Formatech
INTEGRATED LEARNING CENTERS
Learn from the Experts

Course Outline

CISM-Certified Information Security Manager

Duration

35 hours

Learning Objectives:

- Information Security Governance
- Information Risk Management
- Information Security Program Development
- Information Security Program Management
- Incident Management and Response

Prerequisites

Five years of experience with audit, IT systems, and security of information systems; systems administration experience; familiarity with TCP/IP; and an understanding of UNIX, Linux, and Windows. This advanced course also requires intermediate-level knowledge of the security concepts covered in our Security+ Prep Course course.

Target Audience:

Experienced information security managers and those who have information security management responsibilities, including IT consultants, auditors, managers, security policy writers, privacy officers, information security officers, network administrators, security device administrators, and security engineers.

Topics Covered:

- Information Security Governance

  - Develop an Information Security Strategy
  - Align Information Security Strategy with Corporate Governance
  - Identify Legal and Regulatory Requirements
  - Justify Investment in Information Security
  - Identify Drivers Affecting the Organization
  - Obtain Senior Management Commitment to Information Security
  - Define Roles and Responsibilities for Information Security
  - Establish Reporting and Communication Channels

- Information Risk Management

  - Implement an Information Risk Assessment Process
  - Determine Information Asset Classification and Ownership
  - Conduct Ongoing Threat and Vulnerability Evaluations
  - Conduct Periodic BIAs
  - Identify and Evaluate Risk Mitigation Strategies
  - Integrate Risk Management into Business Life Cycle Processes

- Report Changes in Information Risk

- Information Security Program Development

  - Develop Plans to Implement an Information Security Strategy
  - Security Technologies and Controls
  - Specify Information Security Program Activities
  - Coordinate Information Security Programs with Business Assurance Functions
  - Identify Resources Needed for Information Security Program Implementation
  - Develop Information Security Architectures
  - Develop Information Security Policies
  - Develop Information Security Awareness, Training, and Education Programs
  - Develop Supporting Documentation for Information Security Policies

- Information Security Program Implementation

  - Integrate Information Security Requirements into Organizational Processes
  - Integrate Information Security Controls into Contracts
  - Create Information Security Program Evaluation Metrics

- Information Security Program Management

  - Manage Information Security Program Resources
  - Enforce Policy and Standards Compliance
  - Enforce Contractual Information Security Controls
  - Enforce Information Security During Systems Development
  - Maintain Information Security Within an Organization
  - Provide Information Security Advice and Guidance
  - Provide Information Security Awareness and Training
  - Analyze the Effectiveness of Information Security Controls
  - Resolve Noncompliance Issues

- Incident Management and Response

  - Develop an Information Security Incident Response Plan
  - Establish an Escalation Process
  - Develop a Communication Process
  - Integrate an IRP
  - Develop IRTs
  - Test an IRP
  - Manage Responses to Information Security Incidents
  - Perform an Information Security Incident Investigation
  - Conduct Post-Incident Reviews

- Appendix A: ISACA CISM Certification Process