

Fraud and Cybersecurity: Top Issues for the CPA

Course Description

Cybercrime continues to escalate, ranking as the one of the most reported economic crimes. The interconnectivity of people, devices and organizations in today's digital world, opens up a whole new playing field of vulnerabilities and access points where cybercriminals can enter. Cyberattacks are becoming more destructive globally. In today's cybercrime environment, the issue is not whether a business will be compromised, but rather how successful an attack will be.

This course covers digital technology as it continues to transform and disrupt the business world, exposing organizations to both opportunities and threats. Key elements of an effective cybersecurity risk management, including a threats and vulnerabilities awareness, understanding of cyber risks, implementation of an effective framework, and detection of and response to cyberattacks. The challenges, such as the leadership engagement and the approach to managing cyber risks, are discussed, along with government's efforts to address cybersecurity vulnerabilities of the nation, businesses, and individuals.

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: 5 (CPA)

Field of Study: Auditing - Fraud

Prerequisite: None

Advanced Preparation: None

Course Learning Objectives

After completing this course, you should be able to:

1. Recognize concepts used in the cybersecurity world
2. Identify trends such as cyber and the evolution of threats
3. Identify cyber challenges, including issues facing management
4. Recognize government acts to address cybersecurity risks exposed to the nation, businesses, and individuals
5. Recognize cybersecurity standards, including ISO/IEC 27001 and other standards

6. Identify SEC regulatory cybersecurity expectations, including as public companies' disclosure obligations
7. Recognize elements of an effective cybersecurity risk management, such as threats and vulnerabilities awareness, and the understanding of cyber risks
8. Identify the leading practices in the fight against cyber threats
9. Recognize the evolution of the internal audit function.