Certified Information Security Manager Preparation

Course Content

This course is ideal for management-focused professionals who design, build and manage enterprise information security programs.

In the event of digitalization, enterprise executives are required to ensure that their information security managements have the expertise needed to reduce risk and protect the enterprise.

The course will cover all CISM domains of job practice area which will help assure that you will be able to lead the information security program beyond the scope of just information security methodology or framework but through its lifecycle and related standard and best practices

Course Objectives

Upon completion of this course, you will be able to understand all concept of information security program including information security governance, risk management and compliance, information security program development and management and information security incident management.

The course will help embed you with appropriate skill and knowledge to:

- Establish and lead the enterprise information security program
- Manage enterprise information security risks
- Initiate, develop and manage information security plan
- Develop and manage information security incident management to response to and recover from the disruptive and destructive information security events

Course Outline

Day 1: Information Security Management Basics and Information Security Governance

- Information Security Concepts
- Related standards, frameworks, practices and body of knowledges
- Governance, Goals, Strategies, Policies, Standards, and Procedures
- Risk Appetite, Tolerance, and Capacity
- Business Continuity and Disaster Recovery
- Incident Response
- Information Security Metric
- Information Security Governance Overview
- Effective Information Security Governance
- Roles and Responsibilities
- Risk Management

- Governance of Third-Party Relationships
- Information Security Governance and its Metrics
- Information Security Strategy Overview and Objectives
- Determining the Current State of Security, Target State and the GAP between
- Information Security Strategy Development
- Action Plan to Implement Strategy
- Information Security Program Objectives

Day 2: Information Risk Management and Compliance

- Risk Management Overview
- Risk Management Strategy
- Effective Information Risk Management
- Information Risk Management Concepts
- Implementing Risk Management
- Risk Assessment and Analysis Methodologies
- Risk Assessment
- Information Asset Classification
- Operational Risk Management
- Third-Party Providers
- Risk Management Integration with Life Cycle Process
- Security Control Baselines
- Risk Monitoring and Communication
- Training and Awareness
- Documentation

Day 3: Information Security Program Development and Management

- Information Security Program Management Overview
- Information Security Program Objectives
- Information Security Program Concepts
- Scope and Charter of an Information Security Program
- The Information Security Management Framework
- Information Security Framework Components
- Defining and Information Security Program Road Map
- Information Security Infrastructure and Architecture
- Architecture Implementation
- Security Program Management and Administrative Activities
- Security Program Services and Operational Activities
- Controls and Countermeasures
- Security Program Metrics and Monitoring
- Common Information Security Program Challenges

Day 4: Information Security Incident Management

- Incident Management Overview
- Incident Response Procedures
- Incident Management Organization
- Incident Management Resources
- Incident Management Objectives

- Incident Management Metrics and Indicators
- Defining Incident Management Procedures
- Current State of Incident Response Capability
- Developing an Incident Response Plan
- Business Continuity and Disaster Recovery Procedures
- Testing Incident Response and Business Continuity/ Disaster Recovery Plans
- Executing Response and Recovery Plans
- Post Incident Activities and Investigation

Target Student

The primary audience for this course are as follow:

- Experienced practitioners, managers, and executives those required the skillset of information security management from a governance perspective.
- Security Engineer, Professional in IS/IT and related field.
- Individual who interested in advanced certification in information security management as an opportunity for career enhancement and development.

Course Duration

4 days