

Cyber Security Audit

Course Duration: 2 Days

Course Overview

With the increasing number of cyberthreats, it is becoming critical for audit plans to include cybersecurity. ISACA's Cybersecurity Audit Certificate Program provides audit/assurance professionals with the knowledge needed to excel in cybersecurity audits, and IT risk professionals with an understanding of cyber-related risk and mitigating controls

What you'll learn

- Understand Security Frameworks to Identify Best Practices
- Define threat and vulnerability management
- Assess threats with the help of vulnerability management tools
- Build and deploy secure authorization processes
- Explain all aspects of cybersecurity governance
- Distinguish between firewall and network security technologies
- Enhance asset, configuration, change and patch management practices
- Manage enterprise identity and information access
- Identify application security control
- Identify cyber and legal regulatory requirements to aid in compliance assessments
- Identify weaknesses in cloud strategies and controls
- Perform cybersecurity and third-party risk assessments
- Identify the benefits and risks of containerization
- And much more!

Course Outline

Section 1—Introduction

- Digital Asset Protection
- Lines of Defense
- Role of Audit
- Audit Objectives

- Audit Scope

Section 2—Cybersecurity Governance

- Cybersecurity Roles and Responsibilities
- Security Frameworks
- Security Organization Goals & Objectives
- Cybersecurity Policy and Standards
- Cyber and Legal/ Regulatory Requirements
- Information Asset Classification
- Cybersecurity Insurance
- Cybersecurity Risk Assessment
- Cybersecurity Awareness Training & Education
- Social Media – Risk and Control
- Third-Party Assessment
- Service Providers
- Supply Chain Risk Management
- Performance Measurement

Section 3—Cybersecurity Operations

- Concepts and Definitions
- Threat and Vulnerability Management
- Enterprise Identity and Access Management
- Configuration Management / Asset management
- Change Management
- Patch Management
- Network Security
- Build and Deploy/Secure Authorization Process for Information Technology
- Incident Management
- Client Endpoint Protection
- Application Security
- Data Backup and Recovery
- Security Compliance
- Cryptography

Section 4—Cybersecurity Technology Topics

- Firewall and Network Security technologies
- Security Incident & Event Management (SIEM)
- Wireless Technology
- Cloud Computing
- Mobile Security
- Internet of Things (IoT)
- Virtualization Security
- Industrial Control Systems (ICS)

