

# Auditing:

## Independence, Risk and Documentation Standards

### Course Description

---

The level of public confidence in the auditor's work is related to the credibility of the auditor. This course focuses on the principles of independence, audit risk, and audit documentation that establish a foundation for the credibility of an auditor's work. It emphasizes the importance of the audit independence, values of auditor's assessment and response to risk, and the significance of sufficient audit documentation. Competence also significantly influences on audit credibility. One way to maintain competence is through understanding the auditing standards, especially the latest developments. To inform auditors of significant changes affecting audit engagements, this course reviews:

- Rule 3210 and 3211 that improve transparency of audits by requiring disclosure of certain audit participants
- PCAOB's new organizational structure that improves the usability of the auditing standards
- SAS 130, part of the Attestation Clarity Project, providing guidance for integrated audits
- SAS 131, addressing the reporting requirements of GAAS and PCAOB
- Highlights of AICPA's Cybersecurity Risk Management Reporting Framework
- Highlights the Yellow Book such as overall 2011 revision, applicability, and relationship with other standards

**Completion Deadline & Exam:** This course, including the examination, must be completed within one year of the date of purchase. In addition, unless otherwise indicated, no correct or incorrect feedback for any exam question will be provided.

**Course Level:** Overview. This program is appropriate for professionals at all organizational levels.

**CPE Credits:** 8 (CPA)

**Field of Study:** Auditing

**Prerequisite:** None

**Advanced Preparation:** None

### Course Learning Objectives

---

#### Chapter 1: Recognizing the Latest Developments

After studying this chapter you will be able to:

1. Identify disclosure requirements of engagement partners and audit participants on Form AP
2. Recognize the amendments to PCAOB's rules after the reorganization of its auditing standards

3. Identify SAS 130 requirements for an integrated audit
4. Recognize SAS 131 amendments to auditors' reporting responsibilities
5. Identify the key components of the cybersecurity risk management examination report
6. Assess whether an engagement requires the use of the Yellow Book
7. Identify ways that auditors can use the Green Book in their work.

## **Chapter 2: Maintaining Independence**

After studying this chapter you will be able to:

1. Recognize the application of the conceptual framework for independence
2. Identify the different types of threats
3. Recognize auditors' responsibilities when threats to independence are at unacceptable level
4. Identify independence standards set forth by the PCAOB, AICPA, and GAO

## **Chapter 3: Assessing and Responding to Audit Risk**

After Upon completion of this chapter, you will be able to:

1. Identify ways to reduce audit risk to an acceptably low level
2. Identify the components of risk of material misstatement
3. Recognize auditors' responsibilities for assessing and responding to risk of material misstatement
4. Identify assertions used by the auditor to consider the different types of potential misstatements
5. Recognize the inherent limitations of an audit
6. Identify the role of auditors in deterring fraud

## **Chapter 4: Meeting Audit Documentation Requirements**

After studying this chapter you will be able to:

1. Recognize the importance of maintaining sufficient audit documentation
2. Identify the PCAOB, AICPA, and GAO requirements to avoid audit documentation deficiencies
3. Recognize the quality control requirements of the Yellow Book.