Auditing the Cloud

About This Course

Course Description
Cloud computing provides organizations with access to human and technical resources that might otherwise be cost prohibited. Each organization should establish a business case, articulating both the benefits and inherent risks of moving a portion of its operations to the cloud.

Globally, there has been a significant increase in the activity of hackers who breach managed service providers (MSPs) in order to execute ransomware attacks, point-of-sale intrusions, and business email compromise (BEC) scams. The alert explained how the attackers use MSP solutions to gain access into the internal networks of customers.

This Auditing the Cloud course provides participants with a deeper understanding of cloud-related designs, risks, and controls while examining the connection between cybersecurity and cloud environments. Further, this course provides additional insight into cloud-related standards and guidelines, and explains how to audit cloud environments.

Who will benefit from this course?
This four-hour course is designed for internal auditors with a basic understanding of information technology and cybersecurity concepts and for those who have been involved in internal audit engagements that require an understanding of how to manage the impact of cloud computing on organizational risks.

Course Objectives
• Define cloud computing from an internal audit perspective.
• Explore the cloud-cybersecurity connection and the importance of classifying and assessing the cloud environment.
• Examine internal audit considerations regarding contract provisions and first- and third-party insurance.
• Describe cloud standards and guidelines, and how they affect an organization.
• Explain how to assess an organization’s liabilities when utilizing cloud solutions.
Course Topics

Understanding the Cloud Environment
- The cloud, and how it works.
- Common cloud standards and guidelines.
- Cloud models and deployments.
- Cloud provider selection criteria.
- Connectivity between the cloud provider and the client site.

Examining Cloud-based Risks and Controls
- Cloud governance and strategy.
- Cloud-based asset and configuration management.
- Conducting cloud-based risk assessments.
- Risks related to cloud providers.
- Cybersecurity threats.
- Resiliency considerations.
- Key cloud contract considerations (contracts, reciprocal agreements, service level agreements [SLAs]).
- First- and third-party insurance.
- Annual assessment/service organization control (SOC) reports.

Assessing the Cloud Environment
- Assessing cloud tools.
- Assessing the contract.
- Assessing cloud controls at the cloud vendor and client sites.
Course Information

Course Duration: .5 days

CPE Hours Available: 4

Knowledge Level: Intermediate

Field of Study: Auditing

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

Advance Preparation: None

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