Certified Information Security Manager (CISM)

Duration: 5 Days Course Code: CISM

Overview:

The CISM Exam Preparation course is an intensive, four-day review program to prepare individuals who are planning to sit for the Certified Information Security Manager (CISM) exam. The course focuses on the key points covered in the CISM Review Manual 15th Edition and includes class lectures, group discussions/activities, exam practice and answer debriefs. The course is intended for individuals with familiarity with and experience in information security management.

Target Audience:

Individuals who manage, design, oversee and assess an enterprises' information security.

Objectives:

- **After completing this course you should be able to:**
- Establish and/or maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives.
- Manage information risk to an acceptable level based on risk appetite to meet organizational goals and objectives.
- Develop and maintain an information security program that identifies, manages and protects the organization's assets while aligning to information security strategy and business goals, thereby supporting an effective security posture.
- Plan, establish and manage the capability to detect, investigate, respond to and recover from information security incidents to minimize business impact.

Prerequisites:

- There is no set pre requisite for this course. ISACA do require a minimum of five years' professional information security work experience to qualify for full certification. You can take the for CISM exam prior to meeting ISACA's experience requirements, but the CISM qualification is awarded after you meet the experience requirements. However, there is no restriction in getting yourself certified in early stages of your career and start practicing globally accepted Information Security Management practices.

Content:

General Exam Information

Domain 1 - Information Security Governance (24%)

- Information Security Governance Overview
- Effective Information Security Governance
- Roles and Responsibilities
- Risk Management Roles and Responsibilities
- Governance of Third-Party Relationships
- Information Security Governance Metrics
- Information Security Strategy Overview
- Information Security Strategy Objectives
- Determining the current state of Security
- Information Security Strategy Development
- Strategy Resources
- Strategy Constraints
- Action Plan to Implement Strategy
- Information Security Program Objectives
- Case Study

Domain 2 - Information Risk Management (30%)

- 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 Service Providers
- Risk Management Integration with Life Cycle Processes
- Security Control Baselines
- Risk Monitoring and Communication
- Training and Awareness
- Documentation
- Case Study

Domain 3 - Information Security Program Development and Management (27%)

- 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 an 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
- Case Study

Domain 4 - Information Security Incident Management (19%)

- Incident Management Overview
- Incident Response Procedures
- Imcident Management Organisation
- Incident Management Resources
- Incident Management Objectives
- Incident Management Metrics and Indicators
- Defining Incident Management Procedures
- Current State of Incident response Capability
- Developing ad 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
- Case Studies

Exam practice/sample exam

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK