CISM - Certified Information Security Manager (CISM)

Overview

Course Code	CISM	Duration	4.0 days

The CISM certification is the primary certification for information security professionals who manage, design, oversee and/or assess an enterprise's information security.

In comparison to other certifications, CISM covers a wide body of knowledge. It is therefore recommended by the sponsoring organization, ISACA, that those sitting for the CISM certification attend a training session.

We offers a most comprehensive CISM review course in 4 day boot camp format for those wishing to thoroughly prepare for the CISM exam. Every student attending the CISM Boot Camp progresses through a number of skill checks to ensure knowledge is retained. The instructors for the CISM Boot Camp are certified with the CISM designation. Our Exam Preparation workshops are specifically designed to cover the new material that will be on the 2012 exams

Audience

Experienced information security managers and those who have information security management responsibilities, including:

- IT consultants
- Auditors
- Security policy writers
- Privacy officers
- Information security officers
- Network administrators
- Security device administrators
- Security engineers

Pre-Requisites

- Five years of experience with audit, IT systems, and security of information systems

- Systems administration experience

- Familiarity with TCP/IP

- 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

Key Topics

Module 1: Information Security Governance

Module 2: Information Risk Management and Compliance

Module 3: Information Security Programme Development and Management

Module 4: Information Security Incident Management

Objectives

Upon the completion of our CISM Exam Prep, students will be familiar with the following concepts:

- Information Security Governance
- An information security steering group function
- Legal and regulatory issues associated with Internet businesses, global transmissions and transborder data flows
- Common insurance policies and imposed conditions
- Information security process improvement
- Recovery time objectives (RTO) for information resources
- Cost benefit analysis techniques in assessing options for mitigating risks threats and exposures to acceptable levels.
- Security metrics design, development and implementation.
- Information security management due diligence activities and reviews of the infrastructure.
- Events affecting security baselines that may require risk reassessments
- Changes to information security requirements in security plans, test plans and reperformance
- Disaster recovery testing for infrastructure and critical business applications.
- The requirements for collecting and presenting evidence; rules for evidence, admissibility of evidence, quality and completeness of evidence.
- External vulnerability reporting sources
- The key components of cost benefit analysis and enterprise migration plans
- Privacy and tax laws and tariffs, data import/export restrictions, restrictions on cryptography, warranties, patents, copyrights, trade secrets, national security
- CISM information classification methods
- Life-cycle-based risk management principles and practices.
- Cost benefit analysis techniques in assessing options for mitigating risks threats and exposures to acceptable levels.

- Security baselines and configuration management in the design and management of business applications and the infrastructure.
- Acquisition management methods and techniques
- Evaluation of vendor service level agreements, preparation of contracts)
- CISM question and answer review