Certified Information Security Manager (CISM)

Course Overview

In this course, students will establish processes to ensure that information security measures align with established business needs.

Who Should Attend

The intended audience for this course is information security and IT professionals, such as network administrators and engineers, IT managers, and IT auditors, and other individuals who information about information security management, who are looking for career advancement in IT security, or who are interested in earning the CISM certification.

Course Objectives

Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations. Identify and manage information security risks to achieve business objectives. Create a program to implement the information security strategy. Implement an information security program. Oversee and direct information security activities to execute the information security program. Plan, develop, and manage capabilities to detect, respond to, and recover from information security incidents.

Course Outline

1 - 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

2 - 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

3 - 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

4 - Information Security Program Implementation

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

5 - 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

6 - 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