Avoiding Deficiencies in Peer Reviews: Focus on Engagement Quality

ENQ4/26/V1

201 N. King of Prussia Road
Suite 370
Radnor, PA 19087
P : (610) 688 4477
F : (610) 688 3977
info@surgent.com
surgentcpe.com

SURGENT
ContinuingEducation

Calling All **Exceptional**
INSTRUCTORS

Surgent is currently accepting nominations

for prospective new Discussion Leaders in the following areas:

Tax

Accounting & Audit

Gov't and Not-for-Profit A&A

Business and Industry
(all topics)

If you are an experienced CPA, have strong public speaking and teaching skills, and an interest in sharing your knowledge with your peers by teaching live seminars, we would love to hear from you!

Interested in becoming a Surgent discussion leader?

Reach out to us at
recruitment@surgent.com

SURGENT
ContinuingEducation

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

SURGENT FOR ENTERPRISE

Educational Solutions that Advance the Strategic Value of Everyone in Your Firm

At Surgent, we tailor our offerings—**exam review**, **continuing education**, and **staff training programs**—to meet your organization's specific needs in the most convenient and effective ways possible.

Personalized Exam Review

Help associates pass faster with the industry's most advanced exam review courses

- Adaptive study model offered for CPA, CMA, EA, CISA, CIA, and SIE exams
- Monitor employees' exam review progress with Firm360

Continuing Professional Education (CPE)

Make CPE easy for you and your staff with several ways to buy, earn and track CPE

- Flex Access Program – Secure a pool of CPE hours your staff can pull from in live webinar and/or self-study format
- Onsite Training – Reserve an in-firm training with a Surgent instructor
- Course licensing – License content from Surgent to lead your own CPE training

Staff Level Training

Leverage highly practical sessions, organized into suggested curricula according to staff experience levels

- Audit Skills Training Program
- Internal Audit Training Program
- Taxation Training Program

FIRM CPE PORTAL

Track and manage CPE for all users in your organization quickly and easily with Surgent's Firm CPE Portal.

Request a demo today!

Every firm is unique—and that is why we built our customizable, innovative Surgent for Enterprise program.

Contact our Firm Solutions team today to learn how Surgent can partner with you to create a solution to support staff development for your organization.

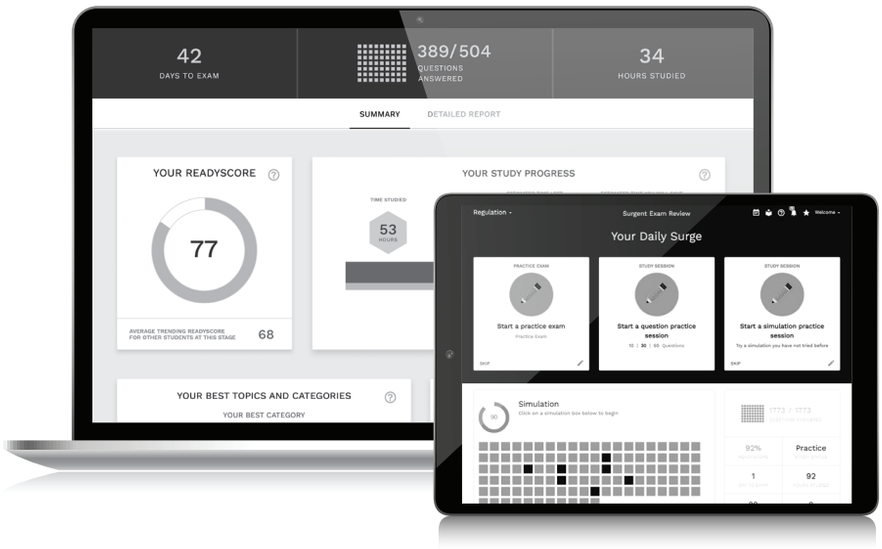
(484) 588.4197
salesinfo@surgent.com

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

STUDY LESS AND PASS FASTER

with the industry's most advanced exam prep courses

Surgent's AI-powered software personalizes study plans for each student, targeting knowledge gaps and optimizing those plans in real-time. This award-winning approach has been shown to save candidates hundreds of hours in study time.



KEY FEATURES

READYSCORE

Know what you're going to score before taking the exam.

PERFORMANCE REPORTS

Leverage your dashboard to know how you're doing every step of the way.

PASS GUARANTEE

If you fail your exam after using our course, we'll refund your money.

A.S.A.P Technology

helps you pass the

- **CPA** Exam
- **CMA** Exam
- **EA** Exam
- **CIA** Exam
- **CISA** Exam
- **SIE** Exam

Leading education for your firm? Surgent offers preferred partner pricing, coaching and more support methods to our firm clients and their staff. **Contact our Firms Solutions team today at salesinfo@surgent.com.**

Ready to explore exam prep course packages from Surgent? **Visit surgent.com to learn more!**

Table of Contents

Revised May 2026

NOTES

AICPA Focus on Audit Quality

AICPA Focus on Audit Quality

Learning objectives

Upon reviewing this chapter, the reader will be able to:

- Identify key elements of the AICPA's Enhancing Audit Quality initiatives;
- Recognize key trends noted in recent peer reviews; and
- Recognize the importance of audit documentation in the system of quality control.

I. AICPA's EAQ initiative

A. Brief history

Business and regulatory environments have evolved significantly over the years and are far more complex than they were when the peer review process began in 1988. As financial markets hold more risk it becomes increasingly important that the audit results accurately support the opinions rendered by CPAs. Accordingly, the AICPA is committed to assisting auditors to perform quality audits.

Tools, templates, and other resources are available on the AICPA website. A practitioner does not have to be an AICPA member to access many of these resources.

The AICPA prepares a work plan each year to enhance quality in the profession. They build their workplan from issues they see in inspections by peer reviewers and others as well as environmental drivers such as emerging technology, increasing complexity in business transactions, and complexity in financial reporting standards.

AICPA launched its Enhancing Audit Quality initiative in 2014. In January 2015, AICPA Peer Review Board approved changes to its Standards for Performing and Reporting on Peer Reviews with a focus on enhanced peer reviewer training. This was effective for peer reviews beginning on or after May 1, 2016.

The changes that were made to the Peer Review program focused on:

a. Resolving disagreements between CPA firms and reviewers;
b. Increasing the qualifications for a peer reviewer; and
c. Strengthening the consistency of peer review performance criteria to facilitate remediation or removal of deficient reviewers.

The AICPA has subject matter experts that perform peer review oversights to further enhance quality.

1. Peer review oversight

Realizing that peer reviewers were part of the problem, the AICPA created new training requirements and educational efforts to help reviewers improve. In addition, the AICPA instituted the Enhanced Oversight Program. In this program, reviewers evaluate the quality of work performed by peer reviewers as well as the firms they review. Oversight reviewers are subject matter experts who perform the reviews after the firm has been peer reviewed but before the peer review has been evaluated by the Peer Review Committee.

Enhanced oversight results indicate improvement in peer reviewer performance with reviewer detection rates of nonconforming engagements increasing since the enhanced oversight program began in 2014. The PRB's focus on oversight and reviewer education has led to significant improvements in peer reviewer performance, which ultimately resulted in improved firm performance and higher audit quality.

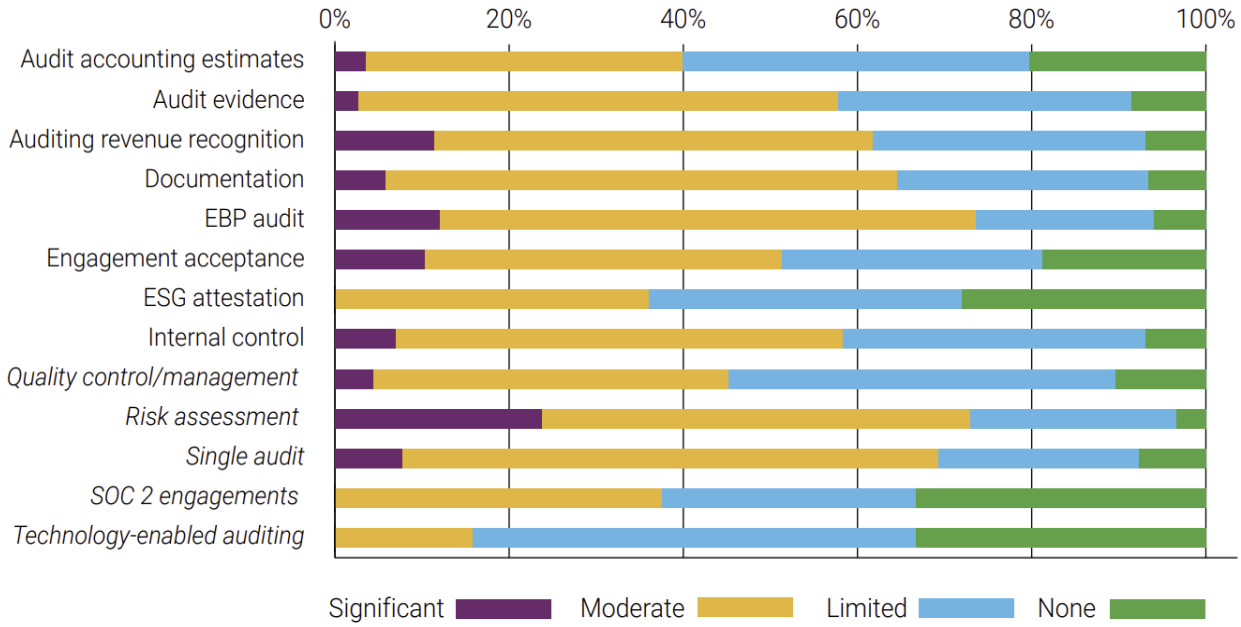
B. Quality is improving

Since that time, the AICPA has performed a number of focused studies, some involving surveys of its peer reviewers. Enhancing Audit Quality Initiative (EAQ) is a data driven approach to improving audit quality.

The AICPA:

a. Collects data from peer reviews and other reviews, for example, from regulatory agencies;
b. Analyzes the data to see where deficiencies are prevalent;
c. Studies emerging trends; and
d. Takes action to create articles, webcasts, tools, and other resources to help auditors improve.

The results of the most recent (2024) study are presented below. One hundred fifty peer reviewers responded to the survey and answered the question, "How much improvement have you noted in your peer review clients for these AICAP focus areas?"



As noted above, the AICPA has been steadily working to improve audit quality. In 2024 they reported the following results.

The AICPA's Focus for **2025** continues its attention to **risk assessment**, **quality management**, **technology-enabled auditing**, and **single audit**.

It adds one more area of focus:

a. **Emerging attestation engagements** – With all of the changes in the environment such as emerging business needs, regulatory changes, and stakeholder demands, including areas such as sustainability reporting, cybersecurity risk management, and AI governance, new and evolving assurance services where practitioners evaluate and report on subject matter other than historical financial statements will continue to evolve. AICPA stands ready to assist. The AICPA is watching and evaluating these opportunities for practitioners to do more but the evolving nature of risks requires information, education, and guidance.

Ongoing focus points are:

a. **Risk assessment (continued from 2024)** – SAS No. 145 has been effective for engagements with year-ends after December 15, 2023, and the EAQ will continue to provide implementation support. CPEA continues to issue high quality alerts.

b. **Quality management (continued from 2024)** – A firm's system of quality management was required to be operational by December 15, 2025. Firms will need to have completed a risk assessment and implemented the risk responses. The AICPA has developed practice aids, training, and support for practitioners in the form of tools, webcasts, and articles.

c. **Single audit (continued from 2024)** – There will be a continued increase in the number of practitioners needed to address the demand for single audit engagements, therefore, the AICPA will continue advocacy efforts to help ensure clear and timely guidance for practitioners.

C. Peer review, an integral part of EAQ

The AICPA's peer review program is an integral part of EAQ and perhaps its most important component. Firms (and individuals) enrolled in the peer review program have a peer review of their accounting and auditing practice every three years. This would include engagements that are performed under Statements on Auditing Standards (SAS), Statements on Standards for Accounting and Review Services (SSARS), Statements on Attestation Standards (SSAE), Government Auditing Standards (GAS), and Public Company Accounting Oversight Board (PCAOB) standards. Note that the AICPA does not require that a firm enroll in the Peer Review Program if the only service it performs is a preparation engagement under the SSARS, unless the firm has another licensing body that requires it.

To enhance audit quality the AICPA developed the Peer Review Oversight Program. Reviewers evaluate the quality of work performed by peer reviewers as well as the firms they review. Oversight reviewers are subject matter experts who perform the reviews after the firm has been peer reviewed but before the peer review has been evaluated by the Peer Review Committee. The AICPA requires that administering entities perform oversights on 2 percent of peer reviews.

There are 26 entities that administer the peer review program. The National Peer Review Committee (NPRC) is one of them. State CPA Societies can elect the level involvement they want in the peer review program.

The three options are:

a. Self-administer;
b. Arrange for another state CPA society or group of state societies to administer the Program for enrolled firms whose main offices are located in that state; or
c. Ask the AICPA to request another state CPA society to administer the Program for enrolled firms whose main offices are located in that state.

Firms can elect to have their peer review administered by the NPRC. In addition, firms are required to have their peer review administered by the NPRC if they are required to be registered with and inspected by the PCAOB or if they perform audits of non-SEC issuers pursuant to the standards of the PCAOB.

1. Overview of the peer review function

Before identifying deficiencies that have been found by peer reviewers, government agencies and others, it is helpful to have an overall understanding of the peer review function and the various levels of findings and reports that can be delivered as a result of a peer review.

There are two main types of peer reviews: the System Review and the Engagement Review. There is also another review called Quality Control Material (QCM) Review which deals with entities that provide QCM materials to firms. The System Review focuses on the firm's system of quality control and the Engagement Review focuses on specific engagements.

The guidance associated with performing and reporting on QCM reviews was eliminated from the clarified peer review standards effective for peer reviews commencing on or after May 1, 2022. It was eliminated because the guidance was not designed to address QCM made available through technology and IT applications as the technology either did not exist or was not extensively employed for QCM at the time. In addition, the Peer Review Board no longer believed it was appropriate for practitioners to perform QCM reviews under the peer review standards. The AICPA is developing a new assertion-based examination performed under AT-C section 205 to replace it. This has led to a decline in the number of National PRC oversights of QCM reviews over the last few years. Only one oversight was performed in each of the years from 2020 to 2022. While the proposed criteria have been in development, some QCM providers have opted to obtain an examination of their QCM performed under the SSAEs using their own criteria. These engagements, and those expected to be performed using the AICPA's proposed criteria, are not subject to the National PRC's oversight or acceptance procedures.

2. Engagement review

An engagement review is performed when the firm only performs:

a. Financial statement preparation engagements under SSARS.
b. Compilations of financial statements under SSARS.
c. Reviews of financial statements under SSARS.
d. Agreed-upon procedures under SSAEs.
e. Review attestation engagements under SSAEs.

An engagement review only includes an examination of a sample of the firm's engagements from those areas. At the conclusion of the peer review, the firm will receive a rating of pass, pass with deficiencies, or fail. Similar to a review of financial statements, the peer reviewer is not issuing an opinion.

3. System review

A system review is far more comprehensive than an engagement review. With a system review, the peer reviewer obtains an understanding of:

a. The firm's accounting and auditing practice, (e.g., industries where it practices); and
b. The design of the firm's quality system, including its policies and procedures and how the firm monitors compliance with them.

The peer reviewer's objective is to determine whether the system is designed to ensure conformity with professional standards and whether the firm is complying with its system. Professional standards for design of a system of quality control include the Statements on Quality Control Standards (SQCSs)[1] issued by the AICPA that pertain to leadership responsibilities for quality within the firm, relevant ethical requirements (e.g., independence, integrity, and objectivity), acceptance and continuance of client relationships and specific engagements, human resources, engagement performance, and monitoring.

During the peer review process, the reviewer may find that the system of quality control is not properly designed or that it is properly designed but the firm is not complying with the requirements of the system. Engagements that were not performed and/or reported on in conformity with applicable professional standards in all material respects are considered "nonconforming."

4. Corrective action

Corrective actions are remedial in nature and are intended to strengthen the performance of the firm. The firm acknowledges that it will perform and complete the required corrective action plan as a condition of its peer review acceptance. The firm's peer review is not complete until the administering entity is satisfied that the corrective actions were sufficiently performed. It is also possible that the firm may be required to complete an implementation plan.

There can be multiple corrective actions and implementation plans required on an individual review. When an implementation plan is required, the firm must acknowledge that it will perform and complete it as a condition of cooperation with the administering entity and the Peer Review Board. If the firm fails to cooperate with the implementation plan, it would be subject to fair procedures that could result in the termination of the firm's enrollment in the Peer Review Program.

5. Must-select engagements

The system review also includes evaluation of a sample of the firm's engagements. A cross section of the firm's types of engagements as well as personnel are selected including "must-select" engagements as follows:

a. Engagements performed under *Government Auditing Standards*.
b. Audits of employee benefit plans.
c. Audits of depository institutions (with assets of $500 million or greater).
d. Examinations of service organizations (Service Organization Control (SOC) 1 and SOC 2 engagements).

Note that in a May 2021 Peer Review Update, the AICPA announced that the Peer Review Board (PRB) determined that audits and the related compliance and exemption engagements for SEC-registered broker-dealers (BDs), including those dually registered with the SEC and the CFTC, should no longer be

[1] Note that beginning with years ended December 31, 2026, the SQCSs will be superseded by the suite of Quality Management Standards (SQMS). They are still in QC 10.

included in the scope of peer review. The Securities Investor Protection Corporation (SIPC) agreed-upon procedures engagements will remain subject to peer review.

6. Classification of issues identified

Peer reviewers use a classification system to distinguish the severity of issues noted during the peer review. Like the findings communicated to auditees by auditors, issues are identified as matters, findings, deficiencies, or significant deficiencies.

a. **Matter for further consideration** – One or more "no" answers to questions in peer review checklists identified during a system review or an engagement review.
   (i) **Engagement reviews** – One or more "no" answers to questions in peer review checklists that were not resolved to the review captain's satisfaction. These are documented as matters for further consideration (MFCs) on an MFC form.
   (ii) **System reviews** – One or more "no" answers to questions in peer review checklists that a reviewer concludes warrant further consideration in the evaluation of a firm's system of quality management. A matter should be documented as a matter for further consideration (MFC) on an MFC form.

b. **Finding for further consideration** – One or more related matters with the same systemic cause related to designing, implementing, operating, or complying that result from a condition in the reviewed firm's system of quality control management or compliance with the system such that there is more than a remote possibility that the reviewed firm would not perform or report in conformity with the requirements of applicable professional standards. A finding should be documented as a finding for further consideration (FFC) on an FFC form (system review).

The peer reviewer will look at similar findings in the aggregate when deciding as to whether a finding is a deficiency or significant deficiency. If the finding does not rise to the level of a deficiency, it is documented on an FFC form. If one or more findings are a deficiency or significant deficiency, a report rating of pass with deficiency or fail would be appropriate.

7. Report classification

a. **Deficiency** – When evaluating the reviewed firm's system of quality management taken as a whole, *one or more matters* that the team captain has concluded could create a situation in which the reviewed firm would not have reasonable assurance of performing or reporting in conformity with the requirements of applicable professional standards *in one or more important respects*. **Deficiencies should be documented in a peer review report with a rating of pass with deficiencies**.

b. **Significant deficiency** – One or more matters in a system review that the reviewer has concluded create a situation in which the reviewed firm's system of quality management does not provide the reviewed firm with reasonable assurance of performing or reporting in conformity with the requirements of applicable professional standards in all material respects. **Significant deficiencies should be documented in a peer review report with a rating of fail**.

If a deficiency or significant deficiency is related to an engagement in a "must select" area or specific industry, the report will identify the area. However, generally since the system review is designed to report on the firm's system of quality control, the report would not necessarily describe every engagement that was deemed nonconforming.

8. Ratings classification

a. **"Pass" rating** – The reviewer is saying that nothing came to their attention to lead them to believe the work was not performed and reported on in accordance with relevant standards in all material respects.

b. **"Pass with deficiencies" rating** – The reviewer has determined that at least one but not all of the engagements submitted for review was not performed and reported on in conformity with applicable professional standards in all material respects and has one or more deficiencies described in the report.

c. **"Fail" rating** – The peer reviewer notes that all of the engagements submitted for review had deficiencies that resulted in the engagements having not been performed or reported on in conformity with applicable professional standards in all material respects.

Since peer review is required by state accounting licensure boards, firms that pass with deficiencies or fail are required to remediate their deficiencies. The Report Acceptance Body will evaluate the firm's letter of response to see if it is an indication of further issues in the quality control system and whether monitoring procedures are deemed necessary. Remediation generally involves targeted continuing professional education and pre-issuance reviews. Firms that do not cooperate with assigned remediation can be removed from the Peer Review Program.

9. PRSU 2, Reviewing a Firm's System of Quality Management and Omnibus Technical Enhancements

The AICPA has been working on its Quality Management standards and has provided tools and education to assist practitioners in implementation. It recently approved Peer Review Standards Update (PRSU) 2, *Reviewing a Firm's System of Quality Management and Omnibus Technical Enhancements*. Its purpose is to better align peer review standards with the QM standards. The updates in PRSU 2 are effective for firms with peer review years ending on or after December 31, 2025. Until then, it is expected that peer reviews will continue to evaluate and report on a firm's system of quality control according to the Statements on Quality Control Standards (SQCSs).

The new QM standards will not change the peer review process itself but will affect the questions and inquiries firms receive from reviewers. For example, while existing standards address tone at the top and the responsibility to ensure all firm members are aware of quality control standards, the new guidance contains an explicit requirement that the firm CEO or managing partner assume ultimate responsibility for the firm's QM system.

The standard says that the CEO is required to evaluate the firm's QM system at least annually and conclude whether the system provides the firm with reasonable assurance that the objectives of the QM system are being achieved. Therefore, peer reviewers may be talking to the managing partner to ensure they really understand the process.

In a recently published article, peer reviewers provided advice to practitioners related to new quality management standards:

a. Understand areas of the standards that present challenges. This may range from revising policies and adding policies to a plan to draft the new quality management document.

b. Risk assessment will be the most challenging part. Remember that the AICPA does not expect firms to be perfect. They expect to see areas of risk to emerge. It's ok to document the struggles and then show how they are being addressed.

c. The monitoring plan is important. There will be more regular monitoring based on risk.
d. Don't wait any longer to get started. Risk assessment takes longer than you think it will if you do it correctly.

D. AICPA identifies challenges for accounting firms

In 2024 the AICPA identified three major challenges faced by accounting firms for the coming years:

a. Talent acquisition;
b. Risk assessment practices; and
c. Evolution of quality management standards.

To address these challenges firms would be wise to adopt strategies that streamline audit processes and enhance compliance and better understand and leverage the power of technology in their audits.

1. Challenge #1 – Talent acquisition

Firms should consider their technology strategy a talent strategy. Technology-enabled auditing has provided powerful tools to assess risk and spot anomalies and fraud. While not a substitute for professional judgment, it allows job roles to broaden and expand. Workforce trends indicate employees are looking for meaningful work experiences. It is important to provide more opportunities for staff to learn about the client's business. Technology can also improve quality because it can assist in investigating data outliers. Staff will be happier when they are able to do less tedious and more meaningful work.

At the start of 2026, the AICPA launched the Profession Ready Initiative to understand the needs of the profession and determine what skills and capabilities will be needed from firm staff in the coming years. This understanding and upskilling initiative is currently performing its research activities and will issue a final report in 2027.

2. Challenge #2 – Risk assessment practices

Risk assessment failures are the leading cause of MFCs in audit practices. Peer reviews have noted the following issues:

a. Continuing with business as usual. The vocabulary has not changed significantly but the meaning behind it has.
b. Not all account balances are significant.
c. Not all assertions in an account balance are relevant.
d. Not all categories of revenue are significant risks.

Risk assessment will be more fully discussed in the next chapter.

3. Challenge #3 – Quality management

The AICPA's new quality management (QM) standards are designed to help firms improve the quality of their accounting and auditing engagements in a modern and scalable way. When properly implemented they will move firms from a policies-based approach to a risk-based approach. The starting point for the standards is the risk assessment process. It is a new component firms will use to determine how to design and implement as part of their system of quality management. The process enables firms to tailor the system of quality management to respond to the nature and circumstances of the firm.

E. Quality issues identified in peer review

The 2024 report on peer review issues identified between 3/01/23 and 6/30/2024, peer review issues related to poor quality control included:

a. *Leadership responsibilities for quality within the firm:*
   (i) Failure to update the quality control document regarding EQCR and monitoring;
   (ii) Failure to devote sufficient resources for the support of its quality control policies and procedures; and
   (iii) Failure to ensure that firm personnel complete the appropriate amount of CPE in areas of practice and in accordance with the requirements of professional standards.
      - Some firms are using templates from practice aids and other vendors and failing to tailor them to the unique qualities and risks of the firm.
      - Some firms are not performing key quality control functions such as consultations with others on engagement issues and engagement quality control reviews (EQCRs).
      - ***Use of outdated quality control materials***.
      - ***Noncompliance with CPE requirements***.
      - ***Failure to get the appropriate engagement letter and tailor it, especially related to engagements under Government Auditing Standards or Uniform Guidance***.
      - ***Failure to communicate with the predecessor auditor (including NOCLAR)***.

b. *Acceptance and continuance:*
   (i) Peer reviewers have noted that firms are not always documenting acceptance and continuance procedures. In addition, they have noted that firms are not always obtaining the proper licensure in the states where engagements were accepted and evaluating the risk of performing an engagement in a specialized industry or obtaining the necessary knowledge of current standards in specialized areas prior to performance of the audit.

c. *Engagement performance:*
   (i) Failure to properly complete or utilize purchased practice aids to assist in performing and documenting engagements; and
   (ii) Failure to perform EQCR on engagements that meet the firm's criteria.
   (iii) ***Failure to perform appropriate analytical procedures, including developing expectations***.

Note that the issues in bold italics are new in 2024. The others are continuing issues identified in earlier years.

Example: An audit firm prepared a quality control document summarizing its policies and procedures under the SCQS. It used a template provided by its practice aid vendor and inserted the firm name and filled in the blanks. When the firm was first started the partner in charge of quality control did not make many modifications to the document before it was finalized as firm policy. Over time the firm's client base grew and auditing standards evolved. One of the provisions in the original document was that the firm would exclusively use the vendor-prepared practice aids. In order to streamline some of the work the staff began to build their own practice aids in excel rather than use the proscribed forms. A peer review pointed out that by doing this and omitting some of the practice aids from the vendor's complete set, the firm was violating their quality control policies.

The partner group amended the document to say that the firm uses the vendor-created practice aids as a base for its audit documentation unless the partner deems a firm-prepared practice aid to be more efficient and effective documentation.

II. Documentation – Peer review issue identified

The most common reason for a nonconforming audit as noted in the AIPCA's enhanced oversight of the peer review program continues to be lack of documentation. In some instances, practitioners may be performing the procedures required by professional standards and simply moving on with their work without sufficient documentation of their work. Documentation with tick mark or check is a practice aid and may not be enough to comply with professional standards. In other cases, practitioners may not even be aware that they have not performed the level of work required by professional standards.

With the continued peer review emphasis on documentation, the AICPA developed several audit documentation resources, including an *Audit Documentation: Frequently Asked Questions* document. This and other resources can be accessed at https://us.aicpa.org/interestareas/peerreview/resources.html.

A. General standards on documentation

Section AU-C 230, *Audit Documentation*, discusses the general standards of documentation but be aware that each individual standard, (e.g., audit, review, compilation, or attestation) also contains its own requirements for documentation. In addition, certain laws, regulations, and other standards may impose additional regulations on the practitioner.

AU-C 230 states "The auditor should prepare audit documentation that is sufficient to enable an experienced auditor, having no previous connection with the audit to understand:

a. The nature, timing and extent of the audit procedures performed to comply with GAAS and applicable legal and regulatory requirements;
b. The results of the audit procedures performed, and the audit evidence obtained; and
c. Significant findings or issues arising during the audit, the conclusion reached, and significant professional judgments made in reaching the conclusions."

When preparing documentation, the auditor should document:

a. The identifying characteristics of the specific items tested;
b. The person who performed the work and the date the work was performed; and
c. The person who reviewed the work performed, the date and the extent of review.

When documenting the nature, timing, and extent of audit procedures the auditor will consider sampling applications. Sampling applications are used when testing attributes such as the occurrence of an internal control. They are more often used in identifying the extent of items to test in substantive testing. AU-C 530 provides guidance on sampling methodologies used in an audit including documentation requirements. These are discussed in a later section.

Auditing standards contain requirements with which the auditor **must** comply. These are unconditional standards. There are very few instances in professional literature where the auditor **must** comply. Most of the standards state that the auditor should do one thing or another. The word ***should*** refers to a presumptively mandatory requirement and if the auditor decides to depart from the standard, they should document the justification for the departure.

Auditors should take care when completing checklists and audit programs. Many times, these practice aids instruct the auditor to perform a procedure. If the auditor checks the box indicating they have performed the procedure or simply comments “done” in the comment box, that does not constitute evidence that the procedure has been performed. Practice aids often have pre-printed consideration points. For example, a team memo practice aid may have a list of required discussion points. This is not considered documentation that the firm discussed them unless there is also some evidence that brainstorming on the risk of fraud or error occurred. Additional language is needed to support the brainstorming requirement.

1. Exercise: Peer review issue identified – Presumptively mandatory requirements

Professional standards require that accounts receivable be confirmed. The audit partner on the engagement knew that in situations involving nursing home patients the chances of confirmations being returned were very low. Therefore, he directed the staff to test subsequent payments instead. The workpaper contained a list of the patients selected for testing along with a record of payments vouched and a summary at the bottom showing the extent of the testing performed and the results. Was this documentation sufficient to meet professional standards?

2. Audit standards are interrelated

Another issue that frequently arises is that auditing standards are interrelated. An SAS may be issued that contains references to guidance that is found in more than one AU-C section. If the auditor is not careful to understand all the guidance impacting a topic, then they may miss some important information.

Example: An auditor was preparing to perform a risk assessment on an engagement. She went to AU-C 315, which contains the guidance an auditor needs related to understanding the entity and its environment and assessing the risk of material misstatement to understand the concept of significant risk. She noted that the guidance was revised and that there was a new definition for significant risk. Instead of a risk that needs further audit consideration, the new definition states that it is a risk on the upper end of the inherent risk spectrum. The auditor assesses characteristics of events or conditions that affect the susceptibility to misstatement, whether due to fraud or error, of an assertion about a class of transactions, account balance, or disclosure, **before** consideration of controls.

Such factors may be qualitative or quantitative and include:

a. Complexity;
b. Subjectivity;
c. Change;
d. Uncertainty;
e. Susceptibility to misstatement due to management bias; and

f. Other fraud risk factors that affect inherent risk.

Once she noted the list of significant risks in the standard, she used that guidance to perform the risk assessment. The peer reviewer asked why she had not considered revenue recognition or related party transactions in the analysis.

The auditor mentioned that AU-C 315 did not specifically mention them. The peer reviewer referred her to the appendix at the back of AU-C 315 and the guidance in AU-C 240.

Note that SAS 145 does not require the auditor to identify overall risks such as management override as significant risks. AU-C 240, *Consideration of Fraud in a Financial Statement Audit*, identifies procedures that should be performed relative to management override.

3. Specific issues in documentation noted

Specific general issues identified by peer reviewers with year ends between March 31, 2021, to June 30, 2023, were:

a. Failure to appropriately document planning procedures, including:
   (i) Risk assessment (and linkage of risks to procedures performed);
   (ii) Planning analytics;
   (iii) Understanding of IT environment;
   (iv) Internal control testing; and
   (v) Consideration of going concern.

b. Failure to properly support and document the assessed level of risk in accordance with professional standards, including:
   (i) Setting control risk at less than high without testing the effectiveness of controls;
   (ii) Performing risk assessment at the audit level rather than at the relevant assertion level;
   (iii) Failure to properly identify and/or document the relevant risks and controls associated with the role of IT;
   (iv) Failure to document linkage between risk assessment procedures and actual substantive procedures performed;
   (v) Failure to document fraud risk assessment procedures regarding inquiries with those in charge of governance and response to management override of controls; and
   (vi) Failure to appropriately address fraud considerations related to revenue recognition.

c. Failure to obtain appropriate management representation letters:
   (i) Update the letter to include all representations required by the applicable professional standards;
   (ii) Date the letter appropriately;
   (iii) Include appropriate financial statement periods;
   (iv) Include required representations; and
   (v) Include appropriate wording concerning consultation with an attorney.

d. Failure to communicate and/or document required communications with those charged with governance.

e. Failure to properly adopt newer standards regarding the presentation of debt issuance costs and revenue recognition;

f. Failure to include audit documentation that contains sufficient competent evidence to support the firm's opinion on the financial statements; and
g. Insufficient review of audit documentation.

Accounting and review services issues noted were:

a. Failure to obtain an engagement letter with the correct language in it as prescribed by professional standards;
b. Failure to disclose the fact that substantially all disclosures have been omitted on the face of the financial statements or in the notes;
c. Failure to include a statement that indicates that at a minimum, no assurance is provided on the financial statements; and
d. Failure to disclose departures from the financial reporting framework including the omission of the statement of cash flows.

III. Independence

A. Peer review issue identified

Section 1.200 of the AICPA's Code of Professional Conduct (Code) addresses independence. Note that the Government Accountability Office (GAO), the PCAOB, SEC, Department of Labor (DOL) and others also set independence rules. We will discuss the independence rules for the GOA and the DOL in later chapters.

The Code refers to two basic risks of independence. One is the risk that the practitioner is not independent (independence in mind) and the second is that the practitioner is perceived as not being independent (independence in appearance). Practitioners are directed to use conceptual framework which involves:

a. Identifying threats to independence.
b. Evaluating the threat that the AICPA member would not be independent or would be perceived by a reasonable and informed third party who is aware of the relevant information as not being independent.
c. Threats must be eliminated or reduced to an acceptable level to be independent.

Threats are considered to be at an acceptable level when they and their potential effects have been eliminated or reduced so that a reasonable and informed third party who is aware of the relevant information would perceive that the member's professional judgment is not compromised.
Professional standards require compliance with the AICPA's independence rule where an attest service is performed. Although a compilation is an attest service, independence is not required if the lack of independence is disclosed in the compilation report.

The Code identifies several types of threats. Since the objective of this program is to discuss issues that frequently arise in peer review, we will only be discussing in detail the threats that arise when performing nonattest services.

The list of threats follows. Those threats that particularly affect nonattest services are bolded.

a. Adverse interest threat;
b. Advocacy threat;
c. Familiarity threat;
d. **Management participation threat**;
e. Self-interest threat;
f. **Self-review threat**; and
g. Undue influence threat.

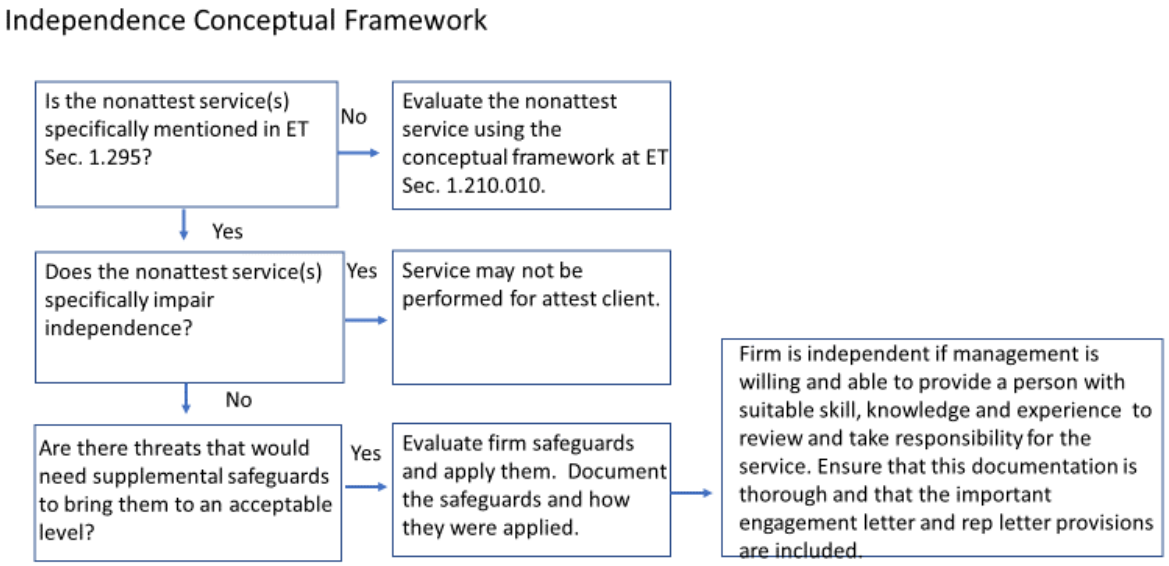
The nonattest service rules apply during the period of professional engagement and during the period covered by the financial statements. There is an exception for prohibited nonattest services. If the member provides an entity with nonattest services that impair independence prior to the entity becoming an attest client, independence is not impaired for prior periods that were audited by another firm. Or in the case of a review engagement reviewed or audited by another firm. There are also exceptions for affiliates of a client.

Examples of nonattest services are:

a. Financial statement preparation;
b. Cash to accrual conversion;
c. Reconciliations;
d. Advisory services;
e. Appraisal, valuation, and actuarial services;
f. Benefit plan administration services;
g. Bookkeeping, payroll, and other disbursements;
h. Business risk consulting;
i. Corporate finance consulting;
j. Executive or employee recruiting;
k. Hosting services;
l. Information systems design, implementation, or integration;
m. Internal audit;
n. Investment advisory or management; and
o. Tax services.

If nonattest services involve leading or directing the entity including making significant decisions regarding the acquisition, deployment, and control of human, financial, physical, and intangible resources, they are considered management responsibilities and are prohibited.

When performing permitted nonattest services, the client must agree to assume all management responsibilities, oversee the services by designating an individual who possesses suitable skill, knowledge and or experience (SKE), evaluate the adequacy and results of the services performed and accept responsibility for the services.



1. Safeguards

The application of safeguards is necessary to reduce threats to an acceptable level when performing routine nonattest services. Examples of those types of services are responding to an attest client's tax questions, providing advice to the client on routine business matters, educating the client on technical matters, and providing the client with best practice and other information that is readily available to the practitioner.

There are three types of safeguards:

a. Safeguards at the entity;
b. Safeguards set forth by the profession; and
c. Safeguards applied by the firm performing nonattest services.

Although safeguards at the entity and those set forth by the profession are helpful, they are only supplemental to those that are applied by the firm. Note that GAGAS only permits safeguards applied by the firm to mitigate significant threats to independence.

Examples of safeguards that could be applied by the firm are:

a. Firm leadership that stresses the importance of independence and the expectation that members of attest engagement teams will act in the public interest.
b. Policies and procedures that are designed to implement and monitor quality control in attest engagements.
c. Documented independence policies regarding the identification of threats to independence, the evaluation of the significance of those threats, and the identification and application of safeguards that can eliminate the threats or reduce them to an acceptable level.
d. Internal policies and procedures that are designed to monitor compliance with the firm's independence policies and procedures.
e. Use of different partners, partner equivalents, and engagement teams that have separate reporting lines in the delivery of permitted nonattest services to an attest client, particularly when the separation between reporting lines is significant.

f. Training on, and timely communication of, a firm's policies and procedures, and any changes to them, for all partners and professional staff.
g. Discussing independence issues with the audit committee or others responsible for the client's governance.
h. Disclosures to the audit committee (or others responsible for the client's governance) regarding the nature of the services that are or will be provided and the extent of the fees charged or to be charged.
i. Involvement of another professional accountant who reviews the work that is done for an attest client or advises the attest engagement team (either from outside the firm or someone from within the firm who is not otherwise associated with the attest engagement).
j. Consultation on engagement issues with an interested third party, such as a committee of independent directors, a professional regulatory body, or another professional accountant.
k. Rotation of senior personnel who are part of the attest engagement teams.
l. Policies and procedures that are designed to ensure that members of the attest engagement team do not make or assume responsibility for management decisions for the attest client.
m. Involvement of another firm to perform part of the attest engagement.
n. Involvement of another firm to reperform a nonattest service to the extent necessary to enable it to take responsibility for that service.

2. Independence under Government Auditing Standards

Auditors should be aware that the independence requirements under Government Auditing Standards (GAS) are more rigorous than those under AICPA standards. GAS is an overlay on the AICPA standards with the effect of building upon the AICPA independence requirements, not superseding them.

The thought process for evaluating independence related to nonaudit (nonattest) services is different in that the documentation requires additional steps. In addition, the auditor makes a distinction between the preparation of financial statements in their entirety and assisting in the preparation of financial statements. When preparing financial statements from accounting records or the trial balance safeguards are required. The safeguards may take the form of a person outside the engagement team performing a review. In many firms, this may be a person with the appropriate level of skill necessary to perform the review who is employed by the firm. In smaller firms, this person may come from another firm or be an independent consultant. The reviewer must have the appropriate level of Yellow Book CPE.

The auditor is also required to determine if the person taking responsibility at the client for the nonaudit service could identify a material error, or omission in the nonaudit service. This is a higher standard than discussed in the AICPA ethics standards.

Discussion question:

The AICPA has been issuing Audit Risk Alerts for over 30 years. Among other things, they focus on deficiencies that have come to light in audits. Why do you believe that audit quality continues to be a problem?

IV. Discussion question and exercise solutions

A. Discussion question

There is no specific answer to this question. Some possible reasons for the issues in audit quality are that the risk assessment standards which were issues beginning in 2006 made significant changes to the way audits were being performed. Some auditors believed that the procedures required by the new standards had little value, so they were not rigorously performed or documented. In addition, there were so many new requirements that auditors felt overwhelmed and defaulted to the way they did things in the past. Some auditors were not aware of all the new requirements including those that were issued when the audit standards were clarified in 2012. This may be magnified now that nine new audit standards are effective for calendar years 2021 and beyond. In addition, there are another four new audit standards that became effective for calendar years 2022 and 2023.

B. Exercise: Presumptively mandatory requirements – Suggested solution

The auditor performed the step as requested by the partner and documented the items selected and the amount of subsequent receipts vouched. AU-C 330.31 states that “the auditor **should** include in the audit documentation the basis for any determination not to use external confirmation procedures for accounts receivable when the account balance is material.

Risk Assessment

Risk Assessment

Learning objectives

Upon reviewing this chapter, the reader will be able to:

- Discuss the changes in auditing standards over the last 20 years, including the direction auditing standards are taking today;
- Note the elements of the risk assessment process that have been identified as deficient in peer reviews; and
- Identify and implement best practice techniques and documentation for key elements of the risk assessment process.

I. Introduction

A. Brief history

Prior to 2008 most audits performed by private companies were primarily substantive. Firms obtained only the briefest understanding of internal control and risk. Then in 2006 the auditing landscape changed for firms with the issuance of what was then SAS 103, *Audit Documentation*, shortly followed by a suite of SAS (104-111), effective for calendar year-ends 2008 and after, changing the way firms are required to assess risk in financial statement audits.

These standards were issued in direct response to changes in the auditing environment which were sparked, in part, by high profile corporate frauds. The Sarbanes Oxley Act and the creation of the PCAOB set the tone. When the PCAOB was created it adopted the AICPA's SAS. However, shortly thereafter it began issuing its own standards which now cover many auditing topics.

1. Definition of audit risk

Audit risk is the risk that the financial statements are materially misstated, and the auditor expresses an inappropriate opinion. It is a function of two components:

a. Risks of material misstatement – not under the auditor's control (Inherent Risk + Control Risk); and
b. Detection risk.

Risk assessment is performed at the overall and assertion-based level. Categories of financial statement assertions include:

a. Classes of transactions; and
b. Account balances.

Presentation and disclosure are assertions that are generally evaluated at the time the financial statements are prepared/reviewed by the auditor.

B. SAS 145, the revised risk assessment standard

In October 2021, the Auditing Standards Board approved a revision to the risk assessment standards. The revised standard, SAS 145, is effective now, for years ending on or after December 15, 2023. SAS 145, for the most part, conforms to the revised risk assessment guidance issued by the International Auditing and Assurance Standards Board (IAASB), and addresses many of the deficiencies found by peer reviewers and other reviewers.

1. Providing clearer guidance to reduce confusion and promote consistency

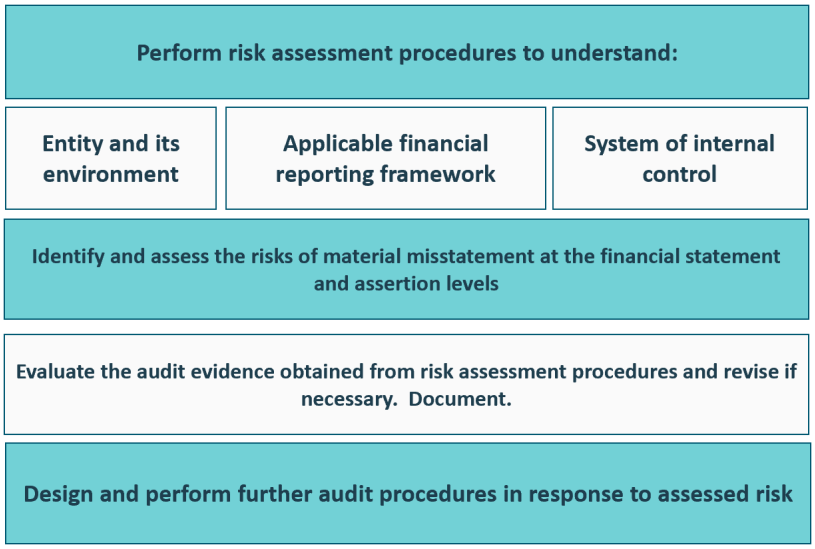
Since one of the intents of the AICPA in drafting this standard was to clarify certain concepts and terminology that were confusing to practitioners, the standard includes six appendices that include consideration points for understanding:

a. Entity and Its Business Model;
b. Inherent Risk Factors;
c. Entity's System of Internal Control;
d. Entity's Internal Audit Function;
e. Information Technology; and
f. General IT Controls.

The consideration points in these six areas are valuable in assessing the risk of material misstatement and help to explain many of the concepts that auditors thought were confusing in the previous standard.

It is important to remember that SAS 145 did not overhaul the concept of risk assessment. It is fundamentally the same. However, the AICPA made **significant** improvements to the guidance which helps auditors to see what the standards were intended to do all along. Many of these improvements are in the area of better defining the terminology that was used in the standard.

Following is a snapshot of the risk assessment process.



2. Interrelated definitions

AU-C 200, which describes the auditor's overall objectives, states that audit risk is a function of the risk of material misstatement plus detection risk. The risk of material misstatement is comprised of inherent risk and control risk. The risk of material misstatement is found at both the financial statement level and the assertion level as it relates to significant account balances, classes of transactions, and disclosures. The assertion level risk is targeted whereas the financial statement level risk is broad and potentially could affect many account balances, classes of transactions, and assertions. Both are important to understand in the risk assessment process. When assessing the risk of material misstatement, the auditor is aware that both the risk of error and the risk of fraud should be assessed since the objective of the auditor is to obtain reasonable assurance that the financial statements are free from material misstatement whether

due to fraud or error. The standard only requires the auditor to assess the risk of significant account balances, classes of transactions, or disclosures.

To conform to international standards the ASB revised a series of definitions related to the identification of material misstatement. Respondents to the exposure draft were confused about when they would be required to assess risk. The number of new definitions and how they relate were unclear. The first important definition to understand is ***significant***. An account balance, class of transactions, or disclosure is significant when there is one or more relevant assertion associated with it. The determination of significance is based on ***inherent risk*** without regard to internal controls.

The next concept that was unclear was the concept of ***relevant assertion***. An assertion must have an identified risk of material misstatement in order to be a relevant assertion.

To determine if an assertion has an identified risk of material misstatement, the auditor would evaluate it to determine if the risk of material misstatement is present. Both factors should be present:

a. **Likelihood** – There is a reasonable possibility that the misstatement could occur; and
b. **Magnitude** – There is a reasonable possibility that the amount could be material.

The term ***reasonable possibility*** needs to be defined so that it is not misinterpreted. As in other professional literature the term reasonable possibility is ***less than probable*** (also defined as likely) but ***more than remote***. A risk of material misstatement may relate to more than one assertion. In that case all the assertions related to the risk are relevant assertions.

The standard further notes that for material classes of transactions, account balances, or disclosures that have not been determined to be significant classes of transactions, account balances, or disclosures, the auditor should evaluate whether the auditor's determination remains appropriate.

SAS 145 requires the assessment of inherent risk and control risk to be performed separately. The AICPA has stressed this concept for years and the standard now codifies the requirement. Since only relevant assertions are assessed for risk, it follows that risk of material misstatement is made at the assertion level as well. Previously, some auditors assessed the risk of material misstatement for inherent and control risk together for an entire account balance or class of transaction.

Another issue that has emerged since the standards are now effective is that auditors are having issues related to identifying assertions as **not relevant** because they are concerned that they will have peer review comments. In addition, if the time is not spent up front in the risk assessment process, a SALY (same as last year) approach is often used.

3. Inherent risk

To assist auditors in their understanding of inherent risk the ASB introduced a new term in its SAS 145, ***inherent risk factors***. Inherent risk factors are defined as characteristics that affect susceptibility to misstatement of an assertion about a class of transactions, account balance, or disclosure, and that may be quantitative or qualitative in nature.

The auditor uses the inherent risk factors to evaluate certain aspects of events or conditions that affect an assertion's susceptibility to misstatement. SAS 145 also introduces the concept of the ***spectrum of inherent risk***. The spectrum refers to the fact that inherent risk factors individually or in combination

affect inherent risk to varying degrees and that inherent risk will be higher for some assertions than for others. Inherent risk varies along the spectrum. This term was introduced in order to try to drive consistency in the auditor's risks assessment process and to provide a framework for considering the likelihood and magnitude of possible misstatements.

Examples of inherent risk factors are:

a. Subjectivity;
b. Complexity;
c. Change;
d. Uncertainty; and
e. Susceptibility to misstatement due to management bias or fraud.

Other inherent risk factors arise from events or conditions related to the entity.

SAS 145 provides guidance to assist auditors in determining the level of inherent risk. Using their understanding of inherent risk factors the auditor will assess where the risk is on the inherent risk spectrum. As noted in the graphic below, the auditor evaluates the risk at the assertion level or event level (for example, an acquisition would be viewed as an event). Certain assertions at the event level, such as valuation, may carry more risk. It is important to note that inherent risk is not influenced by control risk or the ease of the procedures the auditor will perform.

4. Risks at the financial statement level

Auditors will identify risk at the financial statement and assertion level. Financial statement risk is broad and pervasive, potentially affecting several account balances, classes of transactions, and assertions. The auditor is instructed to take the risk down to the account balance and assertion level but that is not always possible. Even though the auditor is **no longer** required to assess whether overall financial statement risks are significant risks, many still do, primarily because some commercial practice aids still have that indicator on the practice aid.

Financial statement level risks are likely to be:

a. Due to external circumstances;
b. Related to the client and its environment;
c. Economic, accounting, or other developments;
d. Business combinations;
e. Going concern issues;
f. Consolidation, such as with respect to variable interest entities; or
g. Management override of controls.

Examples: Risks at the financial statement level may arise from deficiencies in the control environment or from external events or conditions such as declining economic conditions. For example, if there is a lack of management competence or a lack of oversight over the preparation and fair presentation of the financial statements, this may have a more pervasive effect on the financial statements and may require an overall response by the auditor.

Risks of material misstatement due to fraud may arise that affect more than one component of the financial statements. For example, if the auditor understands from inquiries of management that the entity's financial statements are to be used in discussions with lenders to secure further financing to maintain working capital and they know that current loan agreements with these lenders contain financial covenants that the entity is at risk of failing to meet, this condition is likely to be identified as a fraud risk factor. The auditor will then identify assertion level risks for existence, accuracy, or valuation of certain assets and completeness of certain liabilities that are susceptible to material misstatement as a result of this financial statement level risk.

The auditor's understanding of the control environment and other components of the system of internal control may raise doubts about the auditor's ability to obtain audit evidence on which to base the audit opinion or be cause for withdrawal from the audit. In this case the overall risk is the concern the auditor has about management's integrity.

Another overall risk might be the result of evaluating the entity's information system and communication. The auditor may determine that significant changes in the IT environment have been poorly managed, with little oversight from management and those charged with governance resulting in significant concerns about the condition and reliability of the entity's accounting records.

5. Risks at the account balance/assertion level

SAS 145 requires the auditor to assess the risk of **significant** account balances, classes of transactions or disclosures and only for relevant assertions within those account balances and classes of transactions.

a. The definition of significant account balances is now **one with a relevant assertion**.
b. When assessing the risk of material misstatement, the auditor considers both the risk of error and the risk of fraud.
c. Relevant assertions are those where there is a **reasonable possibility** of the risk occurring AND if it did, it would be material.
d. Another way of looking at this is *more than remote*. Whether it is reasonably possible or probable, it is still a relevant assertion.

To understand relevant assertions, it is important to recall what the assertions mean.

Assertion	Description
Existence/occurrence	Assets, liabilities, and equity interests exist. Transactions and events that have been recorded or disclosed have occurred, and such transactions and events pertain to the entity.
Completeness	All assets, liabilities, and equity interests that should have been recorded have been recorded, and all related disclosures that should have been included in the financial statements have been included. All transactions and events that should have been recorded have been recorded, and all related disclosures that should have been included in the financial statements have been included.
Rights and obligations	The entity holds or controls the rights to assets, and liabilities are the obligations of the entity.
Valuation	Assets, liabilities, and equity interests have been included in the financial statements at appropriate amounts, and any resulting valuation or allocation adjustments have been appropriately recorded, and related disclosures have been appropriately measured and described.
Accuracy/classification	Accuracy – Amounts and other data relating to recorded transactions and events have been recorded appropriately, and related disclosures have been measured and described. Classification – Assets, liabilities, and equity interests have been recorded in the proper accounts. Transactions and events have been recorded in the proper accounts.
Cutoff	Transactions and events have been recorded in the correct accounting period.

Many firms complain that they have messy clients where there are a significant number of audit adjustments needed because the client is either unwilling or unable to do it. To keep this from negatively impacting the risk assessment process, consider that bookkeeping work is nonattest work and put the work in another binder. It is important to evaluate independence in these cases.

Relevance, in terms of assertion, is based on inherent risk. This is a difficult concept for auditors because of the temptation to consider control risk or audit procedures as a component of inherent risk.

a. When assessing inherent risk – DO NOT consider the controls in place.
b. When assessing inherent risk – DO NOT consider the tests you intend to perform as the auditor.

Do not make the mistake of evaluating inherent risk in terms of the controls the entity has in place **or** the procedures the auditor intends to perform.

a. “The company has good controls over the cash receipts process and a lockbox is used.”
b. “We will vouch the five largest receivables that make up 80 percent of the balance.”

Property example:

There is not "one size fits all" when it comes to risk assessment. Therefore, it is important to know the client and the industry. This will help the auditor determine whether assertions are relevant. It is important to make the correct judgment or the auditor may spend time auditing account balances or classes of transactions that do not have a reasonable possibility of a material misstatement. In this example, the client has a material amount of plant and equipment. But materiality does not mean significant as auditors are used to interpreting it. It merely means large.

The land and buildings are 20+ years old. The client has very few additions and does not sell its assets. They use them at least until fully depreciated and often longer. Most of the assets at the time of the audit have been depreciated over at least half their useful life. Technology is mainly cloud-based and the computers and other assets that have obsolescence factors are small dollar value items which are depreciated over a short period of time. Where other entities may have construction in progress, assets that have obsolescence factors, components of property that are no longer used, this client does not. Following is the assessment of relevant assertions for property.

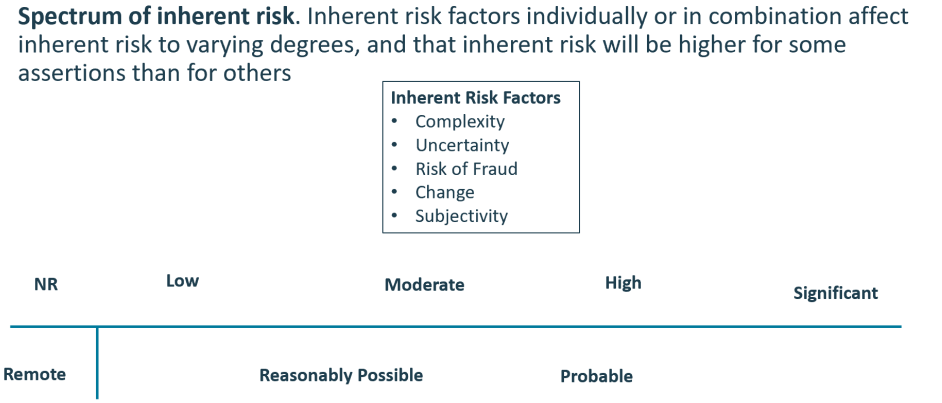
Assertion	Likelihood	Magnitude
Existence	Most of the entity's property is not susceptible to theft and the property that is susceptible (like laptop computers in the classroom) is not material. The entity does not purchase much property. Assessment: Not reasonably possible	Assessment: Not reasonably possible that the balance would be materially misstated. Not a relevant assertion.
Completeness	Likelihood that the asset listing is not complete- when property is purchased it is generally financed. The entity does not purchase much property from year to year. Large capital items are discussed at length and approved by the board. Assessment: Not reasonably possible	Assessment: not reasonably possible that the balance could be materially misstated. Not a relevant assertion.
Assertion	**Likelihood**	**Magnitude**
Valuation	Likelihood that the assets could be impaired. The property is recorded at historical cost and has been on the books for decades. It would not be a reasonable possibility that there could be sufficient decline in property values to cause an impairment issue. The entity is very profitable. Assessment: Not reasonably possible	Assessment: not reasonably possible that the balance could be materially misstated. Not a relevant assertion.
Assertion	**Likelihood**	**Magnitude**
Rights and obligations	Likelihood that the assets or debt reflected on the books are not those of the entity. This is an established entity with very few property transactions. Assessment: Not reasonably possible	Assessment: not reasonably possible that the balance could be materially misstated. Not a relevant assertion.
Cutoff	Likelihood that the depreciation is not recorded in the proper period. This is a routine entry. Likelihood that gains or losses would not be properly recorded in the proper period. The entity is unlikely to have this situation since that it uses the assets for more than the useful lives recorded. Assessment: Not reasonably possible	Assessment: not reasonably possible that the balance would be materially misstated. Not a relevant assertion.

Assertion	Likelihood	Magnitude
Accuracy	Very few purchases or write offs. Depreciation is a routine entry. Assessment: Not reasonably possible	Assessment: not reasonably possible that the balance would be materially misstated. Not a relevant assertion.
Classification	Very few purchases occur. Repairs and maintenance is more likely to be misclassified. Assessment: Not reasonably possible	Assessment: not reasonably possible that the balance would be materially misstated. Not a relevant assertion.
Presentation and Disclosure	Presentation and disclosure of property is not complex. Assessment: Not reasonably possible	Assessment: not reasonably possible that the disclosures would be materially misleading, omitted or misstated. Not a relevant assertion.

Based on the work performed, there are no relevant assertions, so the account balance is not significant. The auditor would, however, tie out the property ledger to the general ledger and would likely evaluate the client's property rollforward for reasonableness.

6. Significant risk

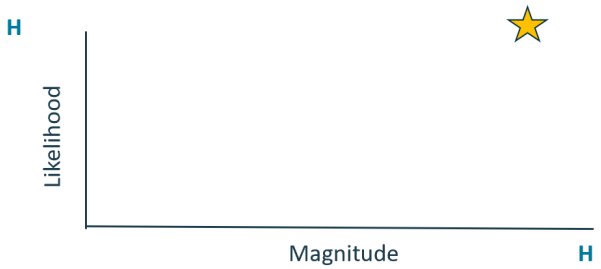
The standard provides a new definition for the term ***significant risk***. A significant risk is defined as a risk of material misstatement where the assessment of inherent risk is close to the upper end of the spectrum of inherent risk due to the degree to which inherent risk factors affect the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement should that misstatement occur or a risk that is required to be treated as a significant risk in accordance with an AU-C section such as the risk of fraud and significant unusual transactions with related parties.

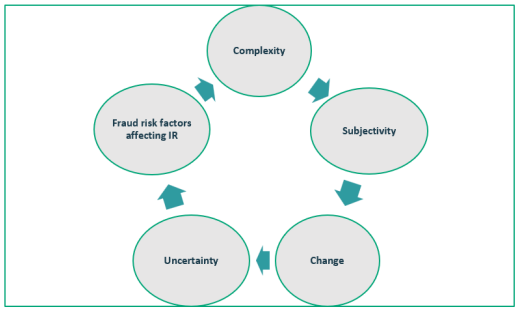


Significant risk is an identified risk of material misstatement for which the assessment of inherent risk is close to the upper end of the inherent risk spectrum due to the degree which inherent risk factors affect the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement should the misstatement occur.

Significant risk is also one that is identified in other AU-Cs like AU-240, management override, risk of fraud identified and revenue recognition (presumed to be a risk of fraud but can be rebutted). If not rebutted, AU-C 240 says that the risk of fraud is a significant risk.

Example 1: Revenue, occurrence, and completeness

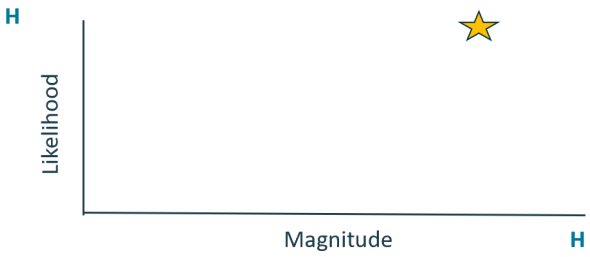


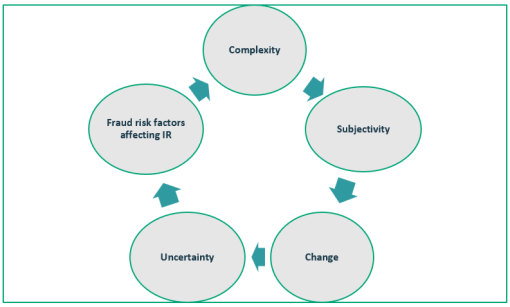


Account balance and assertion: Revenue, occurrence, completeness
Nonprofit that provides outpatient services to patients which include mental health services as well as primary care, pediatric care, and urgent care. The entity's revenue stream is **complex** due to the various third parties that bill for these services (Medicare, Medicaid, insurers, and self-pay) at different rates and the vast number of services performed in a year. It also has an aspect of **subjectivity** to it in that providers are coding services based on the work performed. It is also reasonably possible that to obtain more revenue the billings could be upcoded to a higher reimbursement level which is a risk of fraud.

Determination: Significant risk

Example 2: Notes receivable, valuation





Account balance and assertion: Notes receivable, valuation
The allowance for notes receivable has been accounted for under the incurred loss method. This account contains the elements of subjectivity and uncertainty and in prior audits, adjustments have been made because the client's customers have more risk than the industry average and the client did not recognize it. In addition, the client will be implementing CECL in the current year, which is a change. It is reasonably possible that the balance will be misstated and the amount material. The level of risk (likelihood and magnitude) is at the upper end of the inherent risk spectrum.

Determination: Significant risk

7. Understanding internal control

SAS 145 addresses the auditor's need to put more effort into their understanding of the entity, its environment, and internal control. The extant standard did not include the robust consideration of information technology (IT). This consideration is especially necessary in today's IT environment since the auditor obtains a significant amount of audit evidence through data obtained from the entity's financial reporting system. Therefore, an adequate understanding of how data integrity and access to data is maintained is important. This is true even in many smaller entities, with less complex environments.

The AICPA evaluated the results of peer reviews as well as other inspections along with its outreach activities, and determined auditors frequently had an inadequate understanding of internal control. Data supports that many auditors do not fully understand why the assessment of internal control is so important in planning the audit, which procedures were required when obtaining the understanding, and whether it was important to understand all components of internal control. SAS 145 clarifies which aspects of the entity's system of internal control are integral to the risk assessment process and the level of work that is necessary in obtaining the required understanding. Internal control is addressed in the next chapter.

8. Relationship to other standards

The guidance in SAS 145 is affected by other standards. AU-C 320, *Materiality*, states that materiality and audit risk are considered when identifying and assessing the risks of material misstatement. It is understood that the auditor's determination of materiality is a matter of professional judgment and affected by their perception of the needs of users of the financial statements. As it relates to SAS 145, classes of transactions, account balances, or disclosures are material if there is a substantial likelihood that omitting, misstating, or obscuring information about them would influence the judgment made by a reasonable user based on the financial statements. Therefore, the auditor should consider materiality in that context when evaluating relevant assertions.

When an entity has limited personnel causing a lack of segregation of duties, the auditor may be more likely to conclude that the risk of material misstatement for certain account balances and classes of transactions is likely to be reasonably possible, thereby causing them to be included in the risk assessment process and possibly be considered in the "other control" category.

Finally, the fact that the auditor is required to obtain an understanding of procedures used to initiate, authorize, record, process, and report information in the financial statements whether automated or manual in the information and communication component of internal control should result in the auditor obtaining an understanding over portions of the system that process a material volume of transactions even if they are not identified as significant risks.

9. Understanding and testing journal entries

The level of work to be performed in understanding and testing journal entries was also clarified. The standard does not require the auditor to understand the process and controls over **all** journal entries and other adjustments. The auditor should understand the process surrounding the financial statement closing process including examining material journal entries and other adjustments. The auditor is required to **test** those journal entries and may decide to test others. The auditor should also understand controls over journal entries related to significant risks when testing operating effectiveness and others the auditor feels are appropriate.

SAS 145 emphasizes the importance of professional skepticism and highlights the benefits. As also discussed in SAS 144, *Audit Evidence*, the standard highlights that it is important to be alert for contradictory evidence as well as corroborative evidence when performing a risk assessment.

10. Scalability

The Auditing Standards Board intends the standard to be scalable so that it addresses the needs of auditors with both complex and less complex clients. To this end, the standard is more principles-based and less prescriptive. Possibilities for scalability are integrated throughout the standard for those auditors

who are dealing with less complex entities and require simpler risk assessment procedures. Note that the scalability concept is not based on size but on the nature of the entity and its complexity.

The concept of scalability acknowledges that less complex entities generally have fewer formal policies and procedures, processes, and systems. This is likely to impact the auditor's understanding of the entity and its environment, including its internal control. When entities are less complex, especially those managed by their owners, the auditor may need to rely less on formal documentation and more on inquiry and observation. The auditor will use professional judgment to determine the nature and extent of the risk assessment procedures to be performed. The standard also contains guidance that may be helpful for auditors of governments.

11. Communications to governance

The auditor is required by AU-C 260, *The Auditor's Communication with Those Charged with Governance*, to communicate with those charged with governance in planning. SAS 134 added a requirement that significant risks be identified.

The auditor is required to communicate to governance at the end of the audit including their views on the entity's significant unusual transactions and the potential effects of uncorrected misstatements on future-period financial statements, if significant. These elements assist governance in understanding risk.

The governance communications may be either oral or in writing. Most firms prefer to have them in writing. Some firms comply with the requirement to communicate significant risks in the engagement letter.

12. Test Yourself question

Which of the following best describes the reason the ASB included content on scalability in SAS 145?

A. The guidance is intended to help auditors identify situations where not all of the risk assessment procedures need to be performed. The guidance is intended for smaller accounting firms.
B. The guidance acknowledges that audited entities are sometimes less complex and have fewer formal policies, procedures, and systems. This guidance is intended for auditors to use in those situations.
C. The guidance is intended to be used on smaller audit clients. Typically, they have less than $1,000,000 in revenue.
D. The guidance is useful for less complicated entities that use special purpose frameworks such as the modified cash or income tax basis of accounting.

II. Risk assessment advice from the AICPA

The risk assessment process is centered around risks of material misstatement to the financial statements (ROMMs). For some, starting the audit process with identification of ROMMs is not historically how they were trained, so there may be initial anxiety and resistance. SAS 145 should not be viewed as a compliance driven documentation exercise but a way to efficiently audit in an increasingly complicated business world with challenging financial reporting rules. SAS 145 moves beyond "Beat Up the Balance Sheet" brute force audit accounts approach, which lacks definition and is commonly understood as an audit approach where material is attacked with a high volume of procedures. Under this approach, risk assessment and understanding of internal controls are commonly viewed as a back-end form-driven approach.

Comments from the AICPA based on feedback, much of it from peer reviewers, attributed this issue to:

a. Too much SALY in substantive procedures.
b. Control understanding is perfunctory at best and sometimes misses changes in controls.
c. BUBS is defined by the individual engagement partner.
d. GAAP is too complicated to address with “brute force.”
e. CPA talent shortage puts premium on efficiency.
f. Unclear how to beat up liability that is not recognized.
g. Uniform approaches won’t work because Individual clients are too complex.
h. Risk based focuses align engagement team and drive purposeful audit work.
i. Audit standards presume a proper risk assessment. If not done it becomes a back-end form driven exercise to demonstrate compliance.
j. Significant risks are not understood.
k. Default to filling in all the boxes at the assertion level.
l. Firms don’t know how to support why they are not auditing an area.

It is important to understand and have a rationale to support what the auditor does. Risk of Material Misstatements (ROMM) exist when there is a reasonable possibility (more than remote) of a misstatement occurring (that is, its likelihood), and if it were to occur, there is a reasonable possibility (more than remote) of the misstatement being material (magnitude).

Auditors could consider a top-down approach starting with financial statement line items. For each line item (for example, cash, accounts receivable, revenues, inventory, and cost of sales, to name a few), ask – where is the risk here? Next, the auditor would look at the assertion that matches. If there is a more than remote possibility of material misstatement, then the assertion is relevant.

Financial statement line items can be aggregated or disaggregated for purposes of risk assessment. But sometimes it may be better to disaggregate – for example revenue since when something is blanketed as a significant risk that means D&I for each stream of revenue.

The auditor should also consider risks at the financial statement level. Management override is always a risk but there could be others – related parties, going concern.

For messy clients where the auditor proposes a significant number of “clean up” entries, it is better to have a nonattest file. This properly segregates the service and also avoids a risk to the auditor of failing to grasp a ROMM by concentrating excessively on individual relatively basic accounting tasks.

Standback requirement is applied to material classes of account balances, transactions, or disclosures that have been initially deemed not significant (due to the lack of a relevant assertion) where the auditor reevaluates their initial determination. Although not required by the standard the auditor could perform an additional stand back on any assertions deemed not relevant in material areas.

Example: An auditor has a client where cash is material to the financial statements. It is a significant account balance since the auditor has determined that cash has at least one relevant assertion. The engagement team has identified the existence assertion as **not relevant**. While not required, it may be useful for the engagement team to consider for material areas like cash in this example if the assertions deemed “not relevant” make sense.

For example, in this situation, would the engagement team feel comfortable not sending out a cash confirmation or at least looking at a bank statement on the financial institution's website? If not, the engagement team may have missed a ROMM in cash relative to existence.

Since the definition of a ROMM relies on the concept of materiality, one question that comes up at times is what that materiality should be. The AU-C is not prescriptive but provides some guidance at AU-C 320.09 with the definition of performance materiality. **Performance Materiality** is the amount or amounts set by the auditor at less than materiality for the financial statements as a whole to reduce to an appropriately low level the probability that the aggregate of uncorrected and undetected misstatements exceeds materiality for the financial statements as a whole. If applicable, performance materiality also refers to the amount or amounts set by the auditor at less than the materiality level or levels for particular classes of transactions, account balances, or disclosures. Performance materiality is to be distinguished from tolerable misstatement. AU-C 320.11 further notes that the auditor should determine performance materiality for purposes of assessing the risks of material misstatement and determining the nature, timing, and extent of further audit procedures. Practice aid vendors generally suggest 75 percent, although auditors may justify a different level. Auditors may also set materiality at different levels for different account balances/classes of transactions.

A. Revenue recognition as a significant risk

Although peer reviewers have noted a failure to appropriately identify and address management override and improper revenue recognition as significant risks of fraud, it is important to understand what this really means.

The auditor should, based on a presumption that risks of fraud exist in revenue recognition, evaluate which types of revenue, revenue transactions, or assertions give rise to such risks. The auditor is not required to apply the presumed significant risk related to fraud in revenue recognition across ALL assertions and ALL revenue. Unfortunately, however, this is a common response.

When the auditor makes this a blanket statement (revenue recognition is a significant risk of fraud) it requires the auditor to identify the controls that address this broadly stated significant risk and to perform D&I work. In addition, AU-C 330 requires the auditor to perform substantive procedures that are specifically responsive to the identified significant risk as well as a requirement to obtain more persuasive audit evidence. And further, the auditor is also required under AU-C 260, *The Auditor's Communication With Those Charged with Governance*, to communicate to those charged with governance about the significant risks identified by the auditor.

This issue is pervasive. In cases where there is a group audit, AU-C 600, *Special Considerations – Audits of Group Financial Statements (Including the Work of Component Auditors)*, requires more involvement by the group engagement partner if the significant risk relates to a component in a group audit and for the group engagement team to direct the work required at the component by the component auditor.

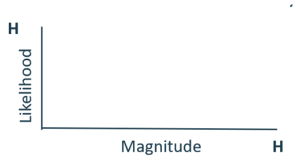
The solution is for the auditor to use the definition of significant risk in the determination of whether each stream of revenue is a significant risk at the assertion level. Only then will the work have more meaning and be streamlined. A significant risk is an identified risk of material misstatement for which the assessment of inherent risk is close to the upper end of the spectrum of inherent risk.

The **spectrum of inherent risk** is illustrated below with the additional feature. Inherent risk factors individually or in combination affect inherent risk to varying degrees and that inherent risk will be higher for some assertions than for others.

1. Case study – Revenue recognition and significant risk

Consider the following example. An entity has the revenue identified in the example below. Evaluate each class of transaction and the assertion level and identify the significant risks, if any.

What about revenue recognition. It is presumed to be a risk of fraud which would make it a significant risk. That means more focused testing- but is it **really necessary for EACH category or revenue and EACH assertion**? Materiality is $46,000.



Step 1: Look at the revenue streams
Step 2: For each where risk is identified- which assertions are high?
Step 3: Which assertions that high are the highest of the high (significant risk)?

Inherent Risk Factors
- Complexity
- Uncertainty
- Subjectivity
- Change
- Risk of fraud

Assertions
- Occurrence
- Completeness
- Valuation
- Rights and obligations
- Classification/ accuracy
- Cutoff

Revenue	
Tuition revenue	$4,000,000
Grant revenue (3 private awards)	350,000
Contribution revenue (unsolicited)	45,000
Advertising revenue	10,000
Investment return	180,000
	$4,585,000

The Center for Plain English Accounting answered the following questions on the classification of risk as a significant risk.

CPEA question: How do I decide whether a high inherent risk is or is not a significant risk?

Answer: Auditors will use the combination of likelihood and magnitude of a possible misstatement when using professional judgment to determine where on the spectrum of inherent risk a specific risk lies. It is the intersection of the magnitude and likelihood that determines whether the risk is significant.

CPEA question: My audit practice consists of auditing small entities that are very simple businesses. Is it possible not to have any significant risks?

Answer: Significant risk is not related to the size of an entity but on the likelihood and magnitude of misstatement **without considering any controls the entity may have**. Revenue recognition is presumed to be a significant risk. And fraud risks are considered significant risks.

Substantive testing and significant risks

a. With a significant risk, the auditor cannot just use substantive analytical procedures (SAP) to test.
b. The requirements are either using tests of details alone or in combination with tests of controls and SAP, or a combination of tests of controls and SAP.
c. Tests of details for many sources of revenue could be prohibitive since revenue tends to be homogenous and there are few significant items.

Revenue Audit Sample Sizes – Example

Assuming a revenue amount of $100,000,000 and applying a common audit methodology, the sample size computation can result in an unwieldy sample size. Plus, the sample may need to be expanded if any errors are expected.

Tolerable misstatement = $510,000 (using a formula)

Sample size = $100,000,000/$510,000*3.0 risk factor

Sample = 588

Clearly, a sample size of 588 is unwieldly, and a more efficient approach is desired. If any misstatements not planned for are identified in the sample after auditing the items, the original sample size of 588 is inadequate to meet the auditor' s desired risk protection.

Note: The risk factor is high risk of material misstatement and other high other procedures risk.

Rebutting the presumption and lowering the risk to reduce large samples

SAS 145 notes that the presumption that revenue recognition is a significant risk can be rebutted. To do that, however, requires the auditor to have a bona fide reason. Consider the three conditions generally present when fraud occurs – incentive/pressure, opportunity, and rationalization/attitude. Then consider:

a. Nature of the entity's revenue streams. Are they limited and "scheduled" or simple in nature?
b. Level of complexity involved in recognizing revenue. Is recognition under FASB ASC 606 straightforward (e.g., recognition occurs upon delivery of a product or service) or more complicated (e.g., difficult determination of transfer of control of a promised asset or service)?

Documentation is important here when rebutting the presumption. Look at the solution to the case study earlier in this chapter for documentation suggestions.

Rebutting the presumption helps to lower the risk and thereby lower the sample size for testing revenue. In addition, there are other strategies that could help:

a. Lower the risk factor by testing controls and performing other procedures. But the sample size is still going to be large. ($100M/$510K = 196 X .9 = 176)
b. Evaluate risk – can the presumption of high risk be overcome?
c. The risk related to revenue streams, like an entity that sells a limited number of products and gives no price concessions where there are few noncomplex payments, is very different from, for example, a healthcare entity with a complex revenue stream or a construction contractor where estimates are heavily involved.
d. A revenue stream that is predictable such as tuition in an independent school is a predictable stream. A revenue stream that is less predictable may be an entity that sells custom products that are individually priced.

Ask the right questions

Revenue accounts are usually related to other accounts such as cash, accounts receivable, contract assets, contract liabilities, and sometimes inventory. Some auditors look at accounts in the balance sheet and the income statement in isolation and fail to consider the inter-connectedness of other accounts. That approach can lead to extra work and inefficiency. By focusing on the connectivity or relationships between revenue and other related accounts, the auditor gains opportunities for auditing revenue more effectively and with less extensive procedures. For example, if a client had fictitious revenue amounts, where would it show up in other places within the financial statements? Perhaps it would be the allowance for credit losses. It is likely, it also would be reflected either in missing cash or excess receivables.

Look at the stream. In the healthcare example, this may not work as well since the risk of fraudulent upcoding might not be detected until sometime later (under payor audit). But with other revenue streams, it would likely show up in past due receivables. If the auditor performs responsive procedures when auditing these accounts, then they should support the existence assertion in the revenue account. Are the cash receipts from revenue in line with the asserted amounts in the revenue account? Look for those relationships and use the audit work being performed on those other accounts, as that may provide evidence related to existence/occurrence in revenue.

The AICPA's Revenue Recognition Guide notes that if the existence of revenues is mostly satisfied through procedures performed in accounts receivable and cash and analytical procedures, then less direct testing of revenues for the existence assertion may be warranted. Taking credit for audit work related to the existence/occurrence assertion for receivables and cash also can serve as evidence of the occurrence of reported revenues. For example, internal audit procedures or regulatory audit procedures may provide existence evidence.

B. Summary of the risk assessment process

The **risk assessment process** can be summarized in 10 steps. Each of the steps is important in gathering the data points necessary to conclude on the places where the risk of material misstatement is present and linking that assessment with the appropriate further audit procedures. This chapter will address these areas along with other weaknesses noted in AICPA risk alerts and among peer reviewers throughout this chapter.

The **objective** of the risk assessment process is to perform **risk assessment procedures** to provide a basis for the identification and assessment of risks of material misstatement at the financial statement and relevant assertion levels.

To summarize the steps in the risk assessment process:

Step 1: **Make inquiries** of management and other members of the client team who may have information that can assist in identifying risks of material misstatement due to fraud or error. The purpose of these inquiries is to develop an understanding of the entity and its environment relevant to the audit. **Assess** prior experience with the entity as well as results of audit procedures performed in prior audits. The assessment of prior experience is documented, in part, in the client continuance form. Obtain an understanding of internal control as discussed in AU-C 315 (as amended by SAS 145). This will consist of inquiries, corroborative inquiries, review of documents, and observations.

Step 2: **Perform** preliminary analytical procedures on financial and nonfinancial **information**. This step will assist the auditor in understanding the entity and its environment, and to identify areas that may present risks of material misstatement due to fraud or error. Remember that more focused analytical procedures should be performed on revenue. This is a fraud risk requirement.

Step 3: **Make inquiries** of management, those charged with governance and others to assist in **identifying** the risk of material misstatement due to **fraud**. Perform other procedures to understand the risk of fraud such as inspection of journal entries, evaluation of significant estimates and the rationale for unusual business transactions. Conclude on the risk of fraud related to revenue recognition and management override of controls.

Step 4: **Identify** the entity's significant accounting processes including the financial reporting process and those that are outsourced and understand internal controls. (See further discussion in the next chapter). The understanding of internal controls also encompasses entity level controls. The auditor is required to evaluate the risk of IT and determine the level of understanding necessary.

Step 5: **Perform D&I for those areas required by SAS 145 and any other controls the auditor wants to identify as important or "key."** In performing D&I the auditor is evaluating the design of controls and determining that they have been implemented.

The auditor is required to perform D&I for controls over significant risks, over journal entries, in areas where the auditor is required to test controls or plans to test controls as part of their audit strategy, and over general information technology.

The auditor should determine whether to test internal controls. Controls may be tested at this time or later but the results of tests, if performed, will be used in the risk assessment process.

Step 6: **Accumulate** the data points on risk identified in the preceding steps and **conduct discussions** with the engagement team, brainstorming where the entity's financial statements are susceptible to material misstatement due to fraud or error. Identify overall financial statement risks (e.g., management override, lack of segregation of duties, ineffective management oversite) and identify significant and fraud risks so they can be specifically documented. Conclusions will be summarized in the risk assessment summary form.

Step 7: **Assess risk** at the overall level. **Assess** inherent risk at the account balance/class of transaction and assertion level. Be sure to identify elements used to assess inherent risk and the rationale for the risk. If there are no relevant assertions then the account balance/class of transaction is not significant and inherent risk is not assessed.

Step 8: **Assess** the risk of material misstatement at the account balance **and** assertion level as high, moderate, or low based on the results of step 7 **and** the results of work on internal control. Ensure that significant and fraud risks are identified. Assess the risk of material misstatement at the overall financial statement level, that is, those risks that cannot be identified as specific to an account balance and assertion.

Step 9: **Develop tailored audit procedures** to be responsive to the risks of material misstatement and link them to the overall risks of material misstatement, the significant risks and the level of risk identified in the other account balances and classes of transactions at the assertion level.

Step 10: **Document** the results of the risk assessment process, including:

a. Significant decisions reached in engagement team discussions, as well as timing of those discussions, and audit team members who participated in those discussions; and

b. Key elements associated with obtaining an understanding of the audit client, its environment, internal control components as well as the sources from which the understanding was obtained, and the risk assessment procedures performed.

c. Risk of material misstatement is assessed at both the financial statement and relevant assertion level. Where there are significant risks, it is important to obtain an understanding of the internal controls related to those risks (i.e., fraud risk, risks associated with significant related-party transactions, economic and accounting matters, etc.).

Revisions to the risk assessment should be made during the audit when additional audit evidence, or new information is obtained that produces inconsistencies with the audit evidence upon which the auditor originally based the assessment. The auditor should make sure to reflect these changes in the nature, timing, and extent of procedures performed and also document it on the risk assessment form.

III. Issues related to the risk assessment process identified by peer reviewers and others

Every year the AICPA issues peer review alerts. This next section identifies matters for further consideration (MFC) that were observed by peer reviewers in engagements with year ends between March 1, 2023, and June 30, 2024.

A. Peer review issue #1 – Failure to communicate or document the communication between the auditor and those charged with governance

The auditor is required by AU-C 260, *The Auditor's Communication with Those Charged with Governance*, to communicate with those charged with governance during the audit. The standards note three separate instances although if there were a need to communicate more frequently the auditor should make those communications. Professional standards do not require that this communication be in writing, only that it be documented.

Planning communication: This communication should be conducted at the **beginning of the audit** as a planning activity. The purpose is to communicate the auditor's responsibilities regarding the financial statement audit and the planned scope and timing of the audit. The communication needs to include:

a. That the auditor is responsible for forming and expressing an opinion about whether the financial statements that have been prepared by management with the oversight of those charged with governance are prepared in all material respects in conformity with the applicable financial reporting framework;

b. That the audit of the financial statements does not relieve management or those charged with governance of their responsibilities; and

c. Planned scope and timing of the audit, including significant risks identified by the auditor. The requirement relative to identification of significant risks is the newest of the requirements. It became effective for calendar year 2021 audits.

If the entity is privately held and those charged with governance are members of management then the communication is generally found in the engagement letter. The initial communication has not been a concern with peer reviewers except in instances where those charged with governance are not members of management. In those cases, it is important that the engagement letter, if that is the preferred method of communication for the engagement team, be addressed to the members of the board.

Inquiries of governance – The auditor is to make inquiries of those charged with governance regarding the risk of fraud. Unless all of those charged with governance are involved in managing the entity, the auditor should obtain an understanding of how those charged with governance provide oversight of management's processes for identifying and responding to the risks of fraud as well as the internal control that management has established to mitigate these risks. The auditor should also discuss whether those charged with governance have any actual, suspected, or alleged fraud affecting the entity as well as their views about the risk of fraud. The information obtained can be used to corroborate information obtained in discussions with management. The documentation of this information is very important.

Certain new requirements may be overlooked because they were recently added by SAS 135 related to inquiries and other procedures concerning those charged with governance, significant unusual transactions, and related parties:

a. The auditor is required to provide their views relating to the entity's significant unusual transactions to those charged with governance. This may include the auditor's views on the policies and practices management used to account for significant unusual transactions and the auditor's understanding of the business purpose for significant unusual transactions.
b. The auditor is also required to discuss the potential effects of uncorrected misstatements on future-period financial statements and report, to governance, matters that are difficult or contentious where the auditor consulted outside the engagement team. This provides information to those charged with governance that may be useful in their oversight role.
c. Unless all of those charged with governance are involved in managing the entity, the auditor is required to obtain, from those charged with governance, the audit committee or, at least, its chair, regarding their understanding of the entity's relationships and transactions with related parties that are significant to the entity as well as whether any of those charged with governance have concerns regarding relationships or transactions with related parties and, if so, the substance of those concerns.

Final audit communication – This communication generally takes the form of a written communication such as a letter or a formal presentation document. The objective of this communication is to provide those charged with governance with timely observations of significant matters that arose during the course of the audit that are significant such as the auditor's views about qualitative aspects of the entity's significant accounting policies, estimates, and disclosures. The auditor will also note whether there have been any disagreements with management, significant difficulties encountered during the audit, significant findings, and significant matters where management consulted with other accountants on accounting or auditing matters. The auditor will also report uncorrected misstatements that are immaterial both individually and in the aggregate to the financial statements as well as material corrected misstatements. The communication also references representations provided by management. This communication has generally not been an issue noted in peer reviews.

B. Peer review issue #2 – Failure to properly perform/document preliminary analytical procedures

AU-C 315 discusses the requirement to perform preliminary analytical procedures during the risk assessment process in order to enhance the auditor's understanding of the client's business, significant transactions and other events that have occurred during the year. The purpose is to identify areas that might indicate the presence of risk whether due to error or fraud. The auditor will investigate the unusual relationships between what they expected to occur based on inquiries with the client, board, and understanding of the industry. Since preliminary analytical procedures are performed at a high level with aggregated data the observations that come from this analysis will probably only provide directional information.

The amendments to AU-C 315 state that the auditor is not required to perform the analytical procedures performed in the risk assessment process in accordance with AU-C 520. AU-C 520 requires a level of precision in expectations and measurement of the expectation to the actual account balance, including testing management's explanations for the differences. However, it is still important to understand that the definition of analytical procedures is "evaluations of financial information through analysis of plausible relationships among both financial and nonfinancial data." This implies some level of expectation to be developed.

The auditor has discretion in how they perform the procedures. The most common procedure is a fluctuation analysis. AU-C 520 provides guidance that may be helpful in performing analytical procedures. The more precise the expectation or disaggregation of data, the more likely it is that the auditor will be able to identify a risk of material misstatement. The auditor gains information to develop an expectation from reading board minutes, having discussions with client personnel (including conversations with those charged with governance), and possessing knowledge of industry information.

1. Analytical procedures should include those relating to revenue accounts

One element of the fraud procedures that relates to preliminary analytical procedures is to perform them on revenue. AU-C 240 says that, based on analytical procedures performed as part of risk assessment procedures, the auditor should evaluate whether unusual or unexpected relationships that have been identified indicate risks of material misstatement due to fraud. To the extent not already included, the analytical procedures should include procedures relating to revenue accounts.

Example: An audit staff member on the audit of a small entity with a lack of segregation of duties prepared a fluctuation to serve as preliminary analytical procedures to meet professional standards. The audit staff member set a scope to examine all fluctuations identified that were greater than a specified scope. The audit senior reviewed the work, noting that it was performed at an aggregate level. The senior wrote a review comment asking the staff member if they had performed any analysis of revenue. The staff member was not aware that this was a requirement. The senior told them that it was not required by the risk assessment standards but by AU-C 240 since revenue recognition is presumed to be a risk of fraud. She further noted that procedures performed during planning provide the auditor with another data point to use to assess risk. The senior further suggested the following procedures be performed:

a. A comparison of sales volume, as determined by recorded revenue amounts, with production capacity.
b. A trend analysis of revenues by month and sales returns by month, during and shortly after the reporting period.

C. Peer review issue #3 – Inappropriate documentation of the risk of fraud including testing of journal entries

Auditors appear to have confusion around the testing of journal entries. The auditor tests journal entries as part of the consideration of fraud related to management override. Other tests of management override include evaluating management estimates and significant unusual transactions. SAS 135 places additional emphasis on this area. The requirements for testing are identified in AU-C 315 and AU-C 240.

As highlighted in SAS 145, the auditor is required to understand the controls around journal entries, including those that are nonstandard and used to record nonrecurring, unusual transactions or adjustments. The auditor is also required to examine material journal entries and other adjustments made during the course of preparing the financial statements. Sometimes entries are posted directly to financial statement drafts. During the testing, the auditor is required to:

a. Obtain an understanding of the entity's financial reporting process and controls over journal entries and other adjustments and conclude on the suitability of design and implementation of the controls;
b. Make inquiries of individuals involved in the financial reporting process about inappropriate or unusual activity relating to the processing of journal entries and other adjustments;
c. Consider fraud risk indicators, the nature and complexity of accounts, and unusual entries processed;
d. Select journal entries and other adjustments made at the end of a reporting period; and
e. Consider the need to test journal entries and other adjustments throughout the period.

It is important to remember to evaluate journal entries for their business purpose and whether the transactions represented by the journal entry are unusual. Another attribute that is important to consider is their approval.

1. Test Yourself exercise 1

An auditor was performing a review of journal entries to comply with AU-C 240, *Consideration of Fraud in a Financial Statement Audit*. The objective of the review of the journal entries is to address, in part, the risk of management override of controls. The auditor tested journal entries made during the financial reporting process. She also tested other adjustments made at the end of each quarter when certain metrics were calculated, for indications of possible material misstatements due to fraud. The audit program required the auditor to perform the following steps:

Step 1: Obtain an understanding of the entity's financial reporting processes and the internal controls over journal entries and other adjustments. Make inquiries of personnel who process journal entries about inappropriate activity that may have taken place.
Step 2: Identify and select journal entries and other adjustments made during the financial reporting period for testing.
Step 3: Based on the risk factors identified, determine the need for testing entries throughout the period.
Step 4: Document the results of the test and conclude on whether there are any indications that there are possible material misstatements due to fraud.

The audit staff person signed off on each of the steps (1–4) and documented that the step was performed. Was this enough documentation to comply with professional standards?

D. Peer review issue #4 – Failure to discuss the risk of fraud with governance

AU-C 315 states that the auditor should make inquiries of management, those charged with governance and others to assist in identifying the risk of material misstatement due to fraud. This is just one of several procedures identified in AU-C 240 related to consideration of the risk of fraud. Peer review comments are noted primarily in the area of failure to hold discussions with members of the board (or whatever body serves as those charged with governance) about their perceptions of the risk of fraud and whether they have knowledge of any actual, suspected, or alleged fraud.

It is important to remember that the primary responsibility for the prevention and detection of fraud rests with both those charged with governance of the entity and management. Where there is no board of directors or other governing body other than management, questions should be addressed to different individuals in management. However, where there is oversight by an oversight body the audit would have these discussions with that body to better understand the potential for override of controls or other inappropriate influence over the financial reporting process. There have been numerous high-profile frauds where override of internal controls, manipulation of accounting estimates or recording of inappropriate journal entries has occurred in order to improve financial results, ratios for debt covenants, etc.

When discussing the risk of fraud with those charged with governance the auditor can use the opportunity to ask the board member, audit committee chair, or other governance representative if there is anything the board feels is important for the auditor to consider or focus on in the audit. This question often yields a very effective discussion about various forms of risk (including the risk of fraud), internal controls, new accounting pronouncements and even succession planning for senior executives. Members of the board may not have a good understanding of how management could override controls. Frequently the transactions initiated by senior executives are not even reviewed.

As noted above, SAS 135 expands the inquiries that are required to be made to those charged with governance focusing on significant unusual transactions and related parties. SAS 134 requires additional communication as well related to significant risks.

E. Peer review issue #5 – Auditors are failing to identify at least one significant risk

Peer reviewers have reported that auditors are failing to identify at least one significant risk in the risk assessment process. Even if the entity has exemplary controls, AU-C 315.28 states that when making the assessment auditors should exclude the effects of controls related to the risk.

Management override is **always** a risk of fraud. No matter the size, complexity, or sophistication of an entity, the risk of management override of controls is always going to be present. There are many ways that management override can occur (e.g., journal entries, through bias in estimates, and by actions on the part of management), and it is not always possible to predict how it will happen.

AU-C 315 states that auditors are not required to evaluate overall financial statement risks to determine if they are significant risks.

Revenue recognition is presumed to be a significant risk for at least one assertion. The auditor can rebut this presumption. For example, if the entity had one source of revenue with a few large checks coming in,

then it may be a nonissue. As mentioned earlier, the auditor is expected to perform analytical procedures, specifically on revenue.

There is a level of risk in all financial statement account balances and classes of transactions. Some account balances/classes of transactions and assertions have more risk than others.

1. Significant risk

Not all significant account balances or classes of transactions are considered significant risks, and a significant account balance or class of transactions may have only one or two relevant assertions. Inherent risk factors are described below.

Inherent risk factor	Condition or event
Complexity	• Regulatory factors – Subject to complex laws and regulations. • Business model – Existence of joint ventures or complex alliances. • Financial reporting framework – Accounting measurements that involve complex processes such as inventories of a paint manufacturer.
Subjectivity	Financial reporting framework – Wide range of management criteria for accounting estimates such as for construction income and expenses
Change	• Economic conditions – Operations in unstable regions with high inflation; • Customer loss; • Volatile markets; • Going concern and liquidity issues; • Changes in the supply chain; • Geographic expansion; • Changes in key personnel; • Changes in the IT environment; • Installation of new IT systems; and • New constraints on the availability of capital and credit.
Uncertainty	Pending litigation and contingent liabilities
Susceptibility to management bias or other fraud risk factors	• Opportunities to engage in fraudulent financial reporting; • Transactions with related parties; • Significant amount of nonroutine, nonsystematic transactions; and • Transactions based on management's intent, such as assets to be sold or classification of marketable securities.

Auditors use professional judgment to determine which of the assessed risks of material misstatement are close to the upper end of the spectrum of inherent risk and, therefore, are significant risks. However, there are risks that are specified in another AU-C section (AU-C 240 and AU-C 550) as those to be treated as significant risks. They are related parties and significant unusual transactions.

A significant risk is a risk that is at the high end of the spectrum of inherent risk as illustrated earlier. To better understand this, the auditor could create a graph and identify where the risk would fall in terms of likelihood and magnitude. This is not required documentation.

Following are examples of where significant risk might arise:

a. Transactions for which there are multiple acceptable accounting treatments such that subjectivity is involved;
b. Accounting estimates that have high estimation uncertainty or complex models;
c. Accounting for unusual or complex transactions (for example, accounting for revenue with multiple performance obligations that are difficult to value);
d. Emerging areas (for example, accounting for digital assets);
e. Complexity in data collection and processing to support account balances;
f. Account balances or quantitative disclosures that involve complex calculations;
g. Accounting principles that may be subject to differing interpretation; and
h. Changes in the entity's business that involve changes in accounting (for example, mergers and acquisitions).

F. Peer review issue #6 – Auditors are performing risk assessments at the overall account balance level rather than at the relevant assertion level

AU-C 315.26 states that the auditor is required to assess risk for account balances and classes of transactions at the relevant assertion level. A relevant assertion is one that has a reasonable possibility of containing a material misstatement. Peer reviewers have noted that some auditors are making a blanket assessment assuming that all assertions are the same.

Example: An auditor was evaluating the risk related to accounts receivable. She noted that revenue transactions were routinely processed (existence) and there were rarely any adjustments. However, the procedures around completeness/cutoff were not on the client's priority list. The team frequently proposed adjustments to record revenue and the corresponding account receivable for the last days of the period.

When evaluating the risk of management override the auditor was aware that in the past there was a significant number of slow paying customers. Based on the preliminary analytical procedures it appeared that the receivables continued to deteriorate from the prior year. The auditor had no question about rights and obligations related to accounts receivable.

Performing the procedure of assessing risk by assertion yielded a very different result than if the auditor assumed that all assertions had the same risk.

It is also important to remember that if the auditor does not test controls and conclude that the control risk is less than high, control risk will be set at high. This also means that the assessed level of inherent risk will become the overall risk of material misstatement. An example of risk assessment documentation follows. Note that the example illustrates a new level of risk H-E (high elevated). This is not prescribed in the standard but was noted as a possibility in an AICPA alert from the Center for Plain English Accounting.

The auditor has the responsibility to discuss their evaluation of inherent risk when it is less than high. There is leeway in the form of documentation. Some firms use space within a practice aid to document the rationale for inherent risk. Others find that a separate word document makes it easier to review the risk assessment documentation. This is a firm choice and not illustrated in the example below.

G. Peer review issue #7 – Auditors are not adequately documenting the rationale for the assessment of inherent risk

The AICPA has stressed in its recent communications to peer reviewers on risk assessment that auditors should document their assessment of inherent risk in more detail. Many auditors are documenting their inherent risk assessment as high, moderate, or low but are not discussing the rationale for the assessment. The AICPA's risk assessment audit guide goes into additional detail as to the consideration points that could be used to assess inherent risk. Different commercial practice aid vendors have prepared documentation templates for firms to use to document the rationale. As noted earlier, the rationale for inherent risk could be documented in words in the risk assessment document itself, in a separate document in words, or through use of a chart.

H. Peer review issue #8 – Auditors are setting control risk at less than high without testing the effectiveness of controls

The only way to assess internal control at a value less than high is to test controls. The auditor is required to obtain an understanding of internal controls by evaluating the design of the controls and whether they have been implemented. This is not considered a test of controls. Tests of controls require evidence that the controls are operating throughout the period under audit.

Some auditors are testing the entity controls and considering this sufficient to reduce control risk below high. This is not appropriate. Entity controls are foundational but are not sufficient to reduce control risk at the relevant assertion level.

1. Test Yourself exercise 2

1. Auditors only need to assess risk for significant account balances/classes of transactions and for their relevant assertions.

   True or False

2. Auditors should document the basis for their risk assessment only if either control risk or inherent risk is set below high. Otherwise, they can carry forward the assessment from the prior year.

   True or False

3. The auditor can combine the assessment of inherent and control risk if they believe that the two are the same.

   True or False

4. The auditor should assess inherent risk for each relevant assertion separately.

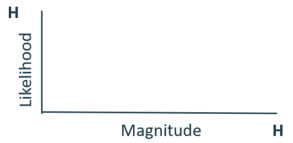
   True or False

IV. Case study and Test Yourself exercises – Solutions

A. Case study – Suggested solution

Consider the following example. An entity has the revenue identified in the example below. Evaluate each class of transaction and the assertion level and identify the significant risks, if any.

What about revenue recognition. It is presumed to be a risk of fraud which would make it a significant risk. That means more focused testing- but is it **really necessary for EACH category or revenue and EACH assertion**? Materiality is $46,000.



Step 1: Look at the revenue streams
Step 2: For each where risk is identified- which assertions are high?
Step 3: Which assertions that high are the highest of the high (significant risk)?

Inherent Risk Factors
- Complexity
- Uncertainty
- Subjectivity
- Change
- Risk of fraud

Assertions
- Occurrence
- Completeness
- Valuation
- Rights and obligations
- Classification/ accuracy
- Cutoff

Revenue	
Tuition revenue	$4,000,000
Grant revenue (3 private awards)	350,000
Contribution revenue (unsolicited)	45,000
Advertising revenue	10,000
Investment return	180,000
	$4,585,000

Tuition: The auditor considered each revenue stream. Tuition revenue was deemed to be a significant account balance because of the risk of fraud. Tuition was not complex, but there was some subjectivity to it related to scholarships that were provided by the school. The auditor believed that there was more than a remote possibility that the calculations for scholarships could be misapplied and improper aid provided. Since the scholarships were numerous and could run up to $25,000 a year for each scholarship a material misstatement could result. The auditor further believed that this could be a risk of fraud. **Assertion affected:** completeness and valuation. Rights and obligations are also not relevant. ***Due to risk of fraud, revenue recognition is a significant risk for completeness and valuation.***

Grant revenue: Grant revenue consists of three amounts. The revenue is expected at a certain amount so there is no uncertainty. There is no subjectivity. There is no change or risk of fraud. The account is not complex. The grants are all operating grants which means they are not conditional. **There were no relevant assertions**. It is not more than remote that there could be a material misstatement. There is some risk as it relates to the valuation of contribution receivable but that is handled in the analysis of another account balance. Rights and obligations is also not relevant. ***Revenue recognition is a not significant risk.***

Unsolicited contribution revenue: The balance is less than materiality so it is more than remote that there could be a material misstatement related to occurrence, completeness. Although it is possible that a check could be stolen and revenue could be understated, the unsolicited contributions are very small. Further, the process involves cash coming to a lockbox so the only possibility of a check being stolen would be slight as checks coming directly to the entity by other means would be rare. Valuation is not relevant due to the fact that unsolicited contributions are cash. Classification and accuracy are not relevant since the amounts of the individual items are so small and this is not a complex area. No subjectivity, no uncertainty, no change. Rights and obligations is also not relevant. ***Revenue recognition is a not significant risk.***

Advertising revenue: This is a peripheral activity and not material. It is not more than remote that there could be a material misstatement in any assertion. ***Revenue recognition is a not significant risk.***

Investment return: The investments are managed by a third party service provider and it is a discretionary money management relationship. It is more than remote that due to the fact that management only records the investment activity from a report provided by the third party, that there could be a risk of material misstatement due to cutoff, completeness accuracy, and occurrence. Investment return comprises gains/losses that are realized and unrealized. Valuation is an assertion associated with the account balance. Rights and obligations is also not relevant. Although there are relevant assertions, **none are significant risks as they are not at the upper end of the inherent spectrum.**

B. Test Yourself exercise 1 – Suggested solution

The audit staff person signed off on each of the steps (1–4) and documented that the step was performed. However, this is not enough documentation to comply with professional standards. An experienced auditor needs to be able to understand the work behind the steps performed. Reviewers have observed that some auditors are considering sign offs as adequate work. Documentation to support the auditor's consideration could take the form of:

a. Discussion of the types of journal entries made by the entity.
b. Internal controls over journal entries could be documented on this workpaper or as part of the financial reporting process.
c. Assessment of completeness of the population (financial statement level, automated, ad hoc JEs made during the year).
d. Journal entries that were selected for testing with characteristics (purpose, amount, etc.).

The tick mark explaining the conclusion about each journal entry should discuss whether the journal entry represented a transaction with a bona fide business purpose, was supported, approved and whether there was anything about the entry that gave the auditor an indication that the risk of fraud was present.

C. Test Yourself exercise 2 – Suggested solution

1. Auditors only need to assess risk for significant account balances/classes of transactions and for their relevant assertions.

   False. The auditor should perform risk assessment procedures at the **overall financial statement** and **relevant assertion** levels. The overall financial statement risks do not need to be identified as significant risks since they are pervasive. Properly assessing a client's risks gives the auditor the necessary basis for designing an audit plan that responds to those risks. (AU-C 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement.*)

2. Auditors should document the basis for their risk assessment only if either control risk or inherent risk is set below high. Otherwise, they can carry forward the assessment from the prior year.

   False. The auditor should perform the risk assessment procedures and document the results of each analysis yearly. One issue that has surfaced in review is that auditors are carrying forward risk assessment documentation to save time but failing to make the modifications necessary to address the circumstances in the current year.

3. The auditor can combine the assessment of inherent and control risk if they believe that the two are the same.

False. Auditors have been cautioned by the AICPA that although the guidance discusses inherent risk and control risk as the risk of material misstatement when combined, in order to properly document the assessment, the two must be identified separately. Inherent risk needs further documentation so that an experienced auditor with no previous connection to the engagement can understand the factors that went into the inherent risk assessment. Control risk should be supported by the understanding and/or tests of controls. If the auditor does not test controls and find them to be effective at some level, then control risk is assessed at high, and the value at which inherent risk is assessed becomes the risk of material misstatement.

4. The auditor should assess inherent risk for each relevant assertion separately.

True. AU-C 315 states that the auditor should identify and assess inherent risk at the account balance and assertion level. The risk is not always the same for each assertion supporting an account balance. For example, AU-C 315 explains that the existence and accuracy assertions may not contain the same level of risk as the valuation assertion. The valuation assertion has a level of subjectivity to it so it is susceptible to management bias and the risk of fraud. The existence assertion may have more complexity in inventory work in process accounts than in accounts payable.

Understanding Internal Control

Understanding Internal Control

Learning objectives

Upon reviewing this chapter, the reader will be able to:

- Identify the changes in internal control from 2013 and beyond;
- Understand the professional standards related to internal controls and where peer reviewers are noting deficiencies; and
- Identify and implement best practice techniques and documentation for key elements of the risk assessment process.

I. Internal controls – Very important and ever-evolving

A. Brief history

Internal control is an important part of a company's systems and processes. Its purpose is to safeguard assets, verify financial records, monitor organizational performance, and ensure efficient and uninterrupted operations. Although entities have had controls over their systems and processes since ancient times and auditing standards have been in place since 1917, the first significant internal control framework was drafted by the Committee of Sponsoring Organization (COSO) in response to the 1977 Foreign Corrupt Practices Act. It was published in 1993.

Audit standards require that the auditor obtain an understanding of the entity and its environment, which includes its internal control. The understanding is based on a recognized framework and although COSO is not the only recognized framework available it is the most widely used in the United States. The guidance set forth in AU-C 315 states that the auditor should obtain an understanding of all five elements of internal control at a sufficient level to assess the risks of material misstatement, and to be able to design the nature, timing, and extent of further audit procedures. At this time nonpublic entities, and small public ones are not required to have an audit of internal control under Sarbanes-Oxley Section 404. In fact, auditors are not required to test internal controls over financial reporting, even under Government Auditing Standards except when controls are in electronic form and/or the auditor is unable to gain enough assurance with substantive testing alone. Auditors are required to test internal controls under other circumstances such as a compliance audit under the OMB's Uniform Guidance.

Internal controls have evolved with changes in technology, global markets, complexity of transactions and other factors so much so that in 2013 COSO revised its integrated framework to reflect these and other changes. Major changes to the framework at that time were in the areas of:

a. Expectations for governance oversight;
b. Globalization of markets and operations;
c. Changes and greater complexities in laws, regulations, and standards;
d. Expectations for competencies and accountabilities;
e. Use of and reliance on technology; and
f. Expectations relating to preventing and detecting fraud.

The COSO Framework, which embodies the five elements of control[1], is the most commonly used framework to evaluate an entity's internal controls.

[1] The five elements are the control environment, risk assessment process, information and communication, monitoring, and control activities.

Significant changes in the business environment since 2013 have necessitated additional changes in internal controls on the part of more complex entities. Even smaller less sophisticated entities have found it necessary to evaluate their information security controls considering the cyber-fraud activity in the environment. In addition, many smaller entities are embracing paperless systems, which increases the likelihood of tests of controls for some significant account balances. Auditing standards are changing as well. SAS 142, effective for calendar 2022 year ends was modified to describe the evidence that is important to collect to correspond to the new techniques and technologies in use today. Advanced data analytics and artificial intelligence are being used by auditors and clients today.

The auditor's work related to understanding internal control has been revised in SAS 145. Peer reviewers noted issues in the auditor's work performed in internal control. The AICPA issued SAS 145, in part, to clarify certain concepts and make revisions to others.

1. Elements of internal control

The term **internal controls** is defined as a process effected by those charged with governance, management, and other personnel that is designed to provide reasonable assurance about the achievement of the entity's objectives with regard to the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. Internal control over safeguarding of assets against unauthorized acquisition, use, or disposition may include controls relating to financial reporting and operations objectives.

The AICPA believed that auditors were confused with the term internal control. Accordingly, SAS 145 clarified the subject by adding a **definition** of ***system of internal control*** and ***controls***:

a. **System of internal control** – The system designed, implemented, and maintained by those charged with governance, management, and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. For purposes of GAAS, the system of internal control consists of five interrelated elements.

b. **Controls** – Policies or procedures that an entity establishes to achieve the control objectives of management or those charged with governance. In this context policies are statements of what should, or should not, be done within the entity to effect control. Procedures are actions to implement policies.

The five COSO Framework elements (control environment, risk assessment process, control activities, information and communication, monitoring) are further broken down into 17 principles. When identifying controls for the auditor's understanding, the auditor should take care to select controls that support the element's objectives.

B. AICPA's clarifications on internal control

As discussed earlier, the risk assessment process was not overhauled. However, there were significant clarifications and refinements to the auditor's responsibility related to internal control. This module will discuss them. The most notable follow.

Auditor is required to understand controls over significant account balances, classes of transactions, and disclosures. SAS 145 makes the distinction between when the auditor is required to just obtain an understanding and when they are required to evaluate the design of the controls and determine if they

have been implemented. This is referred to as D&I or a walkthrough. On a recent A&A Focus webcast, Diane Hardesty, EY Managing Director and ASB Board Member, recalled a SAS 145 ASB task force meeting where five or six different interpretations existed about what AU-C Section 315 required related to evaluating the design and implementation of controls before SAS 145.

D&I work is required for:

a. Controls that address a risk that is determined to be a significant risk;
b. Controls over journal entries and other adjustments as required by AU-C 240, *Consideration of Fraud in a Financial Statement Audit*;
c. Controls for which the auditor plans to test operating effectiveness;
d. Controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence;
e. GITC; and
f. Controls that the auditor chooses to identify.

Based on the controls identified, auditors should identify the information technology (IT) applications and the other aspects of the entity's IT environment that are subject to risks arising from the use of IT.

Because of the confusion, the AICPA's Center for Plain English Accounting issued two white papers on risk assessment in April 2023. One of the white papers addressed questions that were asked related to the implementation of the standard related to internal control. A focus of the white paper was the terminology that is fundamental to understanding the standard. The following terms are used in the portion of the standard on internal control:

a. **Gaining an understanding** – Performing procedures to become knowledgeable about and aware of the entity's controls (policies and procedures) for each of the five internal control components.
   (i) Does not require the auditor to make an evaluation or determination about the system of internal control or about specific controls.
   (ii) To gain an understanding, the auditor may perform procedures such as inquiry or reading documents prepared by management or others.

Example: An auditor wanted to obtain an understanding of the control activities around cash receipts and disbursements. They inquired about the policies, procedures and controls the client used to capture, account for, and record cash in a manner that complies with GAAP. The auditor inquired about the controls the client had in place to mitigate the theft of cash. While doing this the auditor was learning about the system but was not evaluating the system or making a determination of effectiveness. They were simply understanding the controls that are present. Note that the auditor may ask to see documents or observe processes.

b. **Making an evaluation** – The auditor is required to make an evaluation of the design of the identified controls. Those are the controls identified in the standard for which more work is required.
   (i) Controls that address a risk that is determined to be a significant risk.
   (ii) Controls over journal entries and other adjustments required by AU-C 240, (consideration of fraud).
   (iii) Controls for which the auditor plans to test operating effectiveness which includes controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence.

(iv) Other controls based on the auditor's professional judgment.

(v) Entity's general IT controls and the risks arising from the use of IT.

c. **Determination** – After performing evaluation of the design, the auditor determines whether the control is properly designed to meet the control objective. If properly designed, the auditor would further determine if the control was placed in operation. Generally, once the auditor has evaluated the design, there is sufficient evidence to support that the control has or has not been implemented. The auditor is not able to rely on inquiry alone.

For each identified control the auditor makes an **evaluation** of the design of the control and a **determination** that it was implemented. The task of evaluating the design is important because a control can only be effective if it is properly designed and, if implemented, will prevent or detect and correct material misstatements. To complete the D&I the auditor would evaluate the evidence that the control was implemented. Often auditors forget that they need to document their evaluation of the **design**.

Example: The client performed monthly cash reconciliations for bank accounts. The auditor identified this as a "key control." The auditor requests two months' cash reconciliations prepared by the client and then evaluates the quality of the controls (skill in preparation, review and approval, follow up on exceptions). From this the auditor will be able to conclude that the control was **adequately designed and implemented**.

C. Entity level or indirect controls

AU-C 315 specifically states what the auditor is expected to understand relating to the entity's internal controls. It stresses that the auditor must obtain an understanding of all five levels of internal control. The entity level controls, the control environment, risk assessment, communication, and monitoring can all be documented in the form of narratives. D&I is not required here, but the narratives should address the following.

1. Control environment, understanding required

The auditor should obtain an understanding of the **control environment** relevant to the preparation of the financial statements. In this, the auditor will understand:

a. Controls, processes, and structures that address how management's oversight responsibilities are carried out (includes the entity's culture and management's commitment to integrity and ethical values).

b. The oversight of the entity's system of internal control by those charged with governance when those charged with governance are separate from management.

c. Entity's assignment of authority and responsibility.

d. How the entity attracts, develops, and retains competent individuals.

e. How the entity holds individuals accountable for their responsibilities in the pursuit of the objectives of the system of internal control.

Example: Accounting Firm spoke to _____, the _____ and based on the discussion noted that management is committed to strong ethical values. The code of ethics is distributed to Company personnel when they are hired, and each year company personnel sign off as agreeing to abide by the code of conduct and report ethical violations. Management receives a report identifying which employees have not completed this step for follow-up. The Company has a policies and procedures manual. The accounting supervisors for cash receipts/receivables and cash disbursement/accounts payable monitor the work of the clerks. There is no internal audit department, and the controller monitors to ensure reconciliations of the subsidiary ledgers to the general ledger are performed (including bank recs). This is indicated on a monthly check-off sheet that the controller receives from each accounting supervisor.

The board receives a monthly board package that includes an analytic comparison of results of operations current to prior year to date and monthly results compared to the same month in the prior year. They also receive budget to actual information. When results show anomalies, they are investigated at the request of the board.

There are only two CPAs, and they receive training to maintain their licenses, which is paid for by the Company. Other individuals in accounting receive training on changes to the accounting system or other changes of which they need to be made aware. All Company personnel receive periodic training on cyber security and other issues related to laws and regulations. The training system produces information that is reviewed by the controller to ensure that all training has occurred.

2. Risk assessment, understanding required

The auditor should obtain an understanding of the entity's **risk assessment process** relevant to the preparation of the financial statements by understanding the entity's process for:

a. Identifying business risks, including the potential for fraud, relevant to financial reporting objectives.
b. Assessing the significance of those risks, including the likelihood of their occurrence.
c. Based on the auditor's understanding of whether the entity's risk assessment is appropriate to the size and complexity of the entity, the auditor should evaluate whether there are control deficiencies present.
    (i) If the auditor identifies risks of material misstatement that management failed to identify, they should determine how the risk assessment process failed if the auditor believes it should have detected the risk.

3. Monitoring, understanding required

The auditor should obtain an understanding of the entity's process for **monitoring** the system of internal control relevant to the preparation of the financial statements. This could include ongoing as well as separate evaluations for monitoring the effectiveness of controls, identification of deficiencies, and implementing corrective action. Should the entity have an internal audit function, the auditor will understand its nature, responsibilities, and activities. In obtaining the understanding the auditor will want to identify the sources of information used in the entity's monitoring process and how management evaluates the reliability of the information they use. The auditor will then evaluate whether the entity's process for monitoring the system of internal control is appropriate to the entity's circumstances considering the nature and complexity of the entity.

4. Information and communication, understanding required

Information and communication is more complex than the other entity level controls because the information aspect also includes control activities. In addition, there may be situations, generally in more complex entities, where more work is required related to the information aspect based on risk.

The auditor's understanding specifically includes obtaining knowledge about the **flows of transactions and other aspects of the entity's information processing activities for <u>significant</u> classes of transactions, account balances, and disclosures**. This also includes communication of significant matters. However, the auditor is not required to evaluate the design or determine implementation of individual controls in this component unless, as noted earlier, they are identified as necessary for the auditor to obtain sufficient audit evidence to render an opinion on the financial statements.

The individual identification of controls to perform D&I is focused on information processing controls referred to as transaction controls. In addition, the standard requires the auditor to perform D&I on the general information technology controls (GITC).

5. Information technology controls

Application controls – Application controls are built into computer programs. They are designed to provide completeness and accuracy of information processing important to the integrity of the financial reporting process, authorization, and validity. They are specifically related to the classes of transactions and account balances.

Applications may be the general ledger system and its various interfacing modules, such as accounts receivable, accounts payable or payroll, or noninterfacing systems such as fixed asset packages or other systems that process information that ends up in financial statements. Application controls can be programmed; that is, they can be contained in the computer program or manual that is performed by a person. If the entity has an integrated ERP (enterprise resource planning) environment such as SAP, Oracle, or JD Edwards, many of the application controls will be programmed. Where the system is not so robust, the control objectives may be able to be satisfied by manual controls such as investigating exceptions or errors generated in processing.

Overall control objectives of any IT application are to ensure:

a. Complete, accurate, valid data; and
b. Output that is distributed to authorized users.

There are four broad types of application controls used to achieve the internal control objectives of the various cycles:

a. **Input controls** – These controls are designed to ensure that the data entered into the system is complete and accurate.
b. **Processing controls** – These controls are designed to ensure that data is processed completely and accurately and that data integrity is maintained while processing and in storage.
c. **Output controls** – These controls are designed to ensure that reports produced by the system are only distributed to authorized personnel.
d. **Security controls** – These controls ensure that data stored and processed by the application are protected from unauthorized access, modification, or loss.

General computer controls – General computer controls are broad and include controls over:

a. Access;
b. Change and incident management;
c. Systems development;
d. Data backup and recovery; and
e. Physical security that is related to the integrity of financial reporting processes.

They contribute to the overall reliability of the information technology and are not related to a specific application.

IT Process	Examples of General IT Controls (GITC)
Manage access	❖ **Authentication** ❖ **Authorization** ❖ **Deprovisioning - act of removing user access to applications, systems and data within a network** ❖ **Provisioning- act of granting, deploying and activating services for users in a system** ❖ Privilege. access ❖ **User access reviews** ❖ Security confirmation controls ❖ Physical controls **Controls over remote access**
Manage program or other changes to the IT environment	❖ Change management ❖ Segregation of duties over change migration ❖ Systems development or acquisition or implementation ❖ Data Conversion

IT Process	Examples of General IT Controls (GITC)
Manage IT operations	❖ Job scheduling ❖ Job monitoring ❖ **Backup and recovery** ❖ **Intrusion detection**
Manage program or other changes to the IT environment	❖ Change management ❖ Segregation of duties over change migration ❖ Systems development or acquisition or implementation ❖ Data Conversion ❖ **Installation of data tables and other changes to system.**

With many smaller entities, access control is often lacking. Fraud can result when employees have inappropriate access because it effectively eliminates segregation of duties. The auditor should make inquiries into access as to who must be evaluated to determine whether there is a deficiency. Often, lack of access control may preclude reliance on both general and application IT controls as well as certain manual controls. At a minimum, the auditor should determine that:

a. Vendors can access the system only for a short period after installation;
b. Terminated employees no longer have access to the system; and
c. When job responsibilities are changed, access to data is also changed.

6. More robust understanding of information technology

Understanding the entity's information technology (IT) and general IT controls (GITC) is an important part of SAS 145. The entity's information system may include manual as well as automated elements. The

auditor is required to identify IT applications and other aspects of the IT environment that are based on the identified controls addressing the risks of material misstatement.

In obtaining an understanding of the IT environment relevant to the flows of transactions and information processing in the information system, the auditor gathers information about the nature and characteristics of the IT applications used as well as information about the supporting IT infrastructure. This may include understanding the complexity or level of customization related to IT applications, third-party hosting or outsourcing, and the use of interfaces, data warehouses, or report writers. Emerging technology, if used by the entity, may indicate risk.

General IT controls do not need to be identified for every IT process. They are, by nature, supportive of many different applications. It is important to obtain an understanding of those controls that mitigate the risks of material misstatement.

Characteristics that may give rise to risks from the use of IT:

Less likely to give rise to IT risk	More likely to give rise to IT risk
• Standalone applications. • Volume of data is not significant. • Application's functionality is not complex. • Each transaction is supported by hard copy documentation. • Management does not rely on automated controls. • Management does not rely on the system to produce complete and accurate reports – Manual reconciliations are performed. • Auditor intends to directly test information produced by the entity as audited evidence.	• Applications are interfaced. • Volume of transactions is significant. • Functionality is complex because of automatic initiation and processing of transactions. • IT makes complex calculations. • Management relies on the application to perform automated controls.

Less Complex Entities (LCEs) – Even where the entity uses standard programs and does not modify them, general IT controls may still need to be considered.

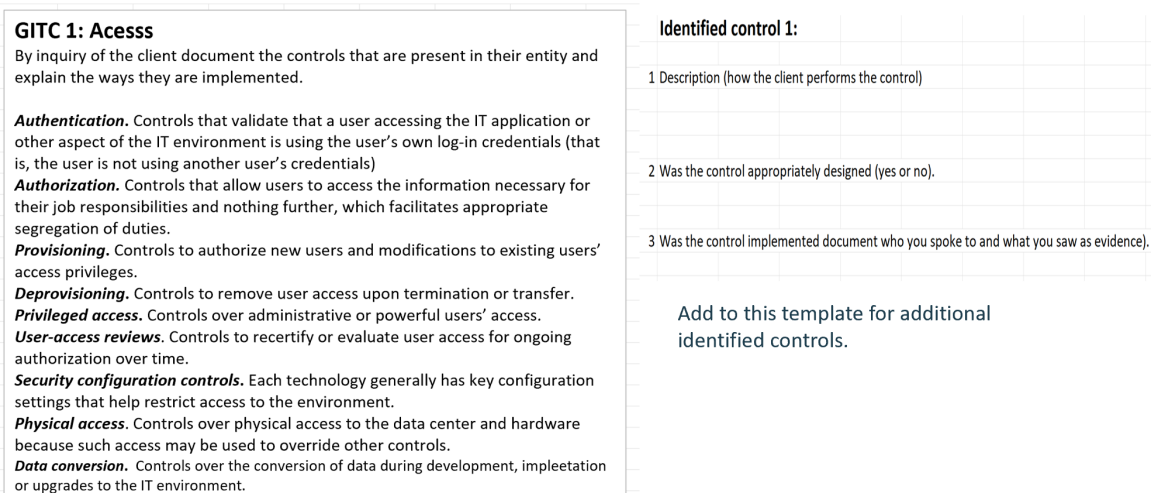
Typical general IT controls in an LCE may include the following:

a. Controls to secure logical **access** to critical applications, databases, operating systems, and networks.
b. Controls related to significant upgrades to the IT operating system or to significant packaged applications (e.g., significant upgrades are tested before they are put into production or installation of updated data tables, installation of patches and other corrections (updating system).
c. Controls to **back up** critical data and programs.

Documentation – When documenting the understanding of information technology, the auditor can use the same format illustrated to document the control environment, documenting:

a. Discussions with client personnel;
b. Review of documents such as policies and procedures; and
c. Observations of IT personnel demonstrating or performing controls.

An example documentation template follows.



GITC 1: Acesss

By inquiry of the client document the controls that are present in their entity and explain the ways they are implemented.

Authentication. Controls that validate that a user accessing the IT application or other aspect of the IT environment is using the user's own log-in credentials (that is, the user is not using another user's credentials)
Authorization. Controls that allow users to access the information necessary for their job responsibilities and nothing further, which facilitates appropriate segregation of duties.
Provisioning. Controls to authorize new users and modifications to existing users' access privileges.
Deprovisioning. Controls to remove user access upon termination or transfer.
Privileged access. Controls over administrative or powerful users' access.
User-access reviews. Controls to recertify or evaluate user access for ongoing authorization over time.
Security configuration controls. Each technology generally has key configuration settings that help restrict access to the environment.
Physical access. Controls over physical access to the data center and hardware because such access may be used to override other controls.
Data conversion. Controls over the conversion of data during development, impleetation or upgrades to the IT environment.

For most IT controls, this will be sufficient. However, the auditor should identify IT application controls where they are deemed to be "key" and evaluate their design and implementation. This step is considered an evaluation (design) and determination (implementation). In this case, the auditor would document the specific controls evaluated, including detailed information about them, along with the conclusion on the design and implementation**. Important:** The auditor would also document the identified (or key) GITC and perform the evaluation of **design and implementation**.

D. Control activities

SAS 145 refers to control activities as primarily direct controls. They are responsive to risk at the transaction level and support specific assertions (sometimes more than one). The auditor will use their understanding of the systems that process transactions to identify the key control activities (also referred to as identified controls).

SAS 145 makes a significant change to the extent of the evaluations of identified controls that must be performed. This may lead to confusion as to why the understanding of control activities does not require the auditor to evaluate the controls over each of the elements of the IT system that processes a significant dollar value or volume of transactions. The ASB believes that the understanding of the system, as defined in the CPEA whitepaper, is adequate, except in the prescribed instances below. If the auditor wants to reduce substantive testing, more controls will need to be tested.

SAS 145 is very specific in what the auditor is required to understand and specifically notes that the auditor is **required to** evaluate the design and implementation of controls over the following:

a. Controls that address a risk determined to be a significant risk;
b. Controls over journal entries and other adjustments;
c. Controls for which the auditor plans to test operating effectiveness;
d. Controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence; and
e. Other controls that, based on the auditor's professional judgment, the auditor considers to be appropriate.

As noted above, application controls arising from the risks of IT would also be considered identified controls. An evaluation should be made for those as well as GITC.

Auditors often have clients with a lack of segregation of duties. This may be a targeted risk over a specific part of the financial reporting system or may be pervasive. Either way, when an entity has this issue, the auditor may be more likely to conclude that the risk of material misstatement for certain account balances and classes of transactions is likely to be reasonably possible, thereby causing them to be included in the risk assessment process and possibly be considered in the "other control" category.

1. Walkthroughs

SAS 145 states that the evaluation of identified controls could be accomplished by a walkthrough. A **walkthrough** involves following a transaction from origination through the entity's processes, including information systems, until it is reflected in the entity's financial records, using the same documents and IT that entity personnel use. Controls are embedded in that process. The auditor would identify specific documents to review that support the client's assertions obtained in inquiry. There may be certain identified controls where this is not possible because the control is not embedded in that process but is supportive to it. For example, a bank reconciliation is performed outside the cash receipts or disbursements process. However, it is likely to be an identified control over cash.

The auditor performs a combination of the following procedures to assess the design and implementation:

a. Inquiry of entity personnel;
b. Observing the performance of specific controls;
c. Inspecting documents and reports; and
d. Re-performing the specific controls.

Inquiry is an important part of performing a walkthrough or other procedures to evaluate the design and implementation of controls. The auditor needs to determine that entity personnel understand the entity's prescribed procedures and controls, particularly for the application of manual controls. These inquiries, combined with the other walkthrough procedures, allow the auditor to gain a sufficient understanding of the process to where they are able to identify important points at which a necessary control is missing or not designed effectively.

E. Auditor's responsibilities related to cyber security

The Center for Plain English Accounting (CPEA), which is a part of the AICPA, published a white paper discussing the auditor's responsibility for Cyber Fraud in a financial statement audit.

Entities are responsible for addressing cyber security risks and implementing internal controls to address those risks. Cyber security is defined as the process of designing, implementing, and operating controls to:

a. Protect information and systems from security events that could compromise the achievement of the entity's objectives; and
b. Detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented.

An entity's cybersecurity program should identify and categorize potential security threats, implement controls designed to prevent the most significant threats whenever possible, and detect when security breaches occur so the organization can respond properly.

Auditors need to address cybersecurity risks and controls to the extent that they could materially affect the financial statements and an entity's assets. Based on that risk assessment, auditors may need to design and perform procedures to address cybersecurity risks.

Auditors focus on systems and data that could impact the financial statements. Accordingly, auditors may need to understand and evaluate controls (including logical controls) over potential access points to those systems and how those controls block and identify unauthorized access. Additionally, auditors may need to understand and evaluate how management addresses successful cyber-attacks and breaches.

Understanding the risk of cyber fraud involves asking questions of management and IT professionals at the client. Some questions the auditor should consider asking are:

a. Does the entity conduct periodic risk assessments of cybersecurity threats?
b. Have those risk assessments identified threats that could affect the financial statements?
c. Has the entity established cybersecurity policies and procedures to help prevent and detect cyber incidents?
d. Are those measures effective?
e. Are individuals at the entity assigned cybersecurity roles and responsibilities?
f. Are backups of critical data and programs maintained?
g. Does the entity have assets, such as intellectual property, that are subject to cybersecurity risk?
h. What controls exist to protect them?
i. Do controls exist to protect personal information, customer and vendor data, and other confidential or sensitive information?
j. Has the entity been victimized by a cyber-attack or breach?
k. Was there an impact on the financial statements, financial reporting systems, or data?
l. Do adequate IT controls exist, including secure logical access to critical applications, databases, operating systems, and networks?
m. Does the entity use multi-factor authentication, antivirus software, firewalls?
n. Is relevant software updated regularly?

If auditors identify cybersecurity-related risks, they should assess those risks at both the financial statement and the relevant assertion level and design an appropriate audit response. The auditor should consider the risk identified, the significance of it, and the complexity of the client's IT system. They may need to:

a. Engage an IT specialist.
b. Assign more experienced staff or those with specialized skills.
c. Determine whether IT controls can be relied on; and if relying on such controls, test them with the help of an IT specialist.
d. Determine whether compensating controls exist that can mitigate the risk of weak IT controls.
e. Emphasize the need for audit staff to maintain professional skepticism when gathering information and evaluating audit evidence, especially the reliance on information provided by the entity's system that may be used to perform analytical procedures.
f. Consider more extensive substantive testing to obtain increased audit evidence.
g. If auditors become aware of a successful cyberattack or breach at an entity, they should use judgment in determining the need to understand the nature and cause of the attack, to determine the effects, if any, on the financial statements (including disclosure).

h. Questions auditors may need to consider when they become aware of a successful cyberattack include:
   (i) Are changes to the entity's financial statements in the reporting period being audited or in future periods necessary?
   (ii) Are there any accounting impacts? (Losses, including lost revenue, expenses or liabilities related to the attack, regulatory fines, or fixing systems, contingent litigation, claims, or assessments, impairment to goodwill, if the entity's brand or reputation was damaged)
   (iii) Is disclosure of the nature and effects of the incident necessary?
   (iv) Should the initial risk assessment be revised and should further planned audit procedures be modified?
   (v) Is the cyberattack indicative of internal control weaknesses and deficiencies?

1. Exercise 1: Peer review issue identified – Primarily indirect controls

An auditor identified the following controls as important controls for their understanding of the entity's control environment. She prepared a workpaper identifying those controls:

a. Management sets the appropriate tone from the top.
b. Those charged with governance meet regularly. They review the internal financial statements at each meeting and ask questions about significant fluctuations.
c. The entity has a code of conduct and all employees are required to acknowledge that they have read it.
d. Management conducts performance evaluations of staff members.

The auditor prepared a workpaper, listing the controls and stating that management had implemented them. If you were reviewing this workpaper, what review comments would you have for the auditor? Assume that you are only reviewing the work on the control environment controls.

F. Peer review issue #1 – Auditors are not performing the appropriate level of procedures on internal control related to the financial reporting system and financial reporting process

Peer reviewers have noted that auditors are omitting critical required audit procedures related to gaining an understanding of the client's internal control over the financial reporting process. Obtaining this understanding is an important part of the risk assessment process.

The financial reporting system begins with the initiation of transactions and culminates in the financial statements that are issued. The auditor should understand but is not required to evaluate the design and implementation of:

a. The entity's information-processing activities, including its data and information, the resources to and the policies that define, for **significant classes of transactions, account balances, and disclosures**.
b. How information flows through the entity's information system, including how transactions are initiated, and how information about them is recorded, processed, corrected as necessary, incorporated in the general ledger, and reported in the financial statements.
c. How the information about events and conditions, other than transactions, is captured, processed, and disclosed in the financial statements.
d. The accounting records, specific accounts in the financial statements, and other supporting records relating to the flows of information in the information system.

e. The financial reporting process used to prepare the entity's financial statements, including disclosures.
f. The entity's resources, including the IT environment.

This includes the correction of incorrect information and how information is transferred to the general ledger. The records may be in either manual or electronic form:

a. How the information system captures events and conditions, other than transactions, that are significant to the financial statements.
b. The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures.
c. The controls surrounding journal entries, including nonstandard journal entries used to record nonrecurring, unusual transactions, or adjustments.

The understanding of the financial reporting process is often not even considered. This may be because a significant number of auditors prepare the financial statements for their clients. Erroneously, some auditors may believe that the client has no controls over the financial reporting process. For auditors to be independent of their clients, a person with the appropriate level of skills, knowledge and experience has to be appointed to oversee the nonattest (nonaudit) service, review the results of the nonattest (nonaudit) service and take responsibility for the financial statements. The financial reporting process is an important part of the financial reporting system.

The financial reporting system can include manual, as well as electronic processes. In fact, electronic processes generally have manual components to them. One example of a manual financial reporting process might be a manual review of exception to other reports. The financial reporting system can, and many times does, include electronic tools such as excel spreadsheets, where information is entered into the general ledger by journal entry. In addition, management must consider processes that they outsourced to other service providers because these are still very much a part of the financial reporting process.

The financial reporting process includes the closing process, combining or consolidating entities, evaluating significant accounting estimates and disclosures. Generally, this will take the form of a narrative on how the process is conducted along with the important controls identified, plus where the information was obtained for the understanding. In addition, auditors often do not conclude as to whether control deficiencies came to light.

G. Peer review issue #2 – Auditors are not obtaining an adequate understanding of controls over information technology (IT)

Auditors are not adequately assessing internal controls over information technology. SAS 145 addresses the auditor's need to put more effort into their understanding of the entity, its environment and internal control especially as it relates to the flow of transactions and supporting general information technology controls (GITC). GITC are controls over the entity's IT processes that support the continued proper operation of the IT environment, including the continued effective functioning of information-processing controls and the integrity of information in the entity's information system. GITC encompass several objectives and directly and indirectly they support the functioning of multiple applications in the entity's information technology system.

This consideration is especially necessary in today's IT environment since the auditor obtains a significant amount of audit evidence through data obtained from the entity's financial reporting system. Therefore, an adequate understanding of how data integrity and access to data is maintained is important. This is true even in many smaller entities, with less complex environments.

This understanding of the information system relevant to financial reporting should include relevant aspects of that system relating to information disclosed in the financial statements that is obtained from within or outside of the general and subsidiary ledgers.

Although the term general computer control (now generally referred to as information technology) is not mentioned in AU-C 315 the common understanding is that the auditor will obtain an understanding of those controls as relevant. They are:

a. Access;
b. Change and incident management;
c. Systems development;
d. Data backup and recovery; and
e. Physical security that is related to the integrity of financial reporting processes.

H. Peer review issue #3 – Auditors fail to understand which controls are relevant to an audit

Peer review findings indicate that auditors do not always obtain an understanding of which controls are relevant to an audit. SAS 145 clarified the terminology used in the risk assessment process. The term relevant is used in connection with significant account balances/classes of transactions. As noted earlier, these are the ones that have a risk of material misstatement.

The understanding of controls is only over those assertions that are relevant, and, as noted earlier, this does not necessarily involve evaluating the design of the control and determining whether it has been implemented.

Auditors should note that controls relevant to an audit that require evaluation and determination include those that:

a. Address significant risks;
b. Address risks where the auditor believes that substantive testing alone will not provide sufficient appropriate evidence (those would be tested) or the auditor wants to achieve control reliance; and
c. Support journal entries.

The auditor may identify other controls and evaluate the design and implementation of those controls that the auditor considers necessary.

I. Peer review issue #4 – Auditors have misconceptions about key controls, walkthroughs, and the level of testing necessary for control reliance

There are several misconceptions that come into play that may be causing this issue to arise:

a. Auditors are reducing control risk due to the results of the tests performed on primarily indirect controls. Auditors may understand a substantial number of primarily indirect controls. However, it is not appropriate to reduce control risk below high without also testing key control activities for significant transaction cycles.

b. Auditors are reducing control risk due to the test results of what they refer to as a disbursement test of transactions for goods/services and payroll disbursements. Often the disbursement test consists of vouching the expenditure and tying information into the general ledger related to the amount and other information and examining the document to see if there are two signatures. This type of test is also often performed on the payroll cycle tracing pay rates to employee files, withholdings to forms, etc. These attributes are very helpful in an audit but are not internal controls.

To be an effective test, relevant assertions need to be covered by internal controls. If an identified control is an approval by an authorized employee, the auditor will also want to understand whether it has been properly designed and implemented. Controls are actions conducted by client personnel. For example, if the initials of an authorized signer evidence the review of information related to a disbursement, then the auditor should conduct inquiries to ensure that they understand what the signature means rather than assume. Contrast this to the test of an attribute that is designed to ensure a disbursement was correctly coded and posted to the correct account number in the general ledger. If the auditor is performing the test and makes the determination, this is not a test of internal control. If the client personnel perform this activity and there is evidence to support that the activity was performed, then it is.

Example: An auditor was performing a test of controls over cash disbursements so he could rely on controls and reduce the level of substantive testing. He obtained a narrative that explained the process used for cash disbursements. The process is the journey that a transaction takes from initiation to authorization to processing and recording. The narrative helped him to understand the flow of the process. However, he realized that this narrative did not provide enough documentation for a complete understanding of controls. The auditor went through the narrative and identified control activities that were designed to prevent, detect, and correct misstatement on a timely basis. To ensure that his understanding was complete he identified activities performed by the client to support the appropriate authorization, safeguarding of assets and reconciliations. He also evaluated the segregation of duties. He then selected key controls to support the assertions that were relevant to the account balance/class of transactions. The auditor's objective was to evaluate the controls in place to ensure that purchases are approved, the goods or services represent bona fide obligations of the entity (i.e., that they were ordered), that the purchases were supported by source documentation evidencing receipt and the amounts are recorded accurately. He identified controls over the relevant assertions as follows:

Expense/accounts payable

a. **Occurrence/existence** – The purchase requisition is attached to the receiving document and the invoice before the expense is recorded in the general ledger. The accountant reviews the documents to ensure that they match and then signs the documentation.

b. **Completeness** – Pre-numbered purchase orders are used. Open purchase orders are investigated at the end of the month to determine if they were void or just failed to be recorded. Management reviews checks written toward the end of the period to ensure the underlying transactions were posted in the appropriate period. This review is documented in an excel checklist that is completed at the end of each month for these activities.

J. Peer review issue #5 – Auditors are not linking control risks to further substantive procedures

Peer review data indicates that some auditors are identifying control weaknesses but failing to link those risks to further substantive procedures. This may be because auditors often do not necessarily obtain their understanding of internal controls prior to completing the other risk assessment procedures and designing the appropriate level of substantive audit procedures. In addition, auditors do not always go back to the team discussion documentation and risk assessment summary to document that a risk has emerged during testing along with the further audit procedures to be performed to lower detection risk. Both steps are important as is the step to link the control deficiency identified with the necessary additional substantive audit or internal control procedures.

1. Exercise 2: Peer review issue identified – Ramifications of control weaknesses

An auditor was gaining an understanding of internal control over a significant accrual for an entity that raises livestock for milk production. In reviewing the process, she noticed that the CFO prepared the unborn livestock accrual (a significant asset) and gave the staff accountant an entry to post to the general ledger. In past years, the controller would prepare the estimate and journal entry with the CFO reviewing it. However, the entity went through a cost cutting initiative after losing a major contract during the year to improve its financial performance. The controller position was eliminated. When asked, the CFO indicated that there was no review of the journal entry. He did not feel it was necessary. The auditor concluded that this estimate had many sensitive and subjective components and therefore was subject to a high degree of estimation uncertainty. She believed that it was a significant deficiency because of the risk of management bias. Due to the loss of the contract the company had been close to violating two of its debt covenants in the second and third quarters. The auditor was aware that the CEO and the board reviewed the financial statements each month, but the auditor was concerned that they were not likely to question an estimate such as this.

In the prior year when controls were functioning, and the company was profitable, the auditor performed the following procedures.

a. Determine whether the assumptions used in forming the estimate are reasonable. This involves challenging management's assumptions and evaluating the quality of the data.
b. Evaluate the internal controls. This includes the review of estimates by management. Understand the data and reliability of the sources used to develop the estimate and recalculate.
c. **In light of the situation in the current year, how might the auditor link this control deficiency to further audit procedures?**

K. Peer review issue #6 – Auditors are not evaluating control weaknesses

Peer reviewers have noted that auditors are failing to identify weaknesses in internal controls and classify them as control deficiencies, significant deficiencies, or material weaknesses.

There are several ways that control deficiencies come to light.

a. The auditor is aware that segregation of duties is poor, the accounting function is either not adequately or appropriately staffed, the client has had significant turnover in the accounting function and processing is behind or other factors. If the auditor is aware of these or other similar conditions at the client's that could impact the quality of the accounting function, they should document these as overall risks in the audit and deficiencies in internal control.
b. The auditor may identify control weaknesses during their understanding of the design of controls and whether they have been implemented.
c. The auditor may identify a misstatement in the financial statements. They will want to identify the significance of the misstatement and its root cause when documenting the control deficiency.

Control deficiency – A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. For example, when a control that is necessary to meet the control objective is missing, or an existing control is not properly designed so that, even if the control operates as designed, the control objective would not be met. A deficiency in operation exists when a properly designed control does not operate as designed or when the person performing the control does not possess the necessary authority or competence to perform the control effectively.

The auditor accumulates instances of control deficiencies during the audit. A best practice would be to have one workpaper where members of the engagement team can list the deficiency, the workpaper reference and whether it is a deficiency in design or operation. At the end of the audit, the team can evaluate the deficiencies for the root cause. For example, if several individual deficiencies point toward a lack of training they would be combined as one deficiency. The auditor would then make an evaluation as to whether the deficiency (ies) noted represent a material weakness or significant deficiency.

Material weakness – A material weakness is a deficiency or deficiencies, where there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. This is a lower level of certainty than probable. **Probable** means that the future events are likely to occur. **Reasonably possible** means that the chance of the future event or events occurring is more than remote but less likely than probable. Of course, sometimes the event is not just reasonably possible, it is certain. For example, if the entity fails to record a material transaction, then this is a material misstatement because it occurred.

Significant deficiency – If the deficiency(ies) do not meet the criteria to be classified as a material weakness, then the auditor will determine if the control deficiency is a significant deficiency. A significant deficiency (ies) in internal control is one that is less severe than a material weakness yet important enough to merit attention by those charged with governance.

Once classified as a deficiency, material weakness or significant deficiency, the auditor should communicate them to management. The auditor has several choices for those deficiencies that are not classified as significant deficiencies or material weaknesses. The auditor can put them in the form of a management letter, communicate them in an agenda that will be discussed with those charged with governance or communicate them orally to management and document that the discussion took place,

with whom and management's comments if any. Significant deficiencies and material weaknesses are communicated in a written communication. The form and the content are prescribed by AU-C 265.

Peer reviewers have noted that auditors:

a. Sometimes fail to identify control deficiencies as such at the workpaper when identified;
b. Identify the control deficiency but do not aggregate it with others;
c. Fail to communicate the deficiencies to management that are not significant deficiencies or material weaknesses;
d. Do not document the evaluation of deficiencies as to type as discussed above; and
e. Do not consider circumstances identified in AU-C 265 that are present at the client as deficiencies.

AU-C 265 identifies the following as indicators of material weaknesses:

a. Identification of fraud, even if not material, on the part of senior management.
b. Restatement of previously issued financial statements to reflect the correction of a material misstatement due to fraud or error.
c. Identification by the auditor of a material misstatement of the financial statements under audit in circumstances that indicate that the misstatement would not have been detected and corrected by the entity's internal control.
d. Ineffective oversight of the entity's financial reporting and internal control by those charged with governance.

Appendix A to AU-C 265 identifies a list of indicators of problems with both the design and operation of internal controls. Auditors may want to consult this list.

Lack of segregation of duties is often an issue in small- to mid-size clients. Although auditors understand that adding additional personnel may not be practicable, this does not prevent the condition from being a control deficiency. The auditor should evaluate whether there are controls exercised by senior management or owner-manager. The auditor should also be aware that if senior management or an owner-manager exercises more oversight that this could increase the risk of management override of controls. The size of the entity or its economic constraints should not inhibit the auditor from reporting deficiencies in internal control. Additionally, if controls added do not adequately mitigate a significant deficiency or material weakness, the auditor should continue to report the deficiency.

Example: An audit firm was hired by a midsized not-for-profit entity to audit the financial statements. In the first meeting with the board of directors the board chair mentioned that she would like to see the material weakness in the AU-265 report be removed. She was concerned with the perception donors would have of the organization. The auditor agreed, subject to one of the board members also reviewing the checks and supporting documentation before they were released. The lack of segregation of duties was related to cash disbursements. There was one bookkeeper who initiated, authorized, processed, and recorded the transactions. She also prepared the bank reconciliation and the analytical comparisons that were reviewed monthly by the CFO and the board.

The material weakness was removed. Two years later it came to light that the bookkeeper was embezzling from the company. As is often the case with fraud, she authorized disbursements to a company she created. This was discovered by a regulator and it made headlines. The auditor's work and ethics were called into question. The firm's workpapers did not contain documentation of why the auditor believed that adding a board member's review of checks could mitigate a lack of segregation of duties as significant as this.

Following is a template that an auditor could use to help ensure complete documentation of deficiencies and their disposition.

Control Deficiency Evaluation Template

1. Consider whether these circumstances identified in AU-C 265 are present at the client.

Circumstance that could give rise to deficiencies, significant deficiencies, or material weaknesses	Control deficiency (Y/N)	Material weakness: Material/reasonably possible	Significant deficiency: Merits attention by those charged with governance	WP Ref.
Ineffective oversight by those charged with governance of the financial reporting and internal control or ineffective overall governance structure				
Restatement of previously issued financial statements to correct a material misstatement				
Identification of fraud of any magnitude on the part of senior management				
Ineffective control environment				

2. Consider whether these deficiencies were identified:
   a. Failure in the operation of effectively designed controls over a significant account or process.
   b. Failure of information and communication element of internal control to provide complete and accurate output because of deficiencies in timeliness, completeness, or accuracy.
   c. Failure of controls designed to safeguard assets from loss, damage, or misappropriation.
   d. Failure to perform reconciliations of significant accounts.
   e. Identification by the auditor of a material misstatement in the financial statements for the period under audit that was not initially identified by the entity's internal control (indicator of material weakness).
   f. Other deficiencies noted.

Significant account or process	Description of deficiency	Merits attention by those charged with governance?	Workpaper Reference	Communication method

3. Consider the interaction of deficiencies:

Does the interaction of deficiencies cause one or more to be aggregated and communicated as a significant deficiency or material weakness? Document the consideration.

L. Peer review issue #7 – Auditors are not evaluating the entity's ability to remain a going concern

Peer reviewers have noted that auditors are not always considering the entity's ability to remain a going concern. It is the auditor's responsibility to evaluate instances where an entity has, for example, experienced operating losses and liquidity issues and is reliant on funding that has not yet been secured or other situations that impact profitability, liquidity, and their ability to meet debt obligations.

Another issue arises when the auditor will consider the entity's ability to remain a going concern but fails to evaluate evidence to support management's assessment, obtaining only a representation from management.

Example: An entity is marginally profitable but is heavily leveraged. The balance on their line of credit, which they have been drawing on for liquidity for the past two years, is high. The variable interest rate was low for several years, so they were able to make the interest payments, but the rate has risen recently. Rates do not appear that they will decrease for the next 18 months at least. The entity has violated its debt covenants and has not been successful in obtaining waivers or refinancing the debt. The auditor should obtain management's assessment of whether the entity can remain a going concern and then test it.

The financial reporting framework may or may not require management to evaluate whether there is substantial doubt about the entity remaining a going concern. If the entity is not reporting under GAAP, that requirement may not be present. However, the auditor is still required to perform the procedures and evaluate disclosures.

The assessment of going concern should be performed during planning unless it is not evident at that time. When it is, if there are issues, the auditor may determine that there is a significant risk associated with management's (or the auditor's) assessment as well as with related disclosures in the entity's financial statements.

SAS 134 requires change to the emphasis paragraph to one that is titled, "Substantial Doubt About the Entity's Ability to Continue as a Going Concern."

1. Exercise 3: Internal control

1. Auditors should always gain an understanding of their client and its internal control.

   True or False

2. When testing operating effectiveness of controls, the auditor should focus solely on controls related to significant risks.

   True or False

3. If the auditor tests the control environment and the monitoring process, they can rely on internal controls at the transaction level.

   True or False

II. Exercise solutions

A. Exercise 1: Primarily indirect controls – Suggested solution

The auditor is not required to identify internal controls for every one of the principles identified in a control element. The auditor identifies the key controls that support the objectives set forth by the principles in the element category. Smaller, less complex organizations will probably have fewer controls. However, the auditor is not only responsible for identifying the controls but concluding they are appropriately designed and have been implemented which includes documentation of client personnel interviewed, the results of the interview, documents examined, and processes observed. The workpaper could be improved by expanding the documentation as follows.

Internal control	Discussions, observations, and review of documents
Management sets the appropriate tone from the top.	I discussed the tone from the top with the CEO, CFO, Operations Manager and key members of the staff. They discussed how decisions are made by management based on compliance with laws, regulations and the entity's policies and procedures without regard to whether there would be an adverse effect on the financial statements. Conference calls and meetings begin with the statement that it is important to put all the facts on the table so they can be analyzed against laws, regulations and internal policies.
Those charged with governance meet regularly. They review the internal financial statements at each meeting and ask questions about significant fluctuations.	The partner on the engagement meets twice a year with the audit committee. The members discuss the financial statements and ask questions about them in areas where they expected a different result. I also noted that in my reading of the minutes that the board package contains a financial statement analysis. The minutes further note the answers to any questions from the previous month that members asked.
The entity has a code of conduct and all employees are required to acknowledge that they have read it.	I looked at the code of conduct on the client's intranet site, noting that it appeared complete and tailored to their company. I asked to see the personnel files of two of the newest hires in order to see the acknowledgment of its receipt. I also discussed the code with the CFO, controller and AP clerk. Based on our discussions I believe that they read and understood the provisions.
Management conducts performance evaluations of staff members.	I noted that the CFO had a performance review schedule that they were finalizing for the year. I asked questions about the performance review frequency and how she determined that each review had been given on a timely basis. I noted performance reviews in the personnel files of two employees.

B. Exercise 2: Ramifications of control weaknesses – Suggested solution

The auditor identified the threat of management bias and a significant deficiency in internal controls over a significant estimate due to lack of controls over its preparation. This means that they will need to consider how this deficiency changes the level of substantive procedures that would have been performed had controls been working. There are several procedures auditors could use to audit an estimate and they may use more than one approach.

In the prior year when controls were functioning, and the company was profitable, the auditor performed the following procedures.

a. Determine whether the assumptions used in forming the estimate are reasonable. This involves challenging management's assumptions and evaluating the quality of the data.
b. Evaluate the internal controls. This includes the review of estimates by management. Understand the data and reliability of the sources used to develop the estimate and recalculate.

The auditor added one further procedure. She performed a hindsight review of the unborn livestock accrual using subsequent birth rates, mortality rates and other inputs updated by operations personnel to form her own estimate. She then compared it to the CFO's estimate.

C. Exercise 3: Internal control – Suggested solutions

1. Auditors should always gain an understanding of their client and its internal control.

   True. The auditor should gain an understanding of internal control in order to assess the risk of material misstatement. Control risk is an important part of RMM.

2. When testing operating effectiveness of controls, the auditor should focus solely on controls related to significant risks.

   False. The auditor should test the operating effectiveness of internal control when they want to reduce control risk below high. The auditor should also test internal control when they believe that substantive testing alone will not reduce audit risk to a low level. Generally, this happens when information is only in electronic form or is very complex.

3. If the auditor tests the control environment and the monitoring process, they can rely on internal controls at the transaction level.

   False. In order to obtain control reliance, control activities over the relevant assertions should be tested. Entity level controls are important, but the auditor cannot use this test alone to reduce substantive testing.