Examining Cybersecurity Concepts

About This Course

Course Description
A data breach can be disastrous, precipitating complex legal obligations, costly remediation, and long-lasting reputational damage. Cyberattacks are a top concern among boards, executive management, and other organizational stakeholders, and internal auditors are expected to assess an organization’s defenses and its ability to recover should an event occur.

Are you up to the challenge?
This course examines cybersecurity concepts that can be used to facilitate integrated auditing efforts within an organization. It examines the connection between cybersecurity and network security, provides greater insight into the pros and cons of technology insurance, and explores how to apply the audit process to social media, mobile, and cloud environments. Finally, the course explores common cyber-related frameworks, standards, and guidelines, and explains how to audit common cybersecurity solutions.

Who will benefit from this course?
This course is designed for internal auditors with a basic understanding of cybersecurity concepts and have been involved in integrated audits, or for those internal auditors who have been involved in internal audit activities that require an understanding of how to manage the impact of cybersecurity events on organizational risks.

Course Objectives
- Define cybersecurity from an internal audit perspective.
- Explore the business process-cybersecurity connection and the importance of classifying and assessing controls.
- Explain cyber liability insurance and its impact on cybersecurity.
- Describe cyber standards, state notification laws, and how they affect an organization.
- Express how to assess an organization’s cyber capabilities from an attacker perspective, using threat modeling.
- Explore how to assess cybersecurity risks and controls related to mobile computing and connected devices.
- Explore how to assess cybersecurity risks and controls related to social media and an organization’s digital presence.
- Explore how to assess cybersecurity risks and controls related to utilizing cloud providers or third-party vendors.
Course Topics

Cybersecurity Connections
- Cybersecurity connection to network security.
- Cybersecurity triad.
- Connection to the OSI Model.
- Defense in depth and layered security.
- Boundary controls.

Risks, Insurance, and State Notification Laws
- Tasks to mitigating costs and risks.
- Scenario-based risk management and its relationship to incident response.
- Common characteristics of cyber liability insurance and why it is important.
- Current U.S. and international notification laws affecting security incident management.

Assessing Cybersecurity Risk in the Cloud Environment
- Cloud definitions.
- Cloud models.
- Cloud deployments.
- Cloud assessment tools.
- Risks related to cloud providers.
- Security analysis of clouds.
- Overview of security threats with the cloud.
- Service organization control (SOC) reports.

Mobile Computing and Connected Devices
- Mobile computing risks, control activities, and incident management.
- Personally owned device risks, control activities, and incident management.
- Corporate owned device risks, control activities, and incident management.

Social Media and Digital Presence
- Social media concepts and types of social networks.
- Social media risks and controls.
- Digital presence assessments.

Understanding the Breach
- Assessing a breach.
  - Network Infiltration Process.
  - Detection Process.
  - Correction Process.
Course Information

Course Duration: 1 day

CPE Hours Available: 8

Knowledge Level: Intermediate

Field of Study: Auditing

Prerequisites: Fundamentals of IT Auditing; Fundamentals of Cybersecurity Auditing, or equivalent information technology experience.

Advance Preparation: None

Delivery Format: eLearning (Group-Internet-Based); Seminar (Group-Live); On-site Training (Group-Live)