Fundamentals of Cybersecurity Auditing

About This Course

Course Description
According to The IIA’s OnRisk 2020 Report, cybersecurity is the top risk faced by organizations. This report states, “The growing sophistication and variety of cyberattacks continue to wreak havoc on organizations’ brands and reputations, often resulting in disastrous financial impacts.” Internal auditors are expected to be cyber savvy and able to assess whether organizations are sufficiently prepared to manage cyber threats that could cause disruption and reputational harm.

Are you up to the challenge?

This course provides a comprehensive overview of key cybersecurity concepts that can be used to facilitate audit efforts within your organization. It examines directive, preventive, detective, corrective, and mitigating controls, and how to apply each within the audit process. Finally, commonly accepted frameworks, standards, and guidelines are presented to prepare you to assess cybersecurity during operational audits.

Who will benefit from this course?
This course is designed for internal auditors who are looking for a fundamental understanding of cybersecurity and common exploits. It is recommended for internal auditors that are involved in audit activities that require a basic understanding of how to manage the impact of cybersecurity events on organizational risks.

Course Objectives
- Define cybersecurity from an internal audit perspective.
- Describe the scope and limitations of cybersecurity.
- Recognize how to measure effectiveness within the cybersecurity program.
- Express the importance of information security governance.
- Examine the importance of cybersecurity and vendor risk assessments.
- Explore basic auditing considerations for cybersecurity-related compliance.
- Recognize typical cybersecurity-related directive, preventive, detective, corrective, mitigating redundant, compensating, and corrective controls.
- Identify simple audit techniques to assess cyber resiliency within existing operational audit programs with a focus on payroll systems.
Course Topics

**Overview of Cybersecurity**
- What cybersecurity means.
- Common risks (outcomes) from cyber exploit.
- Purpose of each control type and how it affects the organization's cyber resiliency.
- Introduction to the ISO Model.
- Explaining defense in depth and layered security.

**Information Security Governance, Risk, and Compliance**
- Security governance.
- Security risk assessments and maturity assessments.
- Cybersecurity-related compliance.
- Auditing cybersecurity governance.
- GRC's role with assurance.

**Control Primer**
- Internal control.
- Control design and maintenance.
- Types of controls.
- Control levels.
- Control classifications.
- Functions by control.
- Asset and control inventory.
- Auditing controls.

**Directive Controls**
- Directive controls.
- Threats.
- Cybersecurity frameworks, standards, and guidelines.
- Cybersecurity training.
- Incentive programs.

**Preventive Controls**
- Preventive controls.
- The anatomy of a breach.
- Monitoring and reporting.
**Detective Controls**
- Purpose of detective controls.
- The cybersecurity triad.
- Detecting cyber incidents.
- Audit logging.
- Security information and event management (SIEM).
- Continuous monitoring.
- The value of the Security Operations Center (SOC).
- Detective control auditing concepts.

**Corrective Controls**
- Purpose of corrective controls.
- Backup and restore threats and controls.
- Business continuity threats and controls.
- Disaster recovery threats and controls.
- Incident response threats and controls.
- Auditing corrective control threats and controls.

**Mitigating Controls**
- Purpose of compensating and redundant controls.
- Common mitigating controls.
- Ways to assess mitigating controls.

**Compensating and Redundant Controls**
- Purpose of compensating and redundant controls.
- Common threats.
- Common controls.
- Example audit approaches.

**Assessing Cybersecurity in Operational Audit Programs**
- IIA Standards and implementation guidance.
- IIA supplemental guidance.
- Industry-recognized cybersecurity and cloud control frameworks.
- Enhancing existing operational audit programs with cyber-related audit activities.
Course Information

Course Duration: 2 day(s)

CPE Hours Available: 16

Knowledge Level: Basic

Field of Study: Information Technology

Prerequisites: Fundamentals of IT Auditing or equivalent experience with auditing IT general controls.

Advance Preparation: None

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