1
Basic description: The system is configured to compare the open receivables from the customer plus the purchase order amount to the credit limit. If the amount exceeds the credit limit, the purchase order is not processed. A report is generated for a customer service representative to contact the customer to discuss options (e.g., apply for an increased credit limit, pay down the outstanding receivable balance, etc.).

Linked GITCs:
— Provisioning of Access (who has access to make changes to the configuration)
— Configuration Change Control (changes to the configuration are tested and approved prior to implementation)
The following table provides additional GITC considerations and illustrations of linking GITCs to process-level automated controls:

<table>
<thead>
<tr>
<th>Process-Level Automated Controls</th>
<th>Relevant GITCs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Segregation of duties</strong></td>
<td><strong>Example key considerations:</strong></td>
</tr>
<tr>
<td>Access controls prevent</td>
<td>— How does the entity know that users were not granted access inappropriately to perform these functions during the period under audit?</td>
</tr>
<tr>
<td>individuals who have access to</td>
<td>— If a user’s role were to change, and that change would create a violation of the SODs we are relying on, how does the entity know that access would be appropriately revoked?</td>
</tr>
<tr>
<td>update the vendor master file</td>
<td><strong>Potentially relevant GITCs:</strong></td>
</tr>
<tr>
<td>from:</td>
<td>— Controls over user provisioning in Oracle (including how user access is added, modified, and removed; and whether the process varies depending on the type of access request, e.g., privileged user access)</td>
</tr>
<tr>
<td>— Generating purchase orders in</td>
<td>— Controls over periodic review of user access to Oracle (including controls over C&amp;A of the report management uses to perform the review, and controls over handling of user access corrections)</td>
</tr>
<tr>
<td>the Purchasing module</td>
<td>— Controls over privileged user access in Oracle (including restrictions over who can set up, modify, or remove user access)</td>
</tr>
<tr>
<td>— Entering invoices into the</td>
<td></td>
</tr>
<tr>
<td>Accounts Payable module</td>
<td></td>
</tr>
<tr>
<td>— Disbursing funds from Oracle</td>
<td></td>
</tr>
<tr>
<td>Payments</td>
<td></td>
</tr>
<tr>
<td>— (This includes access in all</td>
<td></td>
</tr>
<tr>
<td>layers of technology, such as</td>
<td></td>
</tr>
<tr>
<td>the database and operating system.)</td>
<td></td>
</tr>
</tbody>
</table>

| **Exception report**            | **Example key consideration:** |
| Oracle is configured to perform  | How does the entity know that changes made to program code and configurations during the period did not alter the performance of this control? |
| an automated three-way match    | **Potentially relevant GITCs:** |
| reconciling the purchase order, | — Controls over user access to make changes to the Oracle configuration settings |
| receiving document/report, and  | — Controls over any Oracle configuration changes applicable to the configuration and generation of the report (including the approval, testing, and implementation of those changes) |
| vendor invoice. If the three-way | — Controls over program development, if applicable to the configuration and generation of the report |
| match for the invoice does not  | — Controls over changes to the job scheduler and access to perform such changes, if applicable to the generation of the report |
| reconcile, the exception is     |                                  |
| included on the exception report (e.g., unmatched invoice report), and the appropriate personnel follow-up on that exception. |
### Process-Level Automated Controls

<table>
<thead>
<tr>
<th><strong>System configuration control</strong></th>
<th>Relevant GITCs</th>
</tr>
</thead>
</table>
| Oracle is configured to automatically approve payments up to $10,000, but payments over $10,000 require authorization by the controller. | **Example key consideration:** How does the entity know that changes made to program code and configurations during the period did not alter the performance of this control?  
**Potentially relevant GITCs:**  
- Controls over user access to make changes to the Oracle configuration settings  
- Controls over any Oracle configuration changes applicable to the implementation of the control (including approval, testing, and implementation of these changes)  
- Controls over program development, if applicable to the implementation of the control |

<table>
<thead>
<tr>
<th><strong>Interface control</strong></th>
<th>Relevant GITCs</th>
</tr>
</thead>
</table>
| Vendor information is transferred nightly from the Jupiter application to Oracle A/P via an automated interface. Oracle A/P is configured to compare the header file record count against the actual records in the file to ensure that the data is transferred completely and accurately. (Control attributes may include the sequencing of the job, monitoring for completion, and resolution if the job does not run normally.) | **Example key consideration:** How does the entity know that changes made to program code and configurations during the period did not alter the performance of this control?  
**Potentially relevant GITCs:**  
- Controls over user access to make changes to the interface configured between Jupiter and Oracle  
- Controls over any changes to the interface (including approval, testing, and implementation of these changes)  
- Controls over program development, if applicable to the implementation of the interface  
- Controls over changes to the job scheduler and access to perform such changes, if applicable to the execution of the interface |

### Testing the Completeness of Data Used to Test a GITC

**[8.4.90]** In order to properly test controls over user access provisioning and/or program and database changes, we first need to perform adequate procedures to determine that the populations from which we are going to perform testwork are complete. Some systems have built-in tracking that helps identify the population of the relevant user access profiles and program and database changes. Obtaining a complete population of these changes is more difficult in systems without such tracking capability.
Illustration 8.12: Testing the Completeness of Data Used to Test a GITC

User access illustration:
In order to test system access, the testers (management and the auditors) obtain a list of users with access to specific profiles from the entity’s management. The testers did not, however, obtain evidence about the completeness of the list.

What they could do differently:
They may inspect the access control list in the system for a selection of users and verify that these users also appear on the report listing.

Some technologies have well-known utilities for generating an access listing (e.g., Unix, SAP, and Microsoft SQL Server). In these cases, testers may be able to obtain evidence regarding completeness by using knowledge of how to generate the access listing.

To determine the completeness of system-generated and management-prepared reports in these scenarios, testers may be able to perform a combination of procedures such as:
- Observing report generation;
- Collecting system screenshots that cannot be modified;
- Documenting dates and parameters used to create reports;
- Reviewing management’s testing procedures; and
- Performing other system inquiries to determine who actually has access to the reports and/or which specific profiles are used and who has those specific profiles.

Program change illustration:
During testwork over software change management, testers (management and the auditors) note that the entity uses a centralized, but manual, system to track software changes made to the IT environment and IT applications. Testers obtained a listing of software changes, but they did not perform sufficient procedures to determine whether or not the tracking system included the complete population of changes.

What they could do differently:
If there are limitations in the entity’s IT system, management and the auditors may be able to compare the manually prepared information regarding software changes to information in the system (e.g., the “last change” dates in the production library for programs). This procedure could provide evidence over the completeness of the manual report of changes in situations where there were no changes during the period.

Depending on the circumstances, this approach may be a good alternative when the entity does not have a change control function or application that has been configured to enforce appropriate SODs in the promotion of program changes into the production environment. However, this may not provide sufficient evidence in environments where multiple changes are expected to be made because the “last change” date will only show the date of the last change made, not all changes made during the period.
When to Test a GITC Related to Computer Operations

[8.4.100] Computer operations controls address backup and recovery, incident, and problem management procedures, as well as job processing controls. Generally, we are able to identify when entities are dependent upon controls over backup and recovery and incident management (for example, if a system failed and had to be recovered during the year). Identifying when we need to rely upon computer operations controls related to job processing can be more difficult. Entities should identify and test GITCs over job processing when automated controls depend on accurate, complete, and timely processing of system jobs (including batch jobs and interfaces) in information systems relevant to financial reporting. The following example demonstrates automated controls that may be supported by computer operations (job processing) GITCs because of threats to the ongoing effectiveness of those automated controls.

Illustration 8.13: Linking Computer Operation GITCs to Automated Controls

A banking entity performs the following routines during its nightly processing of debits (i.e., customer withdrawals):

- The debit file is sorted by account number and size of the debit.
- The demand deposit file is updated with the transactions from the debit file. Insufficient funds conditions are identified and written to the Not Sufficient Funds (NSF) file.
- The NSF file is processed. Accordingly, the debit items that cannot be paid are returned and the demand deposit account is charged the NSF fee.
- The demand deposit file is updated with the transactions from the credit file.
- The statement printing job identifies the accounts that are due for printing and creates a statement print file.

The following risks were identified:

Debit or credit items are not completely posted to the accounts because:

- The system jobs could be processed out of order or not processed at all, or
- The jobs may not run to completion.

Automated control identified:

The systems analyst establishes the job schedule based upon an approved job sequence.

Related GITCs linked to the automated control:

- Controls over granting and removing access to the job scheduler;
- Controls over making changes to the job scheduler;
- Controls over identifying problem conditions from job routines.
Assessing the Risk of Failure of a GITC

[8.4.110] The extent of evidence gathered for GITCs depends on the risk of failure of the particular controls to be tested, the nature of the control (automated versus manual), and other risk factors. We focus on the risk that the failure of a GITC will render an automated control ineffective and potentially result in a material weakness. We also consider the impact of the ineffectiveness of the automated controls in the aggregate caused by an ineffective GITC.

[8.4.120] The following illustration provides direction on identifying and linking GITCs related to access, change management, program development, and computer operations. The following illustration also demonstrates how to evaluate the risk of failure of each relevant GITC identified.

Illustration 8.14:
Selecting Automated Controls, Linking GITCs, and Addressing Risk of Failure

Process Narrative:
Sails-R-Us is an online retailer that sells yachting clothes. Sails-R-Us offers customers a 60-day return policy. The entity sees a lot of product returns because its customers purchase products in a number of colors and sizes, keep the items that best suit them, and then return the rest. The entity is running SAP as its Enterprise Resource Planning system. Sales are recorded in SAP when the product is shipped. At that time, the system provides the customer an itemized receipt along with a return label that includes a bar code with the transaction information (e.g., SKUs, sales quantity, selling price, date of the transaction, etc.). If a product needs to be returned, the entity instructs customers to affix the return label to the outside of the package and include the receipt with the product being returned.

When products are returned, a clerk in the receiving department scans the barcode on the outside of the package, which brings up the itemized receipt that was sent to the customer in the POS system. The clerk then identifies which returned products are in the package and marks them in SAP. The date of return is recorded in the system in conjunction with the return.

The entity’s financial reporting group runs a monthly report using the most recent 24 months of data to calculate, by product category, the average percentage of sales returns for each of the 60 days after original sale. These percentages are then applied to the most recent 60 days of product sales, by category, to arrive at the estimated sales return reserve. The assistant controller reviews the calculations, and the accounting clerk makes a manual entry to record any required adjustment to the sales return accrual.

The following WCGWs related to IT are identified:
— WCGW 1 – The sales return data within SAP may not reflect complete and accurate information due to unauthorized access.
— WCGW 2 – The sales return data within the POS system may not reflect complete and accurate information due to unauthorized access.
— WCGW 3 – The sales return data within the POS system may not reflect complete and accurate information due to inaccurate data input.

— WCGW 4 – The report that calculates the average sales return percentages by product category in SAP may not be configured to capture all sales returns or product categories.

— WCGW 5 – The manual journal entry to record the allowance for sales returns is not complete or accurate due to unauthorized access.

The following automated controls address the WCGWs and are linked to the relevant GITCs:

— App Control 1 – Direct access to sales return data in SAP is limited to Database Administrators (DBAs). To change the sales return data, the DBA must log into the APPS account. Activity performed by the APPS account is monitored (lower risk of failure).

GITC 1 – DBAs’ access to SAP data is limited to READ access. To make changes to the database, the DBA must log into the APPS account. When a user logs into the APPS account, an e-mail is sent to the IT Operations manager, who then assures that the log-in activity matches an approved change request.

— App Control 2 – The POS system only allows authorized receiving clerks to accept returns at the distribution center (lower risk of failure).

GITC 2 – Access to the Security Administration functions in the POS and SAP systems are limited to Security Operations.

GITC 3 – Security Operations requires an approved access request ticket to set up access for the application functionality.

GITC 4 – Access to application functionality is restricted based upon a set of predefined roles.

— App Control 3 – When the return label for a returned product is scanned at the receiving dock, the POS system is configured to automatically pull up the relevant information (i.e., SKU’s, sales quantity, selling price, date of the transaction, etc.) in the sales returns screen (lower risk of failure).

GITC 5 – Access to implement changes to the configuration of the return label scanning process is limited to Computer Operations; operators have no access to source code.

— App Control 4 – The entity runs a report that calculates the average percentages of sales returns by product category for the past 24 months. This report can only be generated through an automatically scheduled job after the job schedule has been developed and tested (lower risk of failure).

GITC 6 – Access to implement changes to the report is limited to Computer Operations; operators have no access to source code.

GITC 7 – The running of the report is controlled by the Job Scheduler. Changes to the job schedule are tested prior to being placed into production.
GITC 8 – Access to the job scheduler is restricted to Computer Operations; operators have no access to source code.

---

App Control 5 – SAP restricts the recording of manual journal entries to designated individuals (higher risk of failure).

GITC 2 – Access to the Security Administration functions in the POS and SAP systems is limited to Security Operations.

GITC 3 – Security Operations requires an approved access request ticket to set up access for the application functionality.

GITC 4 – Access to the application functionality is restricted based upon a set of predefined roles.

GITC 2, 3, and 4 support the consistent operation of App Controls 2 and 5, which have different risks of failure. App Control 5 has a higher risk of failure because it addresses a fraud risk. As result, the engagement team assessed the risk of failure as higher for GITCs 2, 3, and 4.

[8.4.130] When a GITC has a higher risk of failure, we use judgment to alter the nature, timing, and extent of our monitoring/testing. For example, rather than performing inquiry and observation procedures, we should consider performing inspection or reperformance procedures. We should also consider the need to increase the persuasiveness of evidence obtained during the period between interim testing and year-end (by augmenting inquiry and observation with other procedures) and increasing sample sizes.
Key takeaways:

Identifying, Linking, and Testing GITCs

1. **Properly link GITCs to process-level automated controls.** Remember that we test GITCs that address the consistent operating effectiveness of the automated controls selected for testwork. Completion of the working paper, *Identification of GITCs – Linking GITCs to Automated Controls*, will help address the risks to the consistent operation of process-level automated controls and system generated or management prepared reports being relied upon.

2. **Test the completeness and accuracy of data used in the test of a GITC.** When testing user access provisioning and/or program and database changes, *perform adequate procedures to determine that the populations of user access profiles and program and database changes are complete* in order to test those controls properly.

3. **The extent of evidence we need to gather for a GITC depends on its risk of failure.** When evaluating the risk of failure of a GITC, consider the importance to ICOFR of the automated controls that the GITC is supporting. Consider the nature of the control (automated versus manual). And consider other risk factors such as the materiality of the error the control is designed to prevent, detect, and correct; the inherent risk of error in the account; and the competence of the personnel performing the control.

4. **If we know GITCs might be ineffective, we might choose not to test automated controls.** When GITCs are not effective and we do not test automated controls, we carefully *consider whether manual controls intended to compensate for the ineffective GITCs are dependent upon information that is in turn dependent* upon the automated controls and GITCs that were not tested and/or deemed to be ineffective.
[8.5.10] EUC includes a variety of user-based computer applications, including spreadsheets, databases, ad hoc queries, and stand-alone desktop applications. Management should assess the risk that the data in these applications becomes corrupted. Management should then design controls to secure, back up, and regularly review these applications for process integrity; they might be used as the basis for making journal entries or preparing other financial statement information. Many spreadsheets have errors, and password-protected spreadsheets can be accessed by following instructions available on the Internet. Because of this, IPE used in or produced by EUC should be viewed with an appropriate level of professional skepticism and should be subject to the appropriate controls over completeness and accuracy.

[8.5.20] EUC and other management-prepared documents provide a unique set of control challenges. By its nature, end-user computing brings the development and processing of information systems closer to the user. This environment may not be subject to the same level of rigor and structure as applications processed in a more centrally controlled environment. Nonetheless, the output of the EUC may be used by management in financial reporting. In accordance with COSO and PCAOB guidance, end-user applications are part of the financial reporting process and subject to the same level of controls as the rest of the financial reporting process. EUC is even more prevalent in smaller and less sophisticated IT environments. The importance of EUC has been highlighted in a number of SEC Staff Views papers released and in inspection comments from the PCAOB.

[8.5.30] When an entity uses EUC to support a class of transactions or as part of the financial reporting process, management should adopt sufficient controls to ensure completeness and accuracy of the information. Depending on the nature of the WCGW, manually reviewing and comparing EUC input to output may be enough to ensure the controls around EUC are working as intended. For instance, access to EUC may be controlled automatically, and we can test these process-level automated controls. However, these automated controls may not address the integrity of the operations performed by the EUC (e.g., the calculations in a spreadsheet), so it may be necessary for the entity to implement recalculation or other manual controls.

Illustration 8.15:
End-User Computing

The COSO Framework illustrates appropriate controls over end user computing which may provide a roadmap to our testing approach:
Smythe and Smythe International recently evaluated the use of spreadsheets in its financial close process. In doing so, it identified spreadsheets supporting calculations for LIFO (last-in, first-out) inventory and the fair values of goodwill, intangible assets, and debt. Because these calculations were significant to the financial statements and susceptible to error, the spreadsheets were classified as high in risk.

Smythe & Smythe also classified the spreadsheets as high in complexity because they use macros and multiple supporting spreadsheets to which cells and values are interlinked.

The entity considered the security, maintenance, and update risks of the spreadsheets and then selected and developed the following control activities and GITCs.
— Input Control – Input data is reconciled to source documentation to cover its completeness and accuracy.

— Access Control – File-level access to the spreadsheets on a central server is limited to approved users, and a password is required to access the LIFO inventory spreadsheet.

— Version Control – Standard naming conventions and directory structures ensure that only current and approved versions of the spreadsheet are used.

— Calculation Testing – All changes to formulas are tested against a manual calculation for accuracy. All spreadsheet formulas are checked for accuracy at least once a year.

— Overall Analytics – Analytical business process reviews using preestablished operating income and working capital thresholds find errors in any of the spreadsheets.

Key takeaways:

End-User Computing

1. **Control considerations over end-user applications are similar to control considerations over other applications.** If end user applications are part of the financial reporting process, they should be subject to the same level of controls as the rest of the financial reporting process.

2. **Management should adopt sufficient controls to ensure completeness and accuracy of the information** generated from end-user applications, and should be tested by both management and the external auditor when they address a WCGW.
8.6 Considerations When a GITC Deficiency is Identified

[8.6.10] If GITCs are ineffective, we may not be able to rely on the process-level automated controls they support, which in turn may impact our conclusions on the effectiveness of ICOFR.

[8.6.20] Although GITC deficiencies, on their own, do not directly cause financial statement misstatements, deficient GITCs may render a process-level automated control ineffective, and this may lead to financial statement misstatements that could be material. The significance of a GITC deficiency relates to its impact on the effectiveness of automated controls.

[8.6.30] When a GITC deficiency is identified, it is important to step back and:

— Perform a critical analysis of the GITC deficiency to reconfirm our understanding of the GITC and its design, the nature of the deficiency, and the pervasiveness of the deficiency. For example, the GITC deficiency may impact all the supported automated controls, or it may only impact a particular business function, location, or IT application.

— Determine which of the automated controls originally linked to the GITC are truly impacted by the deficiency. Do not assume that every automated control initially linked to the GITC is now deficient.

The working paper Identification of GITCs – Linking GITCs to Automated Controls included in Appendix 8.1, will help management and auditors identify the automated controls affected by the GITC deficiency.

Illustration 8.16: Identifying the Process-Level Automated Controls that May Be Impacted by the GITC Deficiency

The GITC deficiency and related automated controls:
A GITC deficiency related to programmer access to production is identified. Five automated controls were originally assessed as being supported by the GITC.

Stepping back:
The programmer access to production deficiency in this situation was limited to instances where programmers had inappropriate access at the operating system level. Further analysis by management determined that programmers did not have inappropriate access at the application level.

Management used their understanding of the GITC to determine that the deficiency only impacted application controls that rely on program code, and not to controls that are configured within the application and require privileged access at the application level to be changed. Management and the auditors will need to assess the potential impact of the GITC deficiency on the automated controls that rely on program code changes.

Of the five automated controls originally assessed to be supported by the GITC related to programmer access, three rely on program code and two are related to program configuration. Management and the auditors may find it clearer to represent the programmer access GITC as two different controls:

— Management will need to assess the potential impact of the GITC deficiency on the three code-enabled automated controls and determine whether compensating controls address the same risks to the consistent operation of these code-enabled automated controls.

— Management will need to list an additional GITC for programmer access related to program configuration and link that GITC to the two configurable automated controls.
Once we have a confirmed list of process-level automated controls that may be impacted by the deficiency, we evaluate and document that potential impact. Understanding how an automated control addresses the WCGWs for a particular assertion is important. For example, we understand that a process-level access control over the setup of new revenue contracts addresses a WCGW for the existence of revenue assertion. When this control is impacted by a deficient provisioning of access GITC, fictitious sales may be entered into the system, impacting the WCGW this automated control was intended to address, and potentially resulting in an overstatement of revenue reported.

After we evaluate and document the potential effect of a GITC deficiency on each relevant automated control, we may need to determine whether any compensating controls sufficiently address the same risks as the deficient GITC. We consider:

- Other formally established and regularly performed GITCs that address the same risks to the consistent operation of the automated control as the deficient GITC.
- Process-level controls (manual or automated) that do not rely on the deficient GITC, and address the same risks as the automated controls supported by the deficient GITC.

Illustration 8.17: Identifying a Compensating GITC

The GITC deficiency and related process-level automated control:

- The GITC over provisioning of access is deficient.
- A program change control relies on the provisioning of access GITC to ensure that programmers do not have access to migrate changes to production.
- Automated controls over a key calculation used for an important estimate rely upon the program change control.

Identifying a compensating GITC, should one exist:
With respect to the program change control, the engagement team identified and tested a compensating GITC. Management monitors all program changes made to the production environment each week by performing the following:

- Reviewing a system-generated edit/logging report (that cannot be altered)
- Comparing the report to the approved list of changes to identify any unauthorized changes deployed to production

In this case, the compensating GITC mitigates the impact of the deficient GITC on the program change control.

Note: This illustration focuses on assessing the impact of the provisioning of access deficiency on one automated control. We would need to continue this work, and apply similar focus to assessing the impact of this deficiency on all other relevant automated controls.
If a compensating control can’t be identified, or if the control only partially compensates for the deficient GITC, management may perform alternative procedures to determine whether the deficient GITC actually impacted the automated controls during the period under audit. Management’s ICOFR assessment should include procedures for investigating the impact of the deficient GITC. The example below illustrates this concept.

Illustration 8.18: Illustration of Alternative Procedures Performed in Forming our Risk Assessment

The GITC deficiency:
Management intends to rely on a process-level automated control consisting of a three-way match, but concludes that the program change controls that support the three-way match control are ineffective. (Application developers have unrestricted access to migrate changes into the production environment, allowing them to change the configuration of the three-way match without proper testing and authorization.)

Alternative procedures performed:
Management performed alternative procedures by determining that during the period under audit:

— No changes were made to the application throughout the audit period; or
— The only people who made changes to the application during the audit period were authorized and the changes were appropriate—they were reviewed individually and approved for production.

In this situation, management, as part of its control procedures, determined that the automated control was not impacted by the GITC deficiency. Without this analysis by management, both the GITC and the automated control would be considered deficient.

In contrast, because management performs this analysis as part of its control procedures, only the GITC would be considered deficient, and because the impact on the automated control was shown by management to be nil, the severity of the GITC deficiency is likely to be less than a significant deficiency before consideration of aggregation and root cause analyses.

This illustration shows the importance of timely detection of GITC deficiencies—management needs to have sufficient time to react to GITC deficiencies as part of its control procedures.

If an entity is relying on a GITC to support the consistent operation of its process-level automated controls, it may be challenging to identify compensating GITCs or alternative procedures that are not also reliant upon the ineffective GITC. For example, a provisioning of access deficiency may impact the integrity, and therefore the completeness and accuracy of the data in a report of program changes used to determine whether there were any inappropriate changes made to programs. In addition to impacting these automated controls, the provisioning of access deficiency may also impact other GITCs, such as program change controls.
[8.6.80] For a compensating GITC to effectively mitigate risk, it should address the same risks to the consistent operation of the process-level automated control as the deficient GITC. This evaluation needs to be performed for each automated control supported by the deficient GITC. There may be situations where compensating controls exist for some automated controls supported by the deficient GITC but not for all. Exercise caution and carefully analyze the compensating controls before concluding that they address the same risks as the deficient GITC.

[8.6.90] If there are no compensating GITCs, management and auditors may need to evaluate other manual controls or process-level automated controls that address the same risks as the affected automated control and that do not rely on the deficient GITC. In this evaluation, remember that Management Review Controls might use data from the IT systems that are compromised by the ineffective GITC (one example is shown in the common pitfall illustration in paragraph 8.4.20.) In addition, manual controls often are not designed to fully address deficiencies in automated controls related to the completeness and accuracy of the information. It is often difficult for management to demonstrate that the manual compensating control would detect information that is not materially complete and accurate.

[8.6.100] If no compensating controls are identified, the entity needs to evaluate and document the severity of each automated control deficiency that results from the GITC deficiency. Once all these automated control deficiencies have been evaluated, the entity must determine the severity of the GITC deficiency based on the most severe automated control deficiency resulting from the deficient GITC, and based on the potential total magnitude of deficiencies in all automated controls impacted by the deficient GITC. The external auditor will also assess this evaluation.

[8.6.110] A GITC deficiency also needs to be evaluated to determine its effect when combined with other control deficiencies, possibly in the entity's Control Environment component or with respect to Principle 11 in the COSO Framework. Management's decision not to correct a GITC deficiency affecting the Control Environment, when aggregated with other deficiencies affecting the Control Environment, could lead to the conclusion that a significant deficiency or material weakness in the Control Environment exists. Furthermore, this GITC deficiency also may be determined to be the result of a deficiency in the Control Environment or elsewhere, when a root cause analysis is performed.

[8.6.120] It also may be determined that a prudent official in the conduct of his or her own affairs would conclude that the GITC deficiency, by itself or in combination with other deficiencies, was a significant deficiency or material weakness. As a reminder, significant deficiencies that have been communicated to management and the audit committee and remain uncorrected after some reasonable period of time are strong indicators of a material weakness.
Key takeaways:

Considerations When a GITC Deficiency is Identified

1. **Take time to carefully evaluate the impact of GITC deficiencies.** Ineffective GITCs may affect the extent to which the entity may rely on the consistent operation of specific process-level automated controls that depend on that GITC and, therefore, may impact the entity’s conclusions on the effectiveness of ICOFR.

2. When a process-level automated control cannot be relied upon as a result of a GITC deficiency, **an entity may rely on other GITCs to address that GITC deficiency** (as noted in Illustration 8.17) or rely on manual controls to address a WCGW.
Appendix 8.1: Identification of GITCs-Linking GITCs to Automated Controls
Appendix 8.2: Practice Aid – Segregation of Duties
Chapter 9
Information and Communication
The Information and Communication component of internal control as defined by the COSO Framework highlights the importance of information management and communication between and among those responsible for supporting the achievement of the ICOFR objective. Information from both internal and external sources is needed to support the functioning of the other four COSO Framework components, Control Environment, Risk Assessment, Control Activities, and Monitoring Activities.

The Information and Communication component emphasizes that communication is a continual, iterative process of providing, sharing and obtaining necessary information both internally and externally. Appropriate communication provides the information needed to carry out day-to-day internal control activities and for personnel to understand the role they play in internal control.

This chapter discusses the practical application of the Information and Communication component of ICOFR.
9.1 Principles of Effective Information and Communication

[9.1.10] The COSO Framework points out that “information is necessary for the entity to carry out internal control responsibilities in support of achievement of its objectives. Communication occurs both internally and externally and provides the organization with the information needed to carry out day-to-day internal control activities. Communication enables personnel to understand internal control responsibilities and their importance to the achievement of objectives.”

[9.1.20] The Information and Communication component supports the functioning of the other four COSO Framework components, Control Environment, Risk Assessment, Control Activities, and Monitoring Activities.

[9.1.30] The COSO Framework establishes three principles necessary for effective information and communication within an entity’s ICOFR:

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

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

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

[9.1.40] Remember that these are principles that need to be met. Often, entities attempt to demonstrate that they have met the principles by taking a bottoms up approach: namely, they map existing controls to each principle to determine whether there are controls for each principle. Mapping controls is important, but not likely to be sufficient to demonstrate that an entity has met each principle. What might be missing from this approach is an overall assessment of whether the controls that have been mapped are sufficient to demonstrate that the objectives of the principle have been achieved.

[9.1.50] The following Illustrations describe the three principles and underlying points of focus for the Information and Communication component under the COSO Framework. The illustrations provide examples of questions that may be asked to understand the entity’s processes and controls around information and communication. Keep in mind that a “no” answer to any of these questions does not necessarily mean that the particular principle or component is deficient; however, this answer might influence the assessment of other COSO components and principles.

---

1 Internal Control – Integrated Framework published by COSO on May 14, 2013, p.14
2 Internal Control – Integrated Framework published by COSO on May 14, 2013, p. 105
### Illustration 9.1:
Considerations for Principle 13 of Information and Communication

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

<table>
<thead>
<tr>
<th>Points of Focus</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Identifies information requirements</td>
<td>— When considering “what could go wrongs” (or WCGWs) within business processes (see chapter 5 of the ICOFR Reference Guide – Risk Assessment), does the entity consider the WCGWs related to the completeness and accuracy of information (produced by the entity) used in the operation of controls?</td>
</tr>
<tr>
<td>— Captures internal and external sources of data</td>
<td></td>
</tr>
<tr>
<td>— Processes relevant data into information</td>
<td>— Does the entity have policies and procedures in place to ensure consistency in securing data, retaining data, and converting data into information suitable for financial reporting?</td>
</tr>
<tr>
<td>— Maintains quality throughout processing</td>
<td>— Does the entity evaluate the information (including information obtained from external sources) for relevance and reliability?</td>
</tr>
<tr>
<td>— Considers costs and benefits</td>
<td></td>
</tr>
</tbody>
</table>

### Illustration 9.2:
Considerations for Principle 14 of Information and Communication

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

<table>
<thead>
<tr>
<th>Points of Focus</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Communicates internal control information</td>
<td>— Does the entity structure and tailor communication (inbound, outbound, and cross-functionally) based on the need and the audience?</td>
</tr>
<tr>
<td>— Communicates with the board of directors</td>
<td>— Does the entity ensure the communication of information pertaining to external financial reporting objectives and internal control?</td>
</tr>
<tr>
<td>— Provides separate communication lines</td>
<td></td>
</tr>
<tr>
<td>— Selects relevant methods of communication</td>
<td></td>
</tr>
</tbody>
</table>
Illustration 9.3:
Considerations for Principle 15 of Information and Communication

<table>
<thead>
<tr>
<th>Points of Focus</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Communicates to external parties</td>
<td>— Does the entity structure communication to external parties based on the need and the audience?</td>
</tr>
<tr>
<td>— Enables inbound communications</td>
<td>— Does the entity allow for inbound communication?</td>
</tr>
<tr>
<td>— Communicates with the board of directors</td>
<td></td>
</tr>
<tr>
<td>— Provides separate communication lines</td>
<td></td>
</tr>
<tr>
<td>— Selects relevant methods of communication</td>
<td></td>
</tr>
</tbody>
</table>

[9.1.60] Entities must consider whether the Information and Communication principles have been met, and document their considerations with supporting evidence. The nature and extent of documentation will vary from entity to entity as there is no one correct approach. One possible approach is to answer the relevant questions posed in the Illustrations above, and maintain supporting documentation that led to that answer. Ask, based on the supporting documentation assembled, would a prudent official be able to answer the same relevant question in the same manner? If not, the supporting documentation may need to be supplemented with further evidence or explanation.

Information

[9.1.70] When considering the information used by management, the COSO Framework states that the quality of information depends on whether it is accessible, correct, current, protected, retained, sufficient, timely, valid, and verifiable.3

[9.1.80] Pertinent information is used at all levels of the entity. It should be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities to achieve financial reporting objectives.

[9.1.90] It can be challenging to identify what information is pertinent to an entity’s ICOFR. One way to evaluate this is through a “bottom-up” approach: management evaluates information needs for each relevant business process, and then establishes a mechanism to ensure that information is disseminated across the entity to meet those needs.

[9.1.100] Management is required to have controls over the propriety of information used in the operation of all control activities. This includes controls over the completeness and accuracy of information produced internally and the relevance and reliability of information obtained externally.

[9.1.110] While these controls are necessary for all relevant information used in the operation of control activities, the need is found most often when considering management review controls as these types of controls often require internal and external information to perform the review. An extensive discussion of the completeness and accuracy of information produced internally is included in chapter 7 of the ICOFR Reference Guide – Management Review Controls.

3 COSO Framework, p. 111
Illustration 9.4:
Impact of Information and Communication on Control Activities

Example:
The tax director performs a review (a management review control) over a multinational entity’s tax provision. This review is likely a set of controls that includes reviews over all relevant aspects of the tax provision.

Impact of Information and Communication:
To effectively execute this review control, the tax director needs to be informed of business activities in areas that may be outside his or her function. These may include the launch of new products or new geographic markets, related-party transactions (to evaluate the impact of transfer-pricing), employee activities in other jurisdictions (to determine in which jurisdiction the entity’s revenue was earned and where it is taxable), and other information such as changes in tax laws in foreign jurisdictions.

Review controls such as this may be deficient if the tax director is not informed of relevant information—for instance, if a cross-functional management meeting is held to communicate information about strategy to sell product in a new foreign jurisdiction, and the tax director is not invited.

Failure to obtain relevant and sufficient information is a deficiency in the Information and Communication component. It may also indicate that a similar issue with respect to the flow of information might exist in other controls. If this issue is more pervasive, a more severe ICOFR deficiency evaluation may result.

Illustration 9.5:
Relevance and reliability of information obtained externally

Example:
The entity uses a third party to assist in preparing a discounted cash flow analysis used in its annual goodwill impairment test. There is information used in the analysis by the third party, for example the discount rate. As part of management’s review of the third-party analysis, management should consider the relevance and reliability of the discount rate selected by the third party. The more important the discount rate is to the overall analysis, the more evidence the entity should produce to show the effectiveness of the review.

There are other WCGWs and controls related to the information used in the annual goodwill impairment test. For example the entity provides cash flow projections to the third party. Those cash flow projections need controls around the propriety of the projections and the accuracy of the cash flow information.
Communication

[9.1.120] Management should establish expectations such that when control operators become aware of significant matters relating to internal control that may impact other functions, operating units, or divisions, they communicate their observations up, down, and across the entity. Significant matters include instances of weak or deteriorating internal controls, absence of key controls and non-adherence to established controls. The entity also should enable inbound communication from external parties to support its system of internal control. Management should establish a process to make sure that complete, accurate and appropriate information is made available on a timely basis to control operators.

[9.1.130] Personnel should understand how their roles, responsibilities, and actions relate to the work of others in the entity and how they may affect the achievement of effective internal control over financial reporting.

[9.1.140] Information about an entity's objectives, policies and procedures, and control requirements, as well as information necessary for the effective operation of internal controls, may be communicated through a variety of different channels such as:

- Departmental vision and mission objective signs posted in high-traffic areas or on the entity's web site;
- Accounting and finance internal meetings or conferences to discuss internal control matters and accounting policy changes;
- Public display of the code of conduct;
- Regular entity-wide emails, newsletters, conference calls, webcasts, or meetings about updates on internal control matters; and
- Senior finance and executive management visits to plants, sales offices, major customers, and other locations.

Key takeaways:

Information and Communication

1. **Be familiar with the points of focus** described in the COSO Framework related to information and communication. They are helpful in describing what is required to maintain an effective Information and Communication component.

2. Pay particular attention to the controls over the propriety of information used in the operation of a control, especially management review controls. This includes the **completeness and accuracy of information produced internally** and the **relevance and reliability of information obtained from external sources**.
Chapter 10
Monitoring
One of the five integrated components of internal control over financial reporting (ICOFR) under the COSO Framework is Monitoring Activities (Monitoring). The Monitoring component includes Principles 16 and 17. Principle 16 and its related points of focus, which are the emphasis of this chapter, relate to organizations having a process in place “to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning.”¹

While all of the components of internal control are related and must operate together in an integrated manner for effective internal control, the Monitoring component deals primarily with determining that the established controls functioned in a manner to effectively address the current risks to the organization’s financial reporting process. Monitoring activities may include ongoing evaluations, separate evaluations that are performed periodically, or a combination of both.

Monitoring activities do not replace control activities because they generally do not operate at a level of precision that would prevent or detect monetary errors in specific financial statement assertions. This is the key differentiating factor between monitoring activities and control activities, which are discussed in more detail in chapter 6 of the ICOFR Reference Guide – Control Activities. While control activities are responsive to risks to specific financial statement assertions and are generally designed with sufficient precision to prevent or detect material misstatements in the financial statements, monitoring activities are not—rather, they provide evidence that the other components in general, and control activities in particular, are operating effectively.

Principle 17 of the COSO Framework relates to evaluation of deficiencies in internal controls and communication of those deficiencies to the parties responsible for taking corrective action, including those charged with governance. Chapter 11 of the ICOFR Reference Guide – Identifying and Evaluating Deficiencies addresses the evaluation and communication of internal control deficiencies in accordance with Principle 17.

¹ Internal Control – Integrated Framework published by COSO on May 14, 2013, p. 123
10.1 Principles of Effective Monitoring

[10.1.10] Monitoring assesses whether the controls within each of the components of internal control, including controls to effect the principles within each component, are operating as intended. Results of effective monitoring also assist in the determination of what needs to change in the system of ICOFR to prevent or detect, on a timely basis, future errors in an entity’s financial statements. Monitoring also includes evaluating the entity’s overall compliance with the COSO Framework by evaluating the severity of identified deficiencies.

[10.1.20] The SEC Staff stated that the evidence of the operating effectiveness of the control activities is required to support management’s assessment under Section 404(a) of the Sarbanes-Oxley Act of 2002 (SOX). This evidence comes from monitoring activities.2

[10.1.30] This statement by the SEC Staff is consistent with the guidance in the COSO Framework, which establishes the following principles necessary for effective monitoring of ICOFR:3

<table>
<thead>
<tr>
<th>Principles of the Control Activities Component</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

[10.1.40] These principles are required to be met in order to demonstrate effective ICOFR.

[10.1.50] Often, entities attempt to demonstrate that they have met the principles by taking a bottom-up approach: namely, they map existing controls to each principle to determine whether there are controls for each principle. Mapping controls is important but not likely to be sufficient to demonstrate that an entity has met each principle. What might be missing from a bottom-up approach is an overall assessment or a top-down evaluation of whether the controls that have been mapped to a principle are sufficient to address all important aspects of the principle.

---

3 COSO Framework, p. 123.
Illustration 10.1:
Contrasting a bottom-up approach vs. a top-down approach to demonstrating whether a principle has been achieved

**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.

**Bottom-Up Approach:**
Entity A is a manufacturer of residential flooring products. It has an internal audit department which assists management and the board of directors in monitoring the entity’s business operations and financial reporting. Management identifies the internal audit function as a monitoring activity, adds the activity to the COSO 2013 Mapping tool and links it with Principle 16. Management concludes that the principle has been sufficiently addressed by the entity.

This bottom-up approach is not effective because it does not demonstrate that the entity has appropriately addressed a number of important aspects of Principle 16, including the need to monitor the continuing effectiveness of all components of internal control, consider a mix of ongoing and separate evaluations, their scope and frequency, integrate these evaluations with the significant business processes, and adjust the monitoring activities in response to changes in the organization.

**Top-Down Approach:**
Given the guidance in Principle 16 of the COSO Framework, management and internal audit decide to take a fresh look at the scope and nature of Entity A’s monitoring activities. To accomplish that, management and internal audit prepare and document an overview of their annual monitoring plan. The plan first lays out the existing ongoing evaluations built into each component of internal control, including each significant business process within the Control Activities component. For example:

— Within the Control Environment component, management and internal audit note that the entity conducts an annual survey of its employees regarding their familiarity with the entity’s standards of conduct and their perception of the tone at the top, integrity, and ethics throughout the entity. The survey is added to the annual monitoring plan as a monitoring activity over a key aspect of the Control Environment component of ICOFR.

— Within the sales process, management and internal audit note the existence of several key performance indicators (KPIs) monitored by management 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 the allowance for doubtful accounts as a percentage of gross A/R at the end of each month. 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.
Having mapped out the existing ongoing evaluations built into the individual components of internal control and significant business processes, management and internal audit then consider the need to supplement the existing monitoring activities to fully address the requirements of Principle 16. The additional activities may include both ongoing evaluations, which need to be built into the ICOFR components and significant processes on a go-forward basis, and separate evaluations that will be conducted on an ad-hoc basis by internal audit. For example, management notes that the payroll process experienced a significant change in the past several months following implementation of a new HR/payroll application. Taking this into account, management and internal audit decide that internal audit will perform a walkthrough and testing of the new payroll process and related controls to ensure appropriate safeguarding of the entity’s assets (i.e., no payment to fictitious employees), compliance with applicable tax and labor regulations, and appropriate reporting of payroll costs and related benefits in the entity’s financial statements.

The supplemental monitoring activities are added to the annual monitoring plan. Management and internal audit then evaluate the overall plan and conclude that it appropriately addresses all components of the entity’s ICOFR and is responsive to the requirements of Principle 16 of the COSO Framework. The plan is then presented to Entity A’s audit committee in connection with its annual review and approval of the internal audit work plan.

[10.1.60] Supporting the two principles listed in paragraph 10.1.30 are “points of focus.” As discussed in chapter 1 of the ICOFR Reference Guide – Introduction, these points of focus are example characteristics that may help both management and external auditors determine if a principle is present and functioning.

[10.1.70] Unlike COSO principles, the COSO Framework does not require each point of focus to be met in order for management to conclude that ICOFR is effective.

[10.1.80] The following Illustrations describe the two principles and underlying points of focus for the Monitoring Activities component of the COSO Framework. The Illustrations provide examples of questions that may be asked to gain an understanding of the entity’s Monitoring Activities. Keep in mind that a “no” answer to any of these questions does not necessarily mean that the particular principle or component is deficient; however, this answer might influence the assessment of other COSO components and principles.
Illustration 10.2: Considerations for Principle 16 of Monitoring Activities

<table>
<thead>
<tr>
<th>Points of Focus</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Considers a mix of ongoing and separate evaluations</td>
<td>— Does the entity have a documented monitoring plan for all five components of ICOFR?</td>
</tr>
<tr>
<td>— Considers rate of change</td>
<td>— Do the entity’s monitoring activities consider a mix of ongoing and separate evaluations?</td>
</tr>
<tr>
<td>— Establishes baseline understanding</td>
<td>— Is the appropriateness of that mix reevaluated every year?</td>
</tr>
<tr>
<td>— Uses knowledgeable personnel</td>
<td>— Are the monitoring procedures performed merely to determine that the control activity was performed, or that it was performed effectively?</td>
</tr>
<tr>
<td>— Integrates with business processes</td>
<td>— How does the entity monitor the continuing effectiveness of components and related principles outside of Control Activities?</td>
</tr>
<tr>
<td>— Adjusts scope and frequency</td>
<td>— Does the entity use metrics or dashboards to monitor results or key control indicators within the organization?</td>
</tr>
<tr>
<td>— Objectively evaluates</td>
<td>— Does management monitor the results of service providers?</td>
</tr>
<tr>
<td></td>
<td>— How does the entity monitor controls over non-routine transactions?</td>
</tr>
</tbody>
</table>
Illustration 10.3: Considerations for Principle 17 of Monitoring Activities

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.

<table>
<thead>
<tr>
<th>Points of Focus</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assesses results</td>
<td>Does management have a process to track, communicate, and aggregate the deficiencies identified through both internal and external sources?</td>
</tr>
<tr>
<td>Communicates deficiencies</td>
<td>Does the entity have policies and practices to evaluate the severity of the identified deficiencies?</td>
</tr>
<tr>
<td>Monitors corrective actions</td>
<td>Does the evaluation include a root cause analysis of each deficiency?</td>
</tr>
<tr>
<td></td>
<td>Does the entity have a protocol for reporting significant deficiencies and material weaknesses to those charged with governance?</td>
</tr>
<tr>
<td></td>
<td>Does the entity have a process to develop, monitor, and report corrective actions taken in response to the identified deficiencies?</td>
</tr>
</tbody>
</table>

The remainder of this chapter focuses on applying Principle 16—that is, an entity’s process to monitor whether the components of internal control are present and functioning. Principle 17 related to identifying, evaluating and communicating control deficiencies is analyzed in greater detail in chapter 11 – Identifying and Evaluating Control Deficiencies.
[10.2.10] Demonstrating that the entity has met Principle 16 of the COSO Framework requires more than just implementing procedures to determine that a control activity has been performed. Monitoring procedures are performed to determine that the control activity has been performed effectively. This concept is important when determining which method should be used to monitor and who should perform the monitoring.

[10.2.20] The SEC Staff stated that the evidence of the operating effectiveness of control activities comes from monitoring activities, and may come from direct tests of controls, ongoing monitoring, or a combination of both\(^4\) (or what COSO calls a mix of “separate evaluations” and “ongoing evaluations”\(^5\)).

Separate Evaluations (Direct Tests)

[10.2.30] Separate evaluations are not embedded in the business processes but rather are conducted periodically by individuals. Generally these individuals need to have a high degree of objectivity relative to the processes and controls being evaluated (e.g., internal audit or others working under the direction of management). The scope and frequency of separate evaluations are a matter of judgment and are further discussed below.

[10.2.40] The COSO Framework identifies several possible approaches to separate evaluations depending on the degree of their objectivity and independence. These approaches include:\(^6\)

- Internal audit evaluations – internal auditors are often objective and competent resources, whether in-house or outsourced, and perform separate evaluations either as part of their regular duties or at the specific request of senior management or the board of directors;

- Other objective evaluations – such evaluations may be performed by other internal or external objective reviewers, such as SOX compliance team, IT security specialists, or consultants;

- Cross-functional evaluations – this type of monitoring may be performed by personnel from different functions or departments who are independent of the process and controls subject to evaluation;

- Benchmarking/peer evaluations – these evaluations include comparison or benchmarking of a component of internal control against the corresponding component of another entity or group of entities;

- Self-assessments – evaluations of the presence and functioning of control activities performed by personnel responsible for these controls or the unit or function to which the controls belong.

[10.2.50] An example of a separate evaluation is one where a manager from the controller’s office who is independent of the sales process and control owners within that process obtains an understanding of the process activities and tests the controls being performed within the process (e.g., through observation, re-performance, inspection of underlying documentation, etc.) to determine that they are conducted as intended and address all of the potential risks (what could go wrongs) within the sales process, as documented in the related process flowchart.

\(^4\) SEC Release No. 33-8810, pp. 27-28
\(^5\) COSO Framework, p. 126
\(^6\) Ibid. p. 130
There are a number of significant benefits associated with separate evaluations, including in particular:

— Ability to be applied in a non-routine, targeted manner in areas of concern or interest to management or the board of directors (e.g., areas of significant risk, including fraud risk);
— Ability to be applied in areas where relationships fluctuate significantly and cannot be effectively monitored through, for example, KPIs;
— Objectivity of the evaluation (generally); and
— Ability to be re-designed and adjusted to the changing circumstances of the entity.

Ongoing Evaluations

Ongoing evaluations are built into the routine operations of the entity and are performed on a real-time basis. In the words of the SEC Staff, “ongoing monitoring includes management’s normal, recurring activities that provide information about the operation of controls.”

Ongoing evaluations monitor either the effective operation of other controls or business performance in order to identify unusual trends that may be indicative of control deficiencies. Monitoring business performance is not the same as monitoring of controls although their purposes may overlap.

Monitoring of controls is specifically concerned with the effective operation of internal controls – whether the controls operate as designed, are performed by knowledgeable individuals, etc. An example of monitoring the operation of controls could involve scanning the number of exceptions in a three-way-match control.

Monitoring of business performance is directed at whether the entity’s (or its component’s) business performance 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 which serve as a benchmark for evaluation of the current-period actual results. An example of monitoring trends in business performance could include observing key performance indicators or metrics, such as the allowance for doubtful accounts as a percentage of accounts receivable, and following up on unexpected trends. While an unexpected trend in the allowance percentage may not be a result of a break-down in internal controls, it represents a trigger for management to look more closely at the credit sales, accounts receivable collection, and allowance calculation processes which may identify breakdowns in relevant control activities.

There are a number of important benefits associated with ongoing evaluations, including in particular:

— Routine conduct and continuous operation of the ongoing evaluations 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 more timely response by management.

SEC Release No. 33-8810, p. 28
Determining the Nature, Timing, and Extent of Monitoring Activities

[10.2.120] With reference to the various approaches to the monitoring of internal control, the COSO Framework states that “the scope, nature, frequency and formality of approaches vary with the relative importance of the risk responses and related components and principles of internal control that are being evaluated.” This highlights the need for entities to have a proper process in place for assessing risks (see chapter 4 of the ICOFR Reference Guide – Risk Assessment) as it will drive the entities’ determination of the relative importance of the various areas of ICOFR and the type of monitoring activities to employ in those areas, such as on-going or separate evaluations.

[10.2.130] An overall assessment of changes within the entity’s organization and its environment is another factor that should be considered as the entity develops and continues to assess the effectiveness of its monitoring program and ICOFR, as indicated by the second point of focus of Principle 16.

Illustration 10.4:
Determining the nature and extent of monitoring procedures

<table>
<thead>
<tr>
<th>When separate evaluations may be appropriate</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Moderate or significant inherent risk in the execution of the control or in the related account</td>
</tr>
<tr>
<td>— Moderate or significant judgment in executing the control</td>
</tr>
<tr>
<td>— History of errors in the related account</td>
</tr>
<tr>
<td>— Turnover in key personnel related to the control or process</td>
</tr>
<tr>
<td>— There has been an acquisition, changes in economic conditions, or other such changes that may impact the methods of processing information or the design of the control</td>
</tr>
<tr>
<td>— Management expects the external auditor to place reliance on the work of others relative to this control</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>When ongoing evaluations may be appropriate</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Low inherent risk in the execution of the control or in the related account or disclosure</td>
</tr>
<tr>
<td>— Low judgment in executing the control</td>
</tr>
<tr>
<td>— No history of errors in the related account</td>
</tr>
<tr>
<td>— No turnover in key personnel related to the control or process</td>
</tr>
<tr>
<td>— No changes to the process or design of the control</td>
</tr>
<tr>
<td>— Management does not expect the external auditor to place reliance on the work of others relative to this control</td>
</tr>
</tbody>
</table>

8 COSO 2013 Framework, p. 130
In general, as the risk of material misstatement of the entity’s financial statements related to a particular significant account or disclosure, or the related process, increases, management ordinarily enhances its monitoring activities over the controls in that area. Enhanced monitoring may be warranted in situations where the risk of failure of a control (i.e., risk that the control is not effective and, if not effective, that a material misstatement of the entity’s financial statements would result) is assessed as higher. Enhanced monitoring activities also may be warranted with reference to controls over areas of the entity’s financial reporting process that have been historically prone to errors, are complex, are exposed to significant risks of misstatement due to error or due to fraud, and areas which involve a significant degree of judgment.

Enhanced monitoring could be accomplished, among others, through the following actions:

— Utilizing in monitoring activities personnel who are more objective; this 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 subject to monitoring, evaluations performed by internal audit or other objective evaluators, benchmarking analyses, or peer evaluations;

— Changing or extending the period of time covered by the monitoring activities; and

— Increasing the extent of monitoring by supplementing or replacing ongoing evaluations with periodic direct testing of the underlying controls; in those situations, direct testing of controls may be used 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.

Illustration 10.5:
Determining the nature and extent of monitoring procedures

Controls over revenue
The risk of reporting inaccurate revenue is significant for most entities. In addition, there is often a fraud risk related to fictitious sales or improper cut-off of revenue. If the risk is significant, an entity may determine that it is necessary to have the internal audit department perform direct testing (separate evaluations) of the controls over revenue with highly objective, knowledgeable resources. The internal audit department may select transactions from any time in the year, but depending on the risks, it may determine that selecting more transactions at or near year end is appropriate.

Controls over additions to PP&E
For some entities, capital expenditures are relatively consistent year after year, transactions are straightforward, and the controls are routine in nature. In this situation, an entity may decide that self-assessments by control operators are appropriate because of the low risk of misstatement of the relevant assertion combined with management’s effective analytical review of capital expenditures and depreciation expense.
Regardless of the specific approach adopted by the entity to the monitoring of a particular area of ICOFR (ongoing or separate evaluations), Principle 16 of the COSO Framework highlights the importance of establishing a baseline understanding of how controls function in their current state. That understanding is necessary to properly set expectations for the monitoring activities. The frequency of reassessing this baseline is an area of judgment and should be made considering perceived risks. As the frequency of change increases, the need to refresh the baseline testing also increases. In Illustration 10.5, for example, while an entity may choose to utilize self-assessments and analytical reviews to monitor the operating effectiveness of controls over capital expenditures and depreciation expense for a year or two, eventually the entity should reestablish a baseline of operating effectiveness and test the control activities directly.

It may also be appropriate to have multiple monitoring activities in place that achieve the same objective (i.e., a mix of ongoing and separate evaluations). Such duplication may be beneficial in Monitoring because no individual activity or control can be reasonably designed to prevent or detect all potential issues.

Knowledge and experience of personnel assigned to carry out the entity’s monitoring activities represent additional aspects of Principle 16 that require careful evaluation by both management (when designing the monitoring activities) and external auditors (when evaluating the monitoring activities and planning to place reliance on them). This is particularly true with reference to the separate evaluations. According to the COSO Framework, since separate evaluations are conducted periodically by independent reviewers to provide feedback with greater objectivity, evaluators need to be knowledgeable about the entity’s activities and how the monitoring activities function, and understand what is being evaluated. Only knowledgeable experienced evaluators will be able to critically evaluate both the appropriateness of design and the operating effectiveness of the monitored control activities in the ever-changing business environment of the entity.
Illustration 10.6: Specific skillset required when monitoring

The goal of monitoring is not just to determine that the control activity operated, but that it operated effectively. Sometimes the control activity requires a particular skillset, such as expertise in income tax accounting. With respect to accounting for certain aspects of income taxes or other complicated accounting areas, internal audit may not have the appropriate skillset to be able to determine that the control activity was operating effectively. In such cases, others with the appropriate skillset will need to perform the monitoring of the controls. In the case of accounting for income taxes, the tax director may be the control operator while the VP of tax or a knowledgeable CFO may need to be the monitor.

The same principles would apply to a situation where the income tax function has been outsourced to a third-party service organization. As a general rule, while management may outsource a process to an external service provider, it may not outsource its responsibility for the results of the service provider’s work. Accordingly, management and external auditors should identify and evaluate both (a) controls over the work of the service provider and the relevant assertions over the significant accounts and disclosures impacted by the service provider and (b) monitoring activities over those controls. The control activities and the related monitoring activities should be performed by individuals with the appropriate knowledge and experience in the area of income tax accounting. Evidence related to some or all of the relevant control activities may come from a Service Organization Control (SOC) 1 – Type II report, if such a report is available for the service provider. In the absence of a SOC 1 – Type II report, management of the entity may either directly evaluate relevant controls in place at the service provider or design, implement, and operate its own controls over the work of the service provider and the relevant financial statement assertions. See chapter 5 of the ICOFR Reference Guide – Risk Assessment – Understanding WCGVs for further guidance regarding the role of third-party service organizations in an entity’s system of ICOFR.
An entity has designed its internal control responsibilities along the following general parameters: the Finance group is primarily responsible for designing and implementing controls, while the Internal Audit function is responsible for monitoring the effectiveness of the controls.

As part of its monitoring activities, the Internal Audit function considers the nature, timing and extent of the monitoring of all key controls across all five components of internal control.

— **Example 1**: The entity has a control to ensure that the code of conduct is communicated to all new employees. This may be an important component of the Control Environment with management and the board of directors setting the tone at the top. In order to monitor the continued appropriateness of design and effective operation of this important control, Internal Audit selects a sample of new employees hired in the current year and surveys them as to their receipt, review, and understanding of the requirements of the entity’s code of conduct. Internal Audit then analyzes the survey results and considers whether the control continues to be appropriately designed and operating effectively or whether additional steps need to be taken to facilitate employees’ understanding of and compliance with the entity’s code of conduct. This, coupled with other documented controls over the Control Environment, may be appropriate to address the monitoring of this component of the COSO Framework in the current year.

— **Example 2**: Management’s risk assessment is critical to the design and operating effectiveness of control activities. In order to effectuate the risk assessment process, management has determined that it is appropriate in the current year to walk through their business processes to reassess any changes that could impact the system of internal controls. In this case, Internal Audit chose to monitor risk assessment by attending the walkthroughs of some of the business processes. Their attendance functioned as proper monitoring of the risk assessment. In addition, the knowledge of the processes and WCGWs they gained through the walkthroughs enabled them to better monitor whether the controls were designed and operating effectively when testing control activities at the business process level.

**Illustration 10.7:**
Monitoring all components

An entity has designed its internal control responsibilities along the following general parameters: the Finance group is primarily responsible for designing and implementing controls, while the Internal Audit function is responsible for monitoring the effectiveness of the controls.

As part of its monitoring activities, the Internal Audit function considers the nature, timing and extent of the monitoring of all key controls across all five components of internal control.

— **Example 1**: The entity has a control to ensure that the code of conduct is communicated to all new employees. This may be an important component of the Control Environment with management and the board of directors setting the tone at the top. In order to monitor the continued appropriateness of design and effective operation of this important control, Internal Audit selects a sample of new employees hired in the current year and surveys them as to their receipt, review, and understanding of the requirements of the entity’s code of conduct. Internal Audit then analyzes the survey results and considers whether the control continues to be appropriately designed and operating effectively or whether additional steps need to be taken to facilitate employees’ understanding of and compliance with the entity’s code of conduct. This, coupled with other documented controls over the Control Environment, may be appropriate to address the monitoring of this component of the COSO Framework in the current year.

— **Example 2**: Management’s risk assessment is critical to the design and operating effectiveness of control activities. In order to effectuate the risk assessment process, management has determined that it is appropriate in the current year to walk through their business processes to reassess any changes that could impact the system of internal controls. In this case, Internal Audit chose to monitor risk assessment by attending the walkthroughs of some of the business processes. Their attendance functioned as proper monitoring of the risk assessment. In addition, the knowledge of the processes and WCGWs they gained through the walkthroughs enabled them to better monitor whether the controls were designed and operating effectively when testing control activities at the business process level.
Monitoring activities are NOT a substitute for but interact with control activities at the process level (control activities) in many ways. The following chart demonstrates some of the key differences between control activities, which are discussed in more detail in chapter 6 of the ICOFR Reference Guide – Control Activities, and monitoring activities under Principle 16 of the COSO Framework:

<table>
<thead>
<tr>
<th>Control Activities</th>
<th>Monitoring Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Respond to specific risks (WCGWs) at the process level</td>
<td>— Monitor the effective operation of control activities and other components of ICOFR</td>
</tr>
<tr>
<td>— Designed with sufficient precision to prevent or detect and correct errors in financial statement assertions at the would level of assurance</td>
<td>— Could identify errors themselves but that is not the objective of their design</td>
</tr>
<tr>
<td></td>
<td>— Designed to identify the cause of errors</td>
</tr>
<tr>
<td></td>
<td>— Monitor the remediation of deficiencies</td>
</tr>
</tbody>
</table>

As shown in the table above, the key difference between control activities and monitoring activities relates to their objective and their relationship to the risk of material misstatement of an entity’s financial statements. In the case of control activities, that relationship is direct: the objective of each control activity is to mitigate a specific risk within a business process which could lead to a material misstatement of the entity’s financial statements (we call that risk a “what could go wrong” or WCGW). Accordingly, control activities are designed and operated with a level of precision that provides confidence to both management and external auditors that they would prevent or detect, on a timely basis, a material misstatement to the entity’s financial statements.

On the other hand, monitoring activities have only an indirect relationship to the risk of misstatement of an entity’s financial statements. They do not themselves mitigate risks to specific financial statement assertions. Instead, they monitor the continuing appropriateness of design and operating effectiveness of control activities and controls within other components of ICOFR (Control Environment, Risk Assessment, Information and Communication, and Monitoring). The objective of monitoring activities is to timely identify deficiencies in control activities, analyze their root causes, and design and implement effective remediation plans. While serving all these functions, monitoring activities could identify a misstatement or misstatements in the entity’s financial statements. However, monitoring activities are more likely to identify instances where control activities did not operate effectively and where further investigation as to the propriety of financial reporting may be necessary.

The difference in the level of assurance provided by control activities (would-level of assurance) and monitoring activities (could-level of assurance) when it comes to mitigating the risks of material misstatement of an entity’s financial statements has important consequences for both management’s and external auditors’ approach to reliance on the monitoring activities in their assessment of the entity’s system of ICOFR.
There may be times when a monitoring control (e.g., management’s analytical review of a certain account) may be converted into a control activity. This would require making sure that the analytical review:

— Is responsive to the specific process level WCGWs identified in risk assessment;
— Meets the criteria for being a control activity, including identifying metrics, criteria, outliers, etc.; and
— Is precise enough to detect a material misstatement.

Typically, a flux analysis is not sufficient and will not be able to address relevant WCGWs at the level of assurance. It would need to be modified to define its precision, set an expectation based on relevant metrics, design follow-up procedures for any identified outliers, etc. Refer to chapter 6 of the ICOFR Reference Guide – Control Activities and chapter 7 – Management Review Controls for further guidance regarding design and operation of effective control activities.

Converting monitoring activities into control activities is the exception rather than the rule and may be difficult to achieve. Therefore, both management and external auditors should carefully consider all instances where a monitoring control is relied upon to address an identified risk of material misstatement of the entity’s relevant financial statement assertions.

Monitoring Activities in a Group or Multi-location Setting

Careful consideration of the differences between control activities and monitoring activities is particularly important when designing or evaluating the effectiveness of the system of ICOFR at an entity comprised of multiple locations (e.g. stores, warehouses, manufacturing facilities) or components (i.e. divisions, subsidiaries, business units, etc.).

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 of locations’ or components’ operations and their financial results, including regular reporting routines, which enables management at the consolidated entity level to monitor locations’ and components’ performance against budgets or forecasts, and to take appropriate action;
— Monitoring of timeliness and assessment of the accuracy and completeness of financial information received from locations or components;
— Monitoring of controls, including activities of the internal audit function and self-assessment programs.

Both management and auditors often look to these entity-level reviews to reduce or eliminate the need for reliance on and evaluation of controls that operate within individual locations or components of the entity. Such approach to the consolidated entity-level performance reviews requires careful evaluation.

9 SEC Release No. 33-8810, p. 28
In order 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, i.e. they need to be designed and operated with a level of precision that 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 – either individually or in aggregation with other misstatements – material to the entity’s consolidated financial statements.

Experience shows that the above-described consolidated entity-level reviews often do not represent control activities but rather are designed as monitoring activities; i.e., their objective is to identify unusual trends or anomalies in business or operating performance that may be indicative of possible breakdowns in process level controls at the location or component level. However, 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.

In such situations, unless management can convert the monitoring activities into control activities as described in paragraph 10.4.50, management should design and implement relevant controls at the individual locations or components of the entity, to the extent that such locations or components, either individually or when aggregated with others, include a risk of material misstatement of the group financial statements that is more than remote (see chapter 4 of the ICOFR Reference Guide – Risk Assessment for guidance regarding scoping of ICOFR 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 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, 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 amount of locations at which testing of process level controls needs to be performed. See further discussion of this matter in chapter 5 – Risk Assessment – Understanding WCGWs.
The degree of reliance on monitoring activities by external auditors in their audit of an entity’s ICOFR is governed by the applicable auditing standards. In particular, paragraph 39 of PCAOB Auditing Standard (AS) No. 5 states that in an audit of internal control over financial reporting, “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.”

Because of that direct focus in the ICOFR audit on control activities that mitigate the risk of misstatement to specific assertions over significant accounts and disclosures, it will be rare that an external auditor will be able to obtain sufficient evidence of the design and operating effectiveness of these controls by testing only the monitoring activities operating over the controls. However, as stated in paragraph 40 of PCAOB AS No. 5, “there might be more than one control that addresses the assessed risk of misstatement to a particular relevant assertion.” In some situations, a monitoring activity 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 limited particularly when it comes to the ongoing evaluations due to their characteristics discussed in section 10.2 of this chapter. 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 for example by internal auditors over low risk, routine controls. Whenever an external auditor relies on the work of others, they will have to perform sufficient re-performance to determine that the testwork 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.

Management must keep documented evidence of the effectiveness of controls, including the monitoring procedures performed. See chapter 2 of the ICOFR Reference Guide – Documentation. Regardless of whether the entity has chosen to monitor through on-going or separate evaluations, the documentation of monitoring should be sufficient to enable a prudent official to understand the nature, timing and extent of the monitoring activities performed, and have sufficient information to be able to conclude on the appropriateness of design and operating effectiveness of the monitoring activities.

Following the “prudent official” principle, documentation of the monitoring of the control activities will likely be more robust than the monitoring of the other COSO components. A reasonable level of documentation is always necessary to meet the “prudent official” principle of documentation and in order for management to assert that each of the control components and related principles are present and functioning. Appropriate documentation of management’s monitoring activities is also critical to external auditors’ ability to test these activities and obtain evidence of the entity’s compliance with the requirements of Principle 8 of the COSO Framework.
In Illustration 10.5, management should have controls to address the risk of material misstatement to PP&E. These may include controls over:

— The authorization of the purchase;
— The authorization of the payment after receipt of the asset;
— Assigning a useful life;
— Depreciating the asset; and
— Reviewing for impairment.

In this scenario, because controls are routine and the perceived risk is low, management has determined that a combination of self-assessments by the control operators (e.g., confirmation that the controls operated as designed during the year) and management analytical reviews provide evidence of the proper functioning of these controls for purposes of management’s annual assessment under Section 404(a) of SOX.

Such an approach may be appropriate given the assessed risk; however, external auditors should test the control activities directly to obtain sufficient and appropriate audit evidence that the control activities are operating effectively. There may be an exception if the analytical reviews performed by management are so precise that they are considered to be Management Review Control activities in addition to being monitoring activities. (See chapter 7 of the ICOFR Reference Guide – Management Review Controls)
In cases where management uses ongoing evaluations instead of separate evaluations, sufficient documentation will include the rationale for the nature, timing, and extent of monitoring procedures performed.

External auditors are required to obtain evidence of the effectiveness of the entity’s Monitoring function. This can be accomplished by:

- Understanding management’s approach to monitoring;
- Performing tests of the design and operating effectiveness of the entity’s monitoring activities; and
- Comparing the results of the control testwork performed by the auditors throughout the five components of ICOFR to those of the entity. To the extent that the external auditors discover a deficiency with respect to the design or operating effectiveness of a control, management and the external auditors will need to consider if there is also a deficiency in the entity’s monitoring (i.e., why did the auditors detect a deficiency but the entity’s monitoring process did not).

Key takeaways:

Monitoring

1. Generally, monitoring activities do not operate at a precision level that prevents or detects material misstatements in specific financial statement assertions. Instead, they act as indirect controls that review and investigate expectation gaps to determine whether the entity’s ICOFR continues to be relevant and responsive to changing risks. Monitoring controls allow management to assess whether controls within each of the five components are operating as intended and determine what needs to be changed to prevent future errors.

2. Because of the indirect nature and insufficient precision of monitoring activities, management and external auditors should carefully evaluate their reliance on these activities when deciding to reduce or eliminate the testing of controls at the process level and within other components of internal control. This is particularly important in ICOFR assessments performed at entities with multiple components and/or locations.

3. Management obtains objective evidence to support their assertion that the internal controls are operating effectively for all five COSO components. The nature and extent of that evidence depend on the assessed risk.

4. Effective monitoring does not replace the need to have the remaining components of the COSO Framework present, functioning, and operating together in an integrated manner.

5. Remember: external auditors generally will need to test the control activities directly, even in cases where management chooses a different monitoring procedure.
Chapter 11
Identifying and Evaluating Deficiencies
Management is required to evaluate “the severity of a deficiency in ICOFR by considering whether there is a reasonable possibility that the entity’s ICOFR will fail to prevent or detect a misstatement of a financial statement amount or disclosure; and the magnitude of the potential misstatement resulting from the deficiency or deficiencies.”1

The COSO Framework also requires management to assess the severity of identified control deficiencies.2 Although the COSO Framework suggests classifying the severity into two categories (major or minor deficiencies), entities that use the COSO Framework for the purpose of fulfilling its ICOFR responsibilities under securities laws will nevertheless continue to use the three categories defined by the SEC (material weakness, significant deficiency, and deficiency).3

The responsibility to identify and assess deficiencies under SOX 404 is essentially the same for both management and auditors. Identifying deficiencies in ICOFR and evaluating their severity may seem straightforward, but the task can be challenging. A six-step process, detailed in this chapter, may help management properly evaluate the severity of identified deficiencies while avoiding common challenges.

### Overview: A Six-Step Process

<table>
<thead>
<tr>
<th>Identifying the Internal Control Deficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Determine whether a control deficiency exists</td>
</tr>
<tr>
<td>2. Identify the deficient control by performing a root cause analysis</td>
</tr>
<tr>
<td>3. Determine whether the control deficiency is indicative of other deficiencies</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Evaluating the Internal Control Deficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Evaluate the severity of the deficiency by considering magnitude and likelihood of the potential misstatement</td>
</tr>
<tr>
<td>5. Identify relevant compensating controls and conclude on the severity</td>
</tr>
<tr>
<td>6. Aggregate similar deficiencies and evaluate the aggregated deficiencies for severity</td>
</tr>
</tbody>
</table>

This chapter references flowcharts to illustrate various aspects of the identification and evaluation process. The flowcharts are located in Appendices 11.1 – 11.4.

Further, attached to this chapter are two templates: a template (Appendix 11.5) that may be used to summarize the evaluation of identified deficiencies, and a template (Appendix 11.6) that may be used to document considerations with respect to any individual deficiency. This template may be used when the summary template isn’t sufficient to document relevant considerations, e.g., when the evaluation is complicated, a “close call,” or otherwise in need of a robust description and analysis. In addition, attached to this chapter are examples of completed templates (Appendix 11.7) and a Guide to Understanding the Flow of the SICD (Appendix 11.8).

---

What is a Control Deficiency?

[11.1.10] A deficiency in internal control 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.

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

How to Identify a Control Deficiency

[11.1.30] A deficiency means that there is an opportunity for a misstatement to occur, even though a misstatement may not actually have occurred.

[11.1.40] Deficiencies in internal control can come to management's attention in a number of ways, including but not limited to:

- Management's risk assessment or monitoring processes.
- Internal audit's work, whether related directly to ICOFR or not, or other internal sources.
- External sources such as regulatory reports or SEC comment letters.
- The external auditor's work.
- Restatements.
- Prior period immaterial error corrections.

[11.1.50] Some deficiencies, such as those identified by testing internal controls, may be obvious deficiencies in ICOFR. Deficiencies found in other ways, such as by reading regulatory reports, might be related to operations or compliance objectives, but they also may be indicative of an ICOFR deficiency and should be evaluated for any ICOFR impact.

Illustration 11.1:
Does a control deficiency exist?

**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.

If management identifies and corrects a misstatement in the preliminary financial statements while completing the financial reporting process and related control activities, the identification and correction of that misstatement may indicate that the internal controls are effective, not deficient.

However, if the external auditor detects a misstatement in the preliminary financial statements knowing management has not fully executed relevant controls, judgment needs to be used 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.
Illustration 11.2:
Does a control deficiency exist?

Scenario:
An internal audit finds an unusually high number of products are being returned within the warranty period. This may mean the entity’s quality assurance process needs improving (an operational matter).

If the entity has controls over the process to accurately estimate the warranty reserve, a need for improved quality assurance may not be indicative of an ICOFR deficiency.

Illustration 11.3:
Does a control deficiency exist?

Scenario:
An internal audit finds that the entity’s inventory cycle count program excludes certain categories of inventory from the counts, and it needs to be revised.

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

Illustration 11.4:
Does a control deficiency exist?

Scenario:
A calendar year end company 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 WCGWs identified in the process. However, given the proximity of the acquisition to the fiscal year-end, management and their 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, which as of the reporting date may have significant estimation uncertainty, with that uncertainty to be reduced as management finalizes its fair value estimates within the measurement period.

The underlying principle is it would not be reasonable to expect that management’s controls over the fair value estimates are designed and operating at a higher level of precision than the relevant account framework requires of the estimates themselves. Therefore, the controls around the final purchase price allocation should be more precise that the controls around the initial purchase price allocation, consistent with the increased precision of the underlying accounting for the estimates required by the end of the measurement period. If management’s controls are not at the appropriate level of precision, that would represent a deficiency.
Key takeaways:

Step 1: Determine whether a control deficiency exists

1. Remember: A deficiency represents the potential for misstatement. Therefore, a deficiency can exist in the absence of a misstatement and this deficiency may be a significant deficiency or a material weaknesses.

2. Remember: Generally a misstatement in the financial statements would not exist without a deficiency that permitted it to occur. Therefore, audit differences are usually a result of an underlying deficiency.

3. Consider operating or compliance weaknesses, including those in regulatory findings and internal audit reports, because they often have a related ICOFR effect.
Before evaluating the severity of a control deficiency, management needs to properly identify and describe it.

**Identifying the Control When the Deficiency Is Discovered Through Testing ICOFR**

When deficiencies are identified by directly testing ICOFR, it may be easy to identify the control that is missing, designed inappropriately or operating ineffectively and the related COSO component and principles. The table below provides examples of controls identified as deficient through direct testing of ICOFR.

Notice that the “Situation Identified” column and the “Control” column are very similar. Because these situations are identified during the direct testing of ICOFR, identifying the deficient control is straightforward. Also, notice that deficiencies may be identified in all COSO components and principles, not just Control Activities.

<table>
<thead>
<tr>
<th>Situation Identified</th>
<th>Control</th>
<th>Deficiency</th>
<th>COSO Component (and Principle)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The entity does not have a formal code of conduct.</td>
<td>Management has a formal code of conduct against which it can evaluate employee actions.</td>
<td>Control is missing</td>
<td>Control Environment (Principle 1)</td>
</tr>
<tr>
<td>Management has an annual process to perform risk assessment and adjust its controls accordingly, but the process, and the review of that process, were not thorough. As a result, management is not critically evaluating changes to the external environment, the industry or the entity to determine their impact on the entity’s internal controls.</td>
<td>Management performs, and senior management reviews, an annual risk assessment process at the entity and process levels to identify and evaluate internal and external changes that may impact the design or operating effectiveness of control activities.</td>
<td>Control is not operating effectively</td>
<td>Risk Assessment (Principle 7)</td>
</tr>
</tbody>
</table>

“Much of the dialogue the SEC staff has with companies regarding ICFR continues to focus on fully and accurately describing identified control deficiencies, including understanding the nature of the deficiency and the control that failed or was insufficient. We also routinely engage management in discussions regarding the root cause of identified control deficiencies, which is important because of the potential pervasive impact of certain control issues that may not be immediately obvious.”

– James Schnurr, SEC Chief Accountant

[11.2.10] Before evaluating the severity of a control deficiency, management needs to properly identify and describe it.

[11.2.20] When deficiencies are identified by directly testing ICOFR, it may be easy to identify the control that is missing, designed inappropriately or operating ineffectively and the related COSO component and principles. The table below provides examples of controls identified as deficient through direct testing of ICOFR.

Notice that the “Situation Identified” column and the “Control” column are very similar. Because these situations are identified during the direct testing of ICOFR, identifying the deficient control is straightforward. Also, notice that deficiencies may be identified in all COSO components and principles, not just Control Activities.

“Much of the dialogue the SEC staff has with companies regarding ICFR continues to focus on fully and accurately describing identified control deficiencies, including understanding the nature of the deficiency and the control that failed or was insufficient. We also routinely engage management in discussions regarding the root cause of identified control deficiencies, which is important because of the potential pervasive impact of certain control issues that may not be immediately obvious.”

– James Schnurr, SEC Chief Accountant

4 James V. Schnurr (October 2015), SEC Chief Accountant, Remarks Before the UCI Audit Committee Summit, Newport Beach, CA

© 2016 KPMG LLP a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 580828
<table>
<thead>
<tr>
<th>Situation Identified</th>
<th>Control</th>
<th>Deficiency</th>
<th>COSO Component (and Principle)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management does not require analysis and review of significant or unusual transactions.</td>
<td>Significant or unusual transactions are reviewed by management.</td>
<td>Control is missing</td>
<td>Control Activities or Monitoring (Principle 12 or 16)</td>
</tr>
<tr>
<td>Although designed appropriately, a control established by management to review bank reconciliations was not performed in a timely manner.</td>
<td>Bank reconciliations are reviewed by management.</td>
<td>Control is not operating effectively</td>
<td>Control Activities (Principle 12)</td>
</tr>
<tr>
<td>There does not appear to be communication between in-house counsel and the accounting department to properly accrue for and disclose legal contingencies.</td>
<td>Key information is provided from in-house counsel to the accounting department so that the accrual and disclosure of legal contingencies can be made based on appropriate information.</td>
<td>Control may be missing or designed inappropriately</td>
<td>Information and Communication (Principle 14)</td>
</tr>
<tr>
<td>Management has a process to monitor the operating effectiveness of controls. However, the process did not identify that the control to review bank reconciliations in a timely manner was not operating effectively.</td>
<td>Personnel monitor internal controls in the Treasury process for design and operating effectiveness.</td>
<td>Control is not operating effectively</td>
<td>Monitoring (Principle 16)</td>
</tr>
</tbody>
</table>
Identifying the Control When the Deficiency is Discovered in Other Ways

[11.2.30] There may be other situations where the direct testing of ICOFR did not detect a deficiency, but a deficiency is identified through other means (e.g., when the external auditor discovered an error in the financial statements). This is illustrated in the table below:

<table>
<thead>
<tr>
<th>Situation Identified</th>
<th>Control</th>
<th>Deficiency</th>
<th>COSO Component (and Principle)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The external auditor identified an error in the entity's tax provision</td>
<td>[There are many controls related to the tax provision. Which ones failed?]</td>
<td>[Difficult to determine without a root cause analysis]</td>
<td>[Difficult to determine without a root cause analysis]</td>
</tr>
</tbody>
</table>

[11.2.40] It is common, but inappropriate, to describe the control deficiency in terms of the error rather than specifically identifying which controls within the tax provision process failed and why they failed. Following this approach will lead to difficulty in determining:

- The true scope of the deficiency;
- Whether the deficiency indicates other deficiencies may exist;
- How to evaluate the severity of the deficiency, including its potential magnitude; and
- Whether the deficiency has been remediated.

Illustration 11.5:
Do not describe the deficiency in terms of the error

Scenario:
An error is identified in the entity’s tax provision. The entity identifies the control deficiency as follows: “There was an error in the operating effectiveness of controls related to the income tax provision.”

This description is insufficient because it does not identify the specific control or controls that are deficient. It only describes that the control relates to the income tax provision.

Based on this description, it will be difficult to determine if the deficiency indicates other deficiencies, how to evaluate the severity of the deficiency, and, later on, if the deficiency has been remediated.

See pages 12-14 for examples of appropriate and inappropriate identification of deficient controls.

Understanding the Process
[11.2.50] When determining the deficient control, it may be helpful to review the process to understand which financial reporting risks are present and which risks the deficient control was intended to mitigate. This understanding will also help determine the potential magnitude of the deficiency (step 4) and the relevance of compensating controls (step 5).

5 Kevin M. Stout (December 2015), SEC Senior Associate Chief Accountant, Remarks before the 2014 AICPA Conference on Current SEC and PCAOB Developments
Performing a Root Cause Analysis

[11.2.60] Perform a root cause analysis to appropriately identify and describe the deficient control. A root cause analysis can also identify interrelated controls that also may be deficient and expose more pervasive deficiencies (step 3). A proper root cause analysis is also an important prerequisite to aggregating deficiencies because it allows us to identify which deficiencies have similarities (e.g., whether they affect the same COSO component).

[11.2.70] A proper root cause analysis relies on asking probing questions containing interrogatives such as who, what, where, when, why and how, and continuing to ask those questions to reveal the underlying causal factors behind the error. This is an iterative process until you can't go any further—at which point, you are at the root cause.

The answer to each question should elicit a factual answer and generally cannot be answered with a simple “yes” or “no.”

Illustration 11.6:
Importance of a root cause analysis

Scenario:
Internal Audit discovered an error in a spreadsheet that is 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. Instead of designing a control specifically to address the completeness and accuracy of the information, management was relying on the control operator’s review of the warranty accrual to also address the completeness and accuracy of the information in the spreadsheet.

Root Cause:
As we perform the root cause analysis, we understand the following:

— The control operator was assuming the information in the spreadsheet was accurate;
— The control operator’s review would be difficult to design in such a way that he/she would be able 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, which should be designed to identify risks such as completeness and accuracy of information, never contemplated these risks.

The root cause analysis shows that the deficiency is more than just a design deficiency in one control related to the warranty accrual. It is related to an insufficient risk assessment caused by management’s insufficient knowledge of what is required by the COSO Framework.

This is important information because, as discussed further in the next section, it is important to consider whether other controls that rely on information produced by the entity might have a similar deficiency and all deficiencies eventually will be aggregated in the risk assessment component, by principle, to determine whether a material weakness exists. Without a proper root cause analysis, we may never have associated this deficiency with the risk assessment component and related principles.

[11.2.80] The proposed remediation plans may help us identify the related deficiency.
Illustration 11.7: Consideration of management’s remediation plan when determining which control is deficient

**Scenario:**
The external auditor identifies an error in an entity’s tax provision. If management’s remediation plan is to assign a more senior person to perform the same review, that may indicate either the control was designed inappropriately (e.g., an unqualified person is assigned to perform the review), or the control was designed appropriately but not performed correctly (a personnel issue).

Although management and the external auditor still would need to determine if the remedial action is sufficient and appropriate to address the deficiency, understanding the nature and extent of the remediation plans may be an appropriate starting point for identifying the deficient control.

**Key takeaways:**

**Step 2: Identify the control that is deficient**

1. Describe the deficiency in terms of (1) the control; (2) whether the control was **missing, designed inappropriately, or operating ineffectively**; and (3) the relevant **COSO component and principle**.

2. **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.

3. **Perform a root cause analysis** to determine the cause of the control deficiency.

4. **Consider the nature and extent of the remediation plan.** Remediation plans are helpful in identifying the deficiency.
11.3 Step 3: Determine Whether the Deficiency Is Indicative of Other Deficiencies

[11.3.10] Once the control, the nature of the deficiency, and the relevant COSO component and principle are properly identified, determine whether the control deficiency indicates the presence of other deficiencies. This is often part of the root cause analysis described in step 2. This may be accomplished in two ways:

1. Evaluate similar controls for the same type of deficiency.
2. Determine if the control deficiency represents a more pervasive issue in another component or principle of internal control.

**Evaluate Similar Controls for the Same Type of Deficiency**

[11.3.20] Before the severity of a deficiency can be evaluated, it is important to determine whether the deficiency may exist in similar controls.

**Illustration 11.8:**

Does the deficiency exist in similar controls?

**Scenario:**

Internal Audit’s control testing indicates that a key estimate was not reviewed at a sufficient level of precision by the control operator, resulting in a deficiency related to both the design and operating effectiveness of the control. Consider whether similar issues have been identified in other:

1. Management review controls, and/or
2. Controls performed by the same person.

Internal Audit also may reconsider whether it needs to perform additional testing of similar controls to have sufficient evidence of their operating effectiveness now that a deficiency has been identified in one particular control.

**Determine If the Control Deficiency Represents a More Pervasive Issue in Another Component or Principle of Internal Control**

[11.3.30] When a deficiency is identified in one component, consider whether that deficiency indicates a related, often broader, deficiency in another component or principle. Generally, this is accomplished in conjunction with the root cause analysis started in Step 2. In particular, there may be a relationship between:

- A deficiency in the design of a control within one component, such as Control Activities and another component, such as Risk Assessment; and
- A deficiency in the operating effectiveness of a control within one component, such as Control Activities, and another component, such as Monitoring.

[11.3.40] If a control deficiency indicates the possible existence of other deficiencies, repeat steps 1 and 2 of this six-step process to identify all potential deficiencies.

“While it is possible that some transaction-level control failures are isolated within the Control Activities component, the cause may often stem from a broader breakdown…Without understanding the cause of each identified deficiency, management may not be in a position to appropriately evaluate the effectiveness of each of the components of internal control.”

— Kevin Stout, SEC Senior Associate Chief Accountant

---

6 Kevin M. Stout (December 2015), SEC Senior Associate Chief Accountant, Remarks before the 2014 AICPA Conference on Current SEC and PCAOB Developments
Illustration 11.9:
Does the deficiency indicate a broader issue in another component or principle?

Scenario:
— If 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, this may indicate that the risk assessment process was inadequate.
— Consider 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.
— If a deficiency in the operating effectiveness of internal control is identified because a control to review certain reconciliations was not performed timely, this may mean that the monitoring process was not sufficient to detect that the control was operating incorrectly.

Consider why the monitoring process did not identify the deficiency and if there are other signs of weakness in monitoring.

Examples of Appropriate and Inappropriate Identification of Control Deficiencies and the Importance of Root Cause Analysis

Illustration 11.10:
Have we identified the correct deficiency?

Scenario:
The external auditor finds an error in the entity’s tax calculation. A conclusion is reached that the entity has a deficiency in the controls related to the tax calculation.

What was missed:
The control deficiency was incorrectly identified because it does not identify the specific control that was missing, designed inappropriately or operating ineffectively. Further, it appears as though there was no consideration as to why the control was deficient and whether the deficiency might be indicative of similar deficiencies beyond taxes or more pervasive deficiencies in other components. In this case, other deficiencies in internal control to which accounts and disclosures beyond the tax calculation are exposed may go undetected because a thorough root cause analysis of the tax calculation error was not performed.
Illustration 11.11:
Have we identified the correct deficiency?

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. A conclusion is reached that the entity has a deficiency in the controls related to the review of the tax calculation.

What was missed:
This identification of the deficiency does not specify which control was missing, designed inappropriately or operating ineffectively. It’s simply another way of saying that the error was identified in the entity’s tax calculation.

Illustration 11.12:
Have we identified the correct deficiency?

Scenario:
The external auditor finds an error in the entity’s tax calculation and determines that the deficiency related to a control designed to identify misstatements in the tax contingency accrual. Specifically, a tax director reviews the quarterly tax contingency calculation. Management determined that, as a result of its root cause analysis, the problem was caused because the tax director was unaware of a decision senior management made that affected the tax calculation. To remediate the deficiency, the entity 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 director attended these meetings 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, including the assessment of the technical competence of the tax director as well as the precision of the tax director’s review were also carefully considered. It was concluded that the tax director has the technical competence to perform an effective review and enough information to detect a material misstatement.

The design of the controls related to all other significant accruals and estimates were also evaluated and it was determined that other employees responsible for reviewing significant accruals or estimates already are attending the meeting. Therefore, it was concluded that the design deficiency appears to be limited to the tax contingency accrual review as well as related deficiencies in the information and communication component of COSO, since the tax reviewer, by design, did not receive information necessary for his review, and management’s risk assessment process since it did not identify this design deficiency.

The entity has controls in place where a member of management reviews a key estimate related to the tax contingency accrual. While the review was operating as designed, it was not designed in such a way that the reviewers
had access to critical internal information that may have affected the effectiveness of the review. This is a control weakness in the information and communication component.

Additionally, this may indicate a weakness in management’s risk assessment process. A root cause analysis is necessary to understand why the risk assessment process did not identify this design flaw, and investigate, for example, whether there are similar instances where the risk assessment process did not function properly and determine if there is a deficiency in the risk assessment process.

This is an appropriate identification of the control deficiency. It describes the control, explains how it was inappropriately designed and what was inappropriate about it, gives related information, and identifies the communication deficiency.

In addition, the root cause analysis may reveal a deficiency in the risk assessment component of COSO.

Note the difference in the analysis required to determine the root cause of the control deficiency. Consistent with the discussion in step 2, 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 competence, 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?

Key takeaways:

Step 3: Determine whether the control deficiency indicates other deficiencies

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.

3. An effective and thorough root cause analysis is needed to understand why a deficiency occurred and whether it is indicative of other deficiencies.
11.4 Step 4: Evaluate the Severity of the Deficiency

11.4.10 Once the deficiencies are identified, evaluate each one individually to determine its severity. A deficiency can be a material weakness, a significant deficiency, or a deficiency that is considered to be less severe than a significant deficiency.

11.4.20 A Material weakness is a deficiency, or a combination of deficiencies, in ICOFR, 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.8

11.4.30 A significant deficiency is a deficiency, or a combination of deficiencies, in ICOFR 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.9

Indicators of a Material Weakness

11.4.40 If 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 GAAP, then the deficiency, or combination of deficiencies, is an indicator of a material weakness.10

11.4.50 The SEC Staff has provided specific indicators of material weaknesses:11

1. Identification of fraud, whether or not material, on the part of senior management.
2. Restatement of previously issued financial statements for a material misstatement due to fraud or error.
3. Identification by the auditor of a material misstatement in circumstances that indicate management’s ICOFR would not have detected the error.
4. Ineffective oversight of the entity’s financial reporting and ICOFR by those charged with governance.

11.4.60 If a deficiency consistent with one of these four indicators is identified, ordinarily the deficiency is a material weakness.

11.4.70 However, just because one of these four indicators is absent does not mean the deficiency is not a material weakness.

“It is surprisingly rare to see management identify a material weakness in the absence of a material misstatement. I suggested these results could either stem from deficiencies not being identified in the first instance or from the severity of deficiencies not being evaluated appropriately.

I continue to question whether material weaknesses are being properly identified, evaluated, and disclosed. A take away you should have by the end of this conference is that our efforts throughout the SEC pertaining to the ICFR requirements are ongoing, coordinated, and increasingly integrated into our routine consultation, disclosure review, and enforcement efforts”7

– Brian Croteau, SEC Deputy Chief Accountant

---

7 Brian T. Croteau (December 2014), SEC Deputy Chief Accountant, Remarks before the 2014 AICPA Conference on Current SEC and PCAOB Developments
8 Reg. §. 240.12b-2. Note that the SEC’s definition of material weakness is consistent with the PCAOB’s definition in AS No. 5, An Audit of Internal Control Over Financial Reporting, par. A7.
9 Reg. §. 240.12b-2, consistent with the PCAOB’s definition in AS No. 5, A11.
“It’s important to remember that there are two components to the definition of a material weakness – likelihood and magnitude. The evaluation of whether it is reasonably possible that a material misstatement could occur and not be prevented or detected on a timely basis requires careful analysis that contemplates both known errors, if any, as well as potential misstatements for which it is reasonably possible that the misstatements would not be prevented or detected in light of the control deficiency. This latter part of the evaluation, also referred to as analysis of the so called ‘could factor,’ often requires management to evaluate information that is incremental to that which would be necessary, for example, for a materiality assessment of known errors pursuant to SAB 99. The final conclusions on severity of deficiencies frequently rest on the ‘could factor’ portion of the deficiency evaluation; however, too often this part of the evaluation appears to be an afterthought in a company’s analysis. Yet consideration of the ‘could factor’ is very important.”

— Brian Croteau, SEC Deputy Chief Accountant

[11.4.80] The definition of materiality to ICOFR is applied in the same way that it is applied to financial statements. Materiality includes consideration of both quantitative and qualitative factors.13

— Quantitative factors relate to whether misstatements or potential misstatements that would be missed by ICOFR, 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.

Magnitude of the Potential Misstatement and Likelihood (Reasonable Possibility)

[11.4.90] The severity of a control deficiency is a factor of both its potential magnitude and likelihood of resulting in a material misstatement. In other words, a deficiency is considered a material weakness when it has both the potential to result in a material misstatement and the likelihood is at least reasonably possible for it to result in a material misstatement.

[11.4.100] When evaluating the potential magnitude and likelihood of identified deficiencies, consider not only the actual amount of the misstatement, but also its potential magnitude. The actual misstatement only represents the “floor”; the potential magnitude could be much larger. Evaluating the magnitude of the potential misstatement can be challenging. Keep the following in mind:

— When evaluating the severity, it is the potential for misstatement, not the actual misstatement, or lack thereof, that is key to determining the magnitude of the deficiency.

— 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 (e.g., 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:

a. Financial statement amounts or total of transactions exposed to the deficiency, and

b. 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.

[11.4.110] Assessing potential magnitude involves projecting what could happen in the future if a control deficiency results in a misstatement remaining undetected. For instance, an account balance subject to a deficient control has gradually increased each year as the entity grows in size. The projected continued growth in that account balance in the future should be taken into account when assessing whether the potential magnitude of the deficient control is material. Judgment will be required when making these assessments, including the amount of weight given to past experience with an account that is objective and verifiable compared to projections in the account that are inherently more subjective.

12 Brian T. Croteau (December 2015), SEC Deputy Chief Accountant, Remarks before the 2015 AICPA Conference on Current SEC and PCAOB Developments

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 sentiments. Further, remedial actions taken in response to the control deficiency after the assessment date do not have an impact on potential magnitude.

The severity of the deficiency also depends on the likelihood—that is, 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 mean a misstatement actually occurred. Reasonable possibility means more than a remote possibility (a low threshold).

Risk factors affect whether there is a reasonable possibility that a deficiency, or a combination of deficiencies, will result in a 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 (see section 11.5).
— The interaction of the deficiencies (see section 11.6).
— The possible future consequences of the deficiency.
— The cause and frequency of exceptions detected as a result of the deficiencies.

**Illustration 11.13:**
Evaluating the severity of a deficiency

**Scenario:**
An entity overstates a legal accrual by $2 million. The deficient control is identified before determining its severity. In this case, the control deficiency relates to control design—specifically, the legal department did not inform the finance department of a positive development surrounding a particular legal matter. 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 legal department thought it was being “conservative.” The entity has several legal matters outstanding with a total legal accrual of $15 million.

**In evaluating the severity of this deficiency:**
The “floor” of the potential magnitude is the actual $2 million overstatement. The potential magnitude, or “ceiling,” would only be evaluated for overstatements, because there is evidence that the control is operating effectively for upward adjustments to the legal accrual. If there is not enough evidence to suggest that the controls are operating in a manner to properly and timely record increases in the legal accrual, we would consider both the possibilities of overstatements and understatements.
The evaluation 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. Use judgment 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 say that 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. This ratio of matters close to settlement compared to those not close to settlement is typical for the entity. The other $4 million of accrual is management’s best estimate of probable loss, but the matters are not close to being resolved and no settlement offers have been made. In such a scenario, the likely potential magnitude may be closer to $4 million than $15 million.

If it is determined that the deficiency affects more than just the legal accrual—e.g., the same issues could exist with respect to similar accruals—then consider that the potential magnitude of the error would extend beyond just the legal accrual.

Illustration 11.14:
Evaluating the severity of a deficiency

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 in 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 and no other judgmental accruals rely on underlying data that is manually modified after being extracted from the ERP system. 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.

Evaluating the severity of the deficiency:
The “floor” of the 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 could result in either an overstatement or understatement of the balance. Because of that 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 in this case an amount greater than the $1 million actual misstatement. That assessment 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. Because the Controller’s review over the warranty accrual was otherwise designed and operating effectively, with the exception of the completeness and accuracy of the underlying data, it is reasonable to expect that as the size of the misstatement increases, the Controller will eventually detect the error irrespective of the issues in the underlying claim data. We should consider at what dollar threshold it becomes remote that an error would not be identified through the Controller’s review, despite the deficient controls over the underlying data, and whether that amount is greater than an amount considered material to users of the financial statements.

Illustration 11.15:
Evaluating the severity of a deficiency

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 the 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 department, which were not complemented 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 internal control over financial reporting.

The entity’s CEO and CFO, while aware of the stress put on the accounting and financial reporting department, 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 ICOFR. This conclusion was reached, in part, based on the absence of any actual identified misstatements in the company’s financial statements during this period.

Subsequently, material errors in the company’s financial statements were identified related to certain more complex and judgmental areas of the financial statements. Upon completion of its root cause analysis, management determined the errors were a result of their lack of sufficient, qualified personnel to design and manage an effective control environment. The entity restated its prior year financial statements as a result of the errors.

**Evaluating the severity of the deficiency:**

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 was evidence supporting that the potential magnitude of the deficiency was not material.

Management did not appropriately apply the deficiency evaluation guidance contained in the SEC’s 2007 Management Guidance because it failed to evaluate the control deficiency absent a misstatement to the financial statements. As result, management failed to fulfill its obligations under SEC Rule 13a-15(c).

**Significant deficiencies**

Even if the deficiency is not a material weakness, it may be a significant deficiency. Whether a deficiency is important enough to merit attention by those responsible for oversight of the entity’s financial reporting is a matter of professional judgment. In some cases, those responsible for oversight of the entity’s financial reporting may want to be informed of deficiencies that otherwise would not be expected to be communicated. Factors to consider might include whether those responsible for oversight of the entity’s financial reporting process:

- Have quantified a minimum potential magnitude for communication and whether a lower threshold applies to certain significant accounts, disclosures and relevant assertions or certain locations;
- Wish to be told about deficiencies in a specific area; or
- Wish to be informed of any process with a cumulative number of deficiencies (for example, if greater than 5 deficiencies exist in any single process).

[11.4.170] Discuss the criteria used to evaluate whether a deficiency is significant with those responsible for oversight of the entity’s financial reporting.

[11.4.180] As discussed further in section 11.6, similar deficiencies are aggregated for analysis. Therefore, while a deficiency may be less severe than a material weakness individually, an evaluation of similar deficiencies in aggregate may indicate a material weakness exists.

[11.4.190] As noted in paragraph 11.8.30, management is required to report in writing all significant deficiencies and material weaknesses to those charged with governance and to the external auditors.

**Pervasive Controls**

[11.4.200] Pervasive controls, such as higher-level controls, entity-level controls and GITCs, operate over multiple processes. They vary in nature and precision and may eliminate or reduce the need to evaluate process-level controls depending on their level of precision. When deficiencies in pervasive controls are evaluated, the key is to determine which process-level assertions could be affected. The rest of the evaluation process is similar to evaluating individual or aggregated process-level deficiencies. Given the nature of deficiencies in pervasive controls, the magnitude of the potential misstatement is likely to be material. Therefore, it is important to understand whether there are appropriate compensating controls that operate at the right level of precision for each assertion impacted by the deficient pervasive control.

[11.4.210] If pervasive control deficiencies are found (e.g., the entity does not have sufficiently qualified personnel in key financial reporting positions), evaluate them using Appendix 11.3: Flowchart for Evaluating Deficiencies in Pervasive Controls.

**Illustration 11.16:**

**Evaluating the severity of a deficiency of a pervasive control**

**Scenario:**

While testing entity-level controls, Internal Audit identifies a deficiency in the entity’s control environment related to attracting, developing or retaining competent people. Consider the following:

1. Understand the root cause of the deficiency to be able to identify potentially affected process-level controls.
   - Has the entity shown a commitment to hiring people with necessary skill sets based on the entity’s transactions?
   - Does the entity adequately train their staff on new accounting pronouncements?
   - Do the entity’s personnel have the right skill set to identify significant, unusual transactions?
   - Which relevant assertions in the entity’s financial statements are associated with the root cause;

2. Determine whether there are other controls performed by management that meet the same objective that the deficient pervasive control was intended to meet. For example, if the entity doesn’t have a robust process to hire appropriate personnel, but they ensure that all employees receive adequate training once they are hired and their performance is closely monitored, the deficiency may not have an impact on the process-level controls.
3. Obtain more persuasive evidence for the design and operating effectiveness of such controls (e.g., reperform the control in addition to observing the control being performed); and

4. Determine whether there are specific deficient control activities that indicate the entity’s personnel are not sufficiently competent. Evaluate the severity of those deficiencies individually, in addition to this pervasive control deficiency.

5. Determine the severity of the deficiency in the pervasive control based on the aggregate severity of all of the individual control deficiencies that arose because of the ELC deficiency.

In some cases, the deficiency may not be identified in the initial testing of the control environment. Instead the issue may by identified by testing of control activities, which causes reconsideration of whether the initial assessment of the control environment was appropriate. In either case, perform a root cause analysis, identify potentially impacted process-level controls, reassess the methods of testing those controls, and determine if there are similar deficiencies in other controls.

[11.4.220] Evaluate deficiencies in GITCs with the help of Appendix 11.4: Flowchart for Evaluating GITC Deficiencies. More guidance for evaluating the severity of GITC deficiencies can be found in Chapter 8 of this Guide. When considering the impact of a GITC deficiency, identify which application controls are impacted and evaluate the severity of each application control individually. The severity of the GITC deficiency is an aggregation of the severity of the application control deficiencies.

Prudent Official

[11.4.230] The SEC Staff also requires that an evaluator think about the deficiencies in a holistic manner by applying the prudent official test. When evaluating the significance of a deficiency, evaluators are to step back and consider whether a prudent official with the same knowledge of the situation would agree with our classification of the deficiency. The prudent official test is meant to be performed with the “big picture” in mind.

Offsetting

[11.4.240] When evaluating the significance of potential misstatements resulting from a failure in the design or operating effectiveness of an internal control, consider the impact on related accounts and disclosures. For example, a deficiency in a key control affecting sales transaction processing would result in misstatements in revenue, cost of sales, inventory, sales commissions, royalties and income taxes. Some of the errors produce offsetting effects on net income. Factor in offsetting effects when evaluating the severity of the deficiency only if the offsetting transaction always occurs. Offsetting should not be applied if there is the intention that an offsetting transaction should occur, but the accounting system and controls are not designed and operating to ensure that such offsetting occurs.

Indirect Effects

[11.4.250] It is also important to consider the indirect effects of a misstatement. For example, the level of revenues might impact compliance with debt covenants, the calculation of an earn-out on a business combination, or attaining a performance-based stock award or bonus program. Each of these could affect the evaluation of the severity of a deficiency.

---

Key takeaways:

Step 4: Evaluate the severity of the deficiency by considering the magnitude and likelihood of the potential misstatement

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 remote*

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 most cases, the *magnitude of the potential misstatement is greater than the floor.*

3. **Material weaknesses can and do exist in the absence of a misstatement to the financial statements.**

4. 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 remedial actions taken after the assessment date.

5. **Use the flowcharts** in the appendices to guide you through the steps of determining the severity of the deficiency, especially when the deficiency is pervasive.

6. As part of our severity assessment, **consider the control’s objective** (i.e., the WCGW that the control was purported to address) and how that control relates to the entire process and relevant financial statement assertions.
When a deficient control is identified and the severity (potential magnitude and likelihood) of the deficient control is material, determine whether there are any compensating controls. A compensating control may limit the severity of the deficient control but does not eliminate the deficiency. Controls that compensate for deficiencies, including deficiencies in IT general controls, should be precise enough to prevent or detect a misstatement that could be material. However, they do not need to be so precise as the original control.

When evaluating whether the compensating controls mitigate either the likelihood or the magnitude of the potential misstatement, consider:

— If any compensating controls mitigate the severity of the deficiency for the affected period, those compensating controls should be tested for that period.

— To be effective, compensating controls need to achieve the same objective as the deficient control, meaning they need to address the same WCGW to the relevant financial statement assertions as the original control.

— Compensating controls cannot lower the potential misstatement below the actual known misstatement, or the “floor,” for purposes of evaluating the severity of a deficiency.

— The precision at which the compensating controls operate is an important factor. See Chapter 7 in this guide for more discussion on precision of management review controls. The requirements for precision in a compensating control are the same as those addressed in that chapter.

— High-level analytical procedures and other monitoring controls usually do not constitute effective compensating controls to mitigate the effect of an identified deficiency. See Chapter 7 in this guide, for more discussion on management review controls.

Consideration of the design and precision of high-level analytical procedures and other monitoring controls is particularly important. The assertion that these monitoring controls usually do not constitute effective compensating controls is consistent with the COSO Framework, which states that, “while higher-level controls are important...it is difficult to fully and efficiently address business process risks without [effective] transaction controls.”

Illustration 11.17:
Do compensating controls operate at the correct precision?

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.
- A final review of the financial statements by the CEO and Audit Committee.

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. This CFO review of the financial statements was a control identified and tested by management (i.e., it is inappropriate to rely upon a control that has not been tested). 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 review control functioned as a monitoring control, or as more of an operational review for purposes of evaluating the propriety of 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 the similar reasons. Therefore, final reviews are not compensating controls that can reduce the severity of an identified deficiency.

[11.5.40] As the potential magnitude of the deficiency and the mitigating impact of any compensating controls are contemplated, consider

- The control’s objective—the WCGW and related financial statement assertion;
- The control’s importance in achieving its objective—whether compensating controls achieve the same objective; and
- The precision at which the compensating control operates.
Scenario:
A deficiency in GITCs over the revenue application is identified such that reliance on any of the application controls related to 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 A/R subledger, and a management review control where the CFO reviews the financial statements for existence, completeness and accuracy of revenue.

The subledger to general ledger reconciliation is an important control, but it does not provide any evidence over the existence, completeness and accuracy of revenue recorded in the subledger. Rather, the reconciliation only provides evidence over the propriety of reconciling items between the subledger and the general ledger.

The reconciliation of cash receipts to the A/R subledger does not provide direct evidence over the existence, completeness and accuracy of revenue and therefore this control does 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 revenue application controls, but we need to be careful about whether it provides sufficient evidence at an appropriate level of precision. Further, the CFO’s review may not be designed to meet all of the same objectives as the revenue application controls, including fraud risks. It would be necessary to evaluate the severity of the GITC deficiency by considering the potential magnitude of all controls affected by the GITC deficiency in the aggregate.

Illustration 11.18:
Do compensating controls achieve the same objective as the deficient control?

Compensating controls that may achieve the same objective:
— A few exceptions in the control over provisioning of access are identified. However, management also has a detective control—a quarterly review of access that includes determining whether anyone that had inappropriate access inappropriately used that access. This may be an effective compensating control.

— 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—management reviews the bank reconciliations using specified metrics and thresholds. All of the errors discovered were less than the specified metrics of management’s review control, and the review control is tested and determined that the design, including the precision with which it operates, is appropriate to detect or prevent a material misstatement. This may be an effective compensating control.
Step 5: Identify relevant compensating controls and conclude on the severity

1. Remember: to have a mitigating effect, the compensating control should operate at a level of precision that would prevent or detect a material misstatement of the account assertions impacted 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. Management representations regarding the design and operating effectiveness of a compensating control do not constitute sufficient evidence.

4. Consider whether the compensating control meets the same control objective (i.e., it addresses the same WCGW) as the deficient control.

5. Remember: a compensating control does not have to operate at the same level of precision but must be able to detect a material misstatement.
After evaluating individual deficiencies for severity, we determine whether individual control deficiencies that affect the same significant account or disclosure, relevant assertion, principle or component of internal control, in combination, result in a material weakness or significant deficiency. Deficiencies with other commonalities, such as controls that arise in a common component or location, or in a group or multilocation audit, may need to be aggregated as well.

The requirement to aggregate deficiencies was established to evaluate the “big picture” as it relates to deficiencies. An evaluator takes a step back from the individual deficiencies to determine the potential impact of the combination of similar deficiencies.

One method of addressing the “big picture” scenario that may be helpful is to think about aggregated deficiencies not only in terms of which controls are deficient, but also which relevant controls related to a significant account or assertion are effective and whether having just those effective controls is sufficient to detect or prevent a material weakness.

Additionally, performing an effective root cause analysis is important to the aggregation assessment. Performing a root cause analysis, as discussed in section 11.2, should be focused on understanding why the deficiency occurred, including which COSO components were deficient and which significant accounts were impacted.

Illustration 11.20:
Importance of a root cause analysis

Recall Illustration 11.5 where errors were discovered in a spreadsheet. Our root cause analysis led us to conclude that management’s risk assessment process, specifically principle 7, was deficient.

To the extent that this was the only issue noted related to principle 7 of risk assessment, the impact of that deficiency would be limited to the controls that used IPE. However, if we identify other deficiencies that also have a root cause in a deficient risk assessment process, we would aggregate the impact of those deficiencies as well to determine if the lack of an appropriate risk assessment process could have caused a material misstatement.

As we aggregate the potential magnitude of each individual deficiency caused by the deficient risk assessment process, we determine whether the potential magnitude of the aggregated risk assessment deficiency could have been material.

The aggregation exercise is only as good as our root cause analysis and only as good as our ability to analyze the “big picture” of all related deficiencies.

Similar to when evaluating the severity of individual deficiencies, an evaluator should apply the prudent official test when aggregating deficiencies. Remember, the prudent official test is meant to be performed with the “big picture” in mind.

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 580828265 Chapter 11 – Identifying and Evaluating Deficiencies
Illustration 11.21:
Applying the prudent official test

Scenario:
Several deficiencies related to revenue have been identified. Individually, the deficiencies do not rise to the level of material weakness. When we aggregate all of the individual deficiencies, the aggregated potential magnitude is just below what we would consider to be material. However, as we apply the prudent official test, we realize that:

— Revenue is the key account discussed with and monitored by analysts.
— Movements in revenue drive the stock price.
— Four of the eight controls related to revenue were deemed to be deficient.
— While our analysis shows that the aggregated potential magnitude is just below what we would consider to be material, there is subjectivity in the analysis and another evaluator may conclude that the aggregated potential magnitude is material.

It is likely that a prudent official would evaluate these facts and determine that the deficiency is a material weakness.

[11.6.60] In some cases, the absolute value of all of the audit differences identified by an external auditor is close to what management and the auditor might consider material. A proper aggregation analysis, including the prudent official test, is particularly important in these scenarios because the actual audit differences are close to materiality, but the potential magnitude for misstatement is almost certainly higher than the actual misstatements. In the absence of compelling audit evidence to the contrary, a prudent official may find it difficult to conclude that a material weakness does not exist.
Scenario:
A root cause analysis reveals three deficiencies with the potential to impact the income tax account, plus two additional deficiencies that relate to the information and communications component, specifically COSO principle 13. None of the deficiencies was, individually, considered a material weakness.

The potential magnitude of the aggregated impact of the three income tax deficiencies is evaluated. Each one was determined to be approximately half of what we would consider to be a material error. None of the deficiencies would qualify to offset the others—in other words, all three deficiencies could all 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 and therefore a material weakness exists.

Further, the potential magnitude of the two deficiencies related to information and communication is evaluated. The potential magnitude of each deficiency was determined to be approximately 25 percent of what we would consider to be material. As we aggregate the deficiencies within the information and communication component, they do not rise to the level of a material weakness, and we believe that a prudent official would reach the same conclusion. However, in aggregate, we believe that this is an issue that those responsible for oversight of the entity’s financial reporting process should be informed about and therefore determine that a significant deficiency existed in the aggregate.

Key takeaways:
Step 6: Aggregate similar deficiencies and evaluate the aggregated deficiencies for severity

1. **Look for commonalities** when determining how to aggregate deficiencies.

2. At a minimum, aggregate deficiencies related to the same financial statement account, disclosure or assertion and COSO component/principle. Other aggregation criteria may be considered based on the commonalities identified.

3. While analyzing the aggregation of deficiencies, consider the “big picture” – what controls within the process are deficient, which ones are effective, and whether a prudent official would reach the same conclusion.
Background:
As a result of substantive test work, the external auditor identifies an audit difference related to a tranche of options issued to a nonemployee. Because the award is expected to be settled in cash, it should be treated as a liability. However, management treated the tranche of options as an equity-classified award.

As a liability, the award would be re-measured to fair value at each balance sheet date until it is settled. If management had appropriately remeasured the award at period end, it would have recognized an additional $500,000 of expense in the current year. A misstatement of $1.5 million would be material.

The initial accounting for the nonemployee award was determined in a prior fiscal year by previous management. Key members of the entity’s accounting/finance function (CFO, Controller, Accounting Managers) have been with the entity less than 1.5 years.

The entity never cash settles its awards when issuing share-based awards to its employees. It is not allowed by the plan.

The entity has no history of issuing awards to non-employees except for this one grant. The nonemployee awards were issued in connection with a business combination.

No awards have been granted to nonemployees since the acquisition and there are no plans or discussion at the board level for future nonemployee awards.

With the exception of this issue, the entity has properly accounted for share-based awards, such as stock option modifications and performance awards that include adjustments to milestone achievement and vesting performance conditions.

Step 1: Determining whether a deficiency exists
Even though the tranche of options that caused the error was granted under a previous management regime and in a prior fiscal year, that transaction has a continuing impact on the financial statements that were produced by current management. The error is the result of a deficiency.

Step 2: Identify the control that is deficient
Questions to identify the deficient control include:

— What control failed under previous management to allow the error to first occur?

— Does evidence show that the same deficiency no longer exists?

— Was management aware of the unusual grant and just reached an incorrect accounting conclusion? If so, who reviewed the accounting treatment and does that person have the right skill set to make that determination?

— Was management unaware of the unusual grant, and if so, why? Was there a missing control? Was there a deficiency in the control design? Was there a deficiency in the operating effectiveness of a properly designed control?

Assume there is evidence that current management has well designed controls that govern the issuance of new option grants, including classification. However, in its efforts to get up to speed, management did not revisit certain accounting decisions made under previous management that had a continuing impact on the financial statements. Based on this root cause analysis, an evaluator concluded that the deficiency is that current management lacks a control to evaluate legacy accounting positions with continuing financial statement relevance.
As this root cause analysis is performed, continued weaknesses in the entity’s controls around the issuance of new option grants may be evident. In such a case, the deficient control is likely different from the one identified in the previous paragraph (or there may be multiple deficiencies, including the one identified in the previous paragraph). This means that the total population of transactions subject to misstatement is larger than just the unusual grant, and therefore the potential misstatement is likely to be more significant.

**Step 3: Determine whether the control deficiency is indicative of other deficiencies**

It is determined that the missing control is related to the risk assessment component, because management’s risk assessment process failed to identify this legacy accounting issue. In determining whether the control deficiency indicates other deficiencies, attention is focused primarily on whether this deficiency in risk assessment was limited to share-based payments or whether there were other legacy issues that may not have been considered.

As the issue is further examined, it is learned that prior management had established several accruals that were individually immaterial which had not been evaluated for propriety. Management is of the view that the propriety of these legacy accruals would have been subject to the same type of control that was deficient related to stock compensation.

**Step 4: Evaluate the severity of the deficiency by considering magnitude and likelihood of the potential misstatement**

There is a choice—but either approach will ultimately result in the same analysis. We can identify two separate deficiencies (one related to stock options, the other to the accruals), separately determine the potential impact (step 4), evaluate for compensating controls (step 5), and then determine the aggregate impact of the two deficiencies (step 6). Alternatively, we can identify one deficiency and follow steps 4, 5 and 6. Either approach is acceptable. For the purposes of this example, we will treat them as two separate deficiencies.

For purposes of this example, only the evaluation of the deficiency related to stock options will be discussed. A complete analysis also would require the evaluation of the potential magnitude and likelihood of the misstatement related to the accruals caused by the control deficiency or deficiencies.

Determining the potential magnitude is often tricky. It is generally higher, and never lower, than the actual error. Because the liability amount is driven by the stock price, the following are likely to be important:

- Current-year high stock price
- Stock volatility
- Analyst stock price targets

It is important to assess how significant the misstatement could have been in the current year and how significant the misstatement could be in future periods because, without the auditor having detected the misstatement, the error could have continued until the options were settled. Thus if there is a reasonable possibility that the stock price could be higher in future periods, the impact to future periods may be more material than the current period impact.
**Step 5: Identify relevant compensating controls and conclude on the severity**

In evaluating the matter, the entity points to the CFO's review of the financial statements as a compensating control that would have limited the potential misstatement. However, because of the nature of the deficiency and how the error arose—they were not expecting any effect on the relevant expense account associated with the change in fair value, and the financial statements did not reflect any recorded effect to the relevant expense account—management’s review would not have detected any misstatement related to this deficiency, regardless of the magnitude.

No other compensating controls were identified. Therefore, the potential magnitude determined in step 4 was compared to materiality to determine if a material weakness existed. After careful evaluation of the prospective likelihood of a material misstatement related to stock options, management assessed the potential magnitude as immaterial, but still significant enough to warrant the attention of the audit committee. It was therefore determined to be a significant deficiency.

**Step 6: Aggregate similar deficiencies and evaluate the aggregated deficiencies for severity**

While the individual deficiency did not constitute a material weakness, an assessment was made regarding whether the deficiency should be aggregated and evaluated with other deficiencies. While there were no other deficiencies related to stock option accounting or equity, the root cause analysis in step 3 led management to conclude that there was a similar deficiency in the component of risk assessment related to legacy accruals.

Management evaluated this deficiency (steps 4 and 5, but not illustrated in this Guide), and noted that it represented a significant deficiency. However, when aggregating the two similar deficiencies, the potential magnitude of the misstatements was deemed material and therefore was determined to aggregate to a material weakness.
Deficiencies in Service Organization Reports

[11.8.10] As part of risk assessment, the COSO Framework requires an identification of controls at a service organization that are relevant to the entity’s ICOFR. Often a SOC 1 report (Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization) covers more controls than an entity may rely on. If there is a deficiency in a control at the service provider on which the entity is relying for ICOFR, even if did not cause a qualification in the service auditor’s report, the deficiency should be evaluated for severity.

[11.8.20] Service organizations often process large volumes of transactions, such as payroll, and use automated controls to mitigate related risks. In situations where deficiencies relate to general IT controls, it is important to consider the pervasive nature of those controls and which automated controls the service organization was relying on.

Often the service organization’s SOC 1 report will provide information to help management understand the impact of deficiencies at the service organization. Because an entity may only rely on the service organization for some services as opposed to all services that are offered by the service organization, the lack of a material weakness at the service organization may not be conclusive for management’s purposes – management may need to evaluate how the deficiency at the service organization impacts the service organization’s controls that the entity is relying on for its ICOFR.

Communication Requirements

[11.8.30] The registrant’s certifying officers attest to the fact that all significant deficiencies and material weaknesses have been communicated to the external auditors and to the audit committee.

[11.8.40] External auditors also have requirements to communicate material weaknesses and significant deficiencies on a timely basis to management and to the audit committee in writing before issuing the audit report. All other deficiencies are communicated in writing, at a minimum, to management.

Additional Resources for Identifying and Evaluating Deficiencies

[11.8.50] The following are additional resources that may be helpful in identifying and evaluating deficiencies ICOFR:

- Auditing Standard No. 5, An Audit of Internal Control Over Financial Reporting That is Integrated With An Audit of Financial Statements
- SEC’s Division of Corporation Finance Financial Reporting Manual, Section 4300
- COSO Internal Control Over External Financial Reporting: Compendium of Approaches and Examples (May 2013)
- COSO Internal Control over Financial Reporting—Guidance for Smaller Public Entities (June 2006)
[11.9.10] Management’s annual report on ICOFR must state or disclose the following:18

— Management’s responsibility for establishing and maintaining adequate ICOFR for the entity.
— Management’s criteria for evaluating the effectiveness of ICOFR.
— Management’s assessment of the effectiveness of the entity’s ICOFR at year end, including a statement saying whether or not ICOFR is effective.
— Any material weaknesses in the entity’s ICOFR identified by management.
— 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 ICOFR (if applicable).

[11.9.20] Management must decide if ICOFR is effective or not effective.19

— Management cannot conclude that its ICOFR is effective if there are one or more material weaknesses.
— Management cannot qualify its conclusion by stating that its ICOFR is effective with certain qualifications or exceptions.
— Management may state that its controls are ineffective for specific reasons.
— Because of the substantial overlap between ICOFR and Disclosure Controls and Procedures (DCP), if management concludes that ICOFR is ineffective, it must also consider the impact of the material weakness on its conclusions related to DCP. (This has been interpreted to mean that DCP is also ineffective when ICOFR is ineffective).

[11.9.30] Management must communicate all significant deficiencies and material weaknesses it detects to the audit committee and external auditor. The Sarbanes-Oxley section 302 certifications include an affirmative statement to this effect. Management must also provide written representations to the auditor regarding its internal controls.20 [11.9.40] If an entity’s management concludes that its original assessment of ICOFR was incorrect, it should consider whether or not to revise its original report on ICOFR. An 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 were 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 were not effective, and the reasons why.21
Management should consider disclosing the following with respect to a Material Weakness:

— Describe the nature of the material weakness;
— Describe its impact on the financial reporting and ICOFR, if any; and
— Describe current plans or action already undertaken, if any, for remediating the material weakness.

Although each of these is described in Item 9A, management’s plans are discussed separately from the description of the nature of the material weakness and the impact on the financial reporting and ICOFR because the auditor’s report on ICOFR does not extend to management’s plans. If they are not discussed separately, the auditor’s report on ICOFR should include a disclaimer on management’s plans.

Illustration 11.23:
Example 1 of Item 9A Disclosure

Example Item 9A Material Weakness Disclosures

Management has concluded that a material weakness in its internal control over financial reporting existed as of December 31, 20XX in that the Company did not maintain an effective control environment. Specifically, the operators of review controls over accounting for certain derivative financial instruments pursuant to the provisions of FASB ASC Topic 815, Derivatives and Hedging (ASC Topic 815) did not have sufficient technical expertise to review certain derivative financial instruments transactions (both at inception and during periods subsequent to inception).

The material weakness resulted in material misstatements in the current period. These misstatements were corrected before issuing the financial statements as the entity determined that the hedge accounting treatment applied to interest rate swaps on portions of its variable rate debt, an interest rate cap on variable rate debt, an interest rate swap on fixed rate subordinated debt, and certain interest rate swaps related to specific fixed rate commercial loans were not consistent with the provisions of ASC Topic 815.

To assess internal control over financial reporting, management used the criteria set forth by the Committee of Sponsoring Organizations of the Treadway Commission’s 2013 Framework. Because of the material weaknesses described above, management concluded that, as of December 31, 20XX, the Entity’s internal control over financial reporting was not effective.

22 See FRM 4310.12
Illustration 11.24:
Example 2 of Item 9A Disclosure

In connection with management’s assessment of internal control over financial reporting as of December 31, 20XX, a deficiency was identified in our internal control over financial reporting related to our control environment that was deemed to be a material weakness, as described below:

The entity requires management to review the accounting for significant non-routine and complex transactions to ensure proper application of generally accepted accounting principles. This control did not operate effectively because there weren’t enough qualified people both to account for the transactions and perform the required management review.

As a result, the entity:
- Overstated certain international assets and understated impairment expense for those assets;
- Overstated the write-off of certain programming license fees and overstated the programming license fee payable; and
- Understated the write-off of deferred financing fees and overstated other assets as of and for the year ended December 31, 20XX. This deficiency caused material misstatements in the annual and interim periods, which management corrected before issuing the December 31, 20XX consolidated financial statements.

In assessing internal control over financial reporting, management used the criteria set forth by the Committee of Sponsoring Organizations of the Treadway Commission’s 2013 Framework. Because of the material weakness described above, management concluded that, as of December 31, 20XX, the entity’s internal control over financial reporting was not effective based on those criteria.

Illustration 11.25:
Example 3 of Item 9A Disclosure

As a result of its assessment, the entity identified the following material weaknesses in internal control over financial reporting as of December 31, 20XX:

The entity’s controls were not sufficiently complete and comprehensive to ensure that reconciliations of the differences between the tax basis and book basis of each component of the entity’s deferred tax asset and liability accounts were performed timely and accurately. Specifically:
- There was a lack of segregation of duties; and
- There was inadequate and ineffective analysis and management review of the relevant documentation supporting the deferred tax asset and liability accounts.
What to Disclose in Subsequent Periods

[11.9.70] 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 ICOFR in Item 4 on Form 10-Q. Material changes include both positive and negative developments. Therefore, if management has implemented changes to ICOFR to remediate the material weakness, it should disclose those changes.

[11.9.80] Before 2007, management was required to disclose significant changes to ICOFR in Item 4 (e.g., management may have disclosed changes to ICOFR related to remediating significant deficiencies). The rule was changed to require disclosure of material changes. Changes to ICOFR in response to previously identified significant deficiencies are not likely to meet the material disclosure threshold, although management may elect to disclose more than is required.

[11.9.90] Management may wish to also disclose in an interim filing that the material changes have remediated the material weakness. Management should carefully consider whether to do so, because:

— In general, new controls need to be operating for a sufficient period of time to 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 10-K contains the same material weakness because, after the external auditor has performed the audit, it is determined that the material weakness still exists.

[11.9.100] 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 such controls.
[11.10.10] 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.

[11.10.20] 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 or not 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 because material changes in ICOFR need to be disclosed in an interim filing with the SEC.

[11.10.30] 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 whether the circumstances that gave rise to the material weakness also existed as of the date of the previously issued financial statements. (Also see the section titled “Reporting Considerations in Item 4 on Form 10-Q” below.)

Evaluation Against Interim Financial Statements

[11.10.40] A known misstatement to an interim period is evaluated against the financial results of the interim period for purposes of assessing the severity of the underlying control deficiency.

[11.10.50] Similarly, 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, the deficient controls related to the interim tax provision are different than those over the annual provision and operate at a level that is less precise than the annual provision controls. The annual tax provision controls are 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.

[11.10.60] However, if the deficient control is designed to operate continuously throughout the year, the evaluation assumes the deficiency could result in misstatement equally throughout the year (divide the potential magnitude by four and compare to the average quarterly materiality thresholds).

[11.10.70] If the deficient control is designed to operate at a point in time, evaluate it in relation to the interim financial results for the quarterly period(s) in which the deficiency existed (potential magnitude is compared to the average quarterly materiality thresholds).

Reporting Considerations in Item 4 on Form 10-Q

[11.10.80] SEC rules require that management evaluate the effectiveness of Disclosure Controls and Procedures (DCP) on a quarterly basis.

[11.10.90] There is no requirement for management to perform a full ICOFR evaluation at interim periods. Instead, SEC rules require that “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.” (SEC Release No. 33-8238; emphasis added.)
[11.10.100] The SEC states: “although 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.” (SEC Release No. 33-8238).

[11.10.110] 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 would disclose a material weakness in Item 9 on Form 10-K (see section 11.9 in this chapter).

[11.10.120] Management should conclude that DCP is ineffective because ICOFR is generally a subset of DCP.

[11.10.130] The material weakness ordinarily is described in the disclosure about ineffective DCP because there is no requirement for management to perform an ICOFR evaluation at an interim date.

[11.10.140] 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.

[11.10.150] As discussed in 11.9.90, sometimes entities wish to disclose in Item 4 on Form 10-Q that the material weakness has been remediated. Entities should use caution about making such assertions as the external auditors are not likely to be in a position 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 to later conclude upon audit that the material weakness still exists.

[11.10.160] In certain situations, a material weakness is identified and remediated within the same interim period. Because the material weakness was remediated prior 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 fourth quarter). If a material weakness was remediated prior to 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 ICOFR as discussed above. The remediation of a material weakness within an interim period would most likely constitute a material change in ICOFR.

[11.10.170] Management should also consider whether that material weakness existed in previous periods, the related impact 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 ICOFR.
Appendix 11.1: Flowchart for Identifying Deficiencies
Appendix 11.2: Flowchart for Evaluating Deficiencies in Direct Controls
Appendix 11.3: Flowchart for Evaluating Deficiencies in Pervasive Controls
Appendix 11.4: Flowchart for Evaluating GiTC Deficiencies
Appendix 11.5: Summary of Internal Control Deficiencies (SICD) Template
Appendix 11.6: Internal Control Deficiency Evaluation Template
Appendix 11.7
  11.7a: Summary of Internal Control Deficiencies Template – Completed Examples
  11.7b: Internal Control Deficiency Evaluation Template – Example 1
  11.7c: Internal Control Deficiency Evaluation Template – Example 2
Appendix 11.8: Guide to Understanding the Flow of the Summary of Internal Control Deficiencies (SICD)