Why do auditors ask so many questions about their clients’ internal controls? Assessing internal controls is part of today’s auditing requirements. It helps identify risk factors — but the requirements can sometimes be unclear.

The American Institute of Certified Public Accountants (AICPA) uses Technical Questions and Answers (Q&A) to address inquiries from members seeking guidance on certain technical issues. Here’s a set of five common questions, along with answers that the AICPA issued on April 27 to help clarify an auditor’s responsibility for assessing a client’s internal controls.

Are auditors required to obtain an understanding of business processes relevant to financial reporting in every audit engagement?

Yes, the auditing standards require an auditor to understand a client’s information system, including the related business processes and communication relevant to financial reporting.

The AICPA reminds auditors that it’s important to distinguish between business processes and control activities. Business processes are the activities designed to:

- Develop, purchase, produce, sell and distribute an entity’s products and services,
- Ensure compliance with laws and regulations, and
- Record information, including accounting and financial reporting information.

The AICPA defines control activities as “steps put in place by the entity to ensure that the financial transactions are correctly recorded and reported.” Auditors are expected to obtain an understanding of only those control activities that are considered relevant to the audit. There are no “cookie cutter” approaches when it comes to understanding business processes and control activities; rather, the
requirements differ from audit to audit.

**Does an auditor’s understanding of internal controls encompass more than control activities?**

Yes, an auditor must understand each component of the client’s financial reporting controls. This includes the control environment, risk assessment process, information system, control activities that relate to the audit, and the client’s monitoring of the controls. (See “Close-Up on Internal Controls.”)

**Should the auditor evaluate the design of controls and determine whether they’ve been implemented every year?**

Yes, each year auditors must evaluate the design of the financial reporting controls that are related to the audit and determine if they’ve been properly implemented. This requires more than just inquiring with company personnel. Auditors must use additional procedures — such as observations, inspection or tracing transactions through the information system — to obtain an understanding of controls relevant to the audit. The appropriate procedures are a matter of the auditor’s professional judgment.

For existing clients, an auditor may leverage information obtained from his or her previous experience with the entity and the results from audit procedures performed in previous reporting periods. In doing so, the auditor should determine whether changes affecting the control environment have occurred since the previous audit that may affect that information’s relevance to the current audit.

**Which control activities are considered relevant in every audit?**

Auditors are specifically expected to understand controls that address “significant” risks. These are identified and assessed for risks of material misstatement that, in the auditor’s professional judgment, require special audit consideration. Examples include control activities 1) relevant to the risk of fraud or 2) over journal entries (such as nonrecurring, unusual transactions or adjustments).

**Which relevant control activities may vary from audit to audit?**

Control activities that are relevant to a given audit may vary, depending on the client’s size, complexity and nature of operations. The AICPA advises auditors to consider such issues as materiality, risk, other components of the internal controls, and legal and regulatory requirements. Again, what’s relevant is a matter of the auditor’s professional judgment.

**Close-Up on Internal Controls**

In the 21st century, business and operating environments are rapidly changing. To reflect these changes, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) updated its *Internal Control* —

The updated COSO framework outlines five components of internal controls that are required under the Sarbanes-Oxley Act’s Section 404 provisions:

1. **Control environment.** A set of standards, processes and structures is needed to provide the basis for carrying out internal controls across the organization.

2. **Risk assessment.** This dynamic, iterative process identifies stumbling blocks to the achievement of the company's strategic objectives and forms the basis for determining how risks will be managed.

3. **Control activities.** Policies and procedures are necessary to help ensure that management’s directives to mitigate risks to the achievement of objectives are carried out.

4. **Information and communication.** Relevant and quality information supports the internal control process. Management needs to continually obtain and share this information with people inside and outside of the company.

5. **Monitoring.** Management should routinely evaluate whether each of the five components of internal controls is present and functioning.

The updated COSO framework isn’t just for public companies that must comply with the Sarbanes-Oxley Act. The framework applies to all entities that follow U.S. Generally Accepted Accounting Principles (GAAP): large, midsize and small, whether for-profit, not-for-profit or government body.

If you have questions regarding your internal control audit, please contact Dan Ward, Principal, Audit Services, at 314.983.1237 or dward@bswllc.com.