CISM®

Certified Information Security Manager

Acquire the skills and knowledge expected of a world-class information security manager

Duration: 4 days

The ISACA Certified Information Security Manager® (CISM) is one of the most important and prestigious InfoSec qualifications in the world today. CISM defines the core competencies and international standards of performance that information security managers are expected to master. It provides executive management with the assurance that those who have earned their CISM have the experience and knowledge to offer effective security management and advice.

This 4-day course provides an intense environment in which participants can acquire, thoroughly and properly, the skills and knowledge expected of a world-class information security manager. In the process the course provides outstanding preparation for the CISM exam.

Learning Outcomes

This course has been independently commissioned with two objectives:

- To provide an environment in which security professionals can acquire, thoroughly and properly, the skills and knowledge expected of a world class information security manager. Whether or not you intend to sit for the CISM exam, this course is a powerful way to equip yourself with the knowledge of the five core competencies that define the successful information security manager.
- To maximise your prospects at the CISM exam if you choose to sit it.

Who Should Attend

The CISM designation is for Information Security professionals who have 3-5 years of front-line experience with the security of information. This credential is geared towards Information Security managers and those who have information security management responsibilities.

Examination Procedure

Please note that the CISM exam is not included in this training course. The CISM exam is set, conducted and marked by ISACA.

All exams will be conducted online via computer-based testing centres around the world. You can book your CISM exam direct with ISACA or else you can purchase an exam voucher via ALC (we are an ISACA Accredited Channel Partner) and have both course and exam on the one invoice. For more exam information or to register, click here: http://www.isaca.org/Certification/Pages/Exam-Registration.aspx

Prerequisites

Qualifying for CISM requires a combination of four “e’s”: experience, ethics, education and examination. Specifically, the requirements are:

- Successful completion of
- the CISM exam
- Adherence to a code of professional conduct
- Commitment to continuing professional education
- Submission of verified evidence of a minimum of five years of information security work experience, with a minimum of three years of information security management work experience in three or more of the job practice areas.

Course Contents

1. Information Security Governance and Strategy

- Effective Information Security Governance
- Key Information Security Concepts and Issues
- The IS Manager
- Scope and Charter of Information Security Governance
- IS Governance Metrics
- Developing an IS Strategy – Common Pitfalls
- IS Strategy Objectives
- Determining Current State of Security
- Strategy Resources
- Strategy Constraints
- Action Plan Immediate Goals
- Action Plan Intermediate Goals

2. Information Security Risk Management & Compliance

- Effective Information Security Risk Management
- Integration into Life Cycle Processes
- Implementing Risk Management
- Risk Identification and Analysis Methods
- Mitigation Strategies and Prioritisation
- Reporting Changes to Management

3. Information Security Program Development & Management

- Planning
- Security Baselines
- Business Processes
- Infrastructure
- Malicious Code (Malware)
- Life Cycles
- Impact on End Users
- Accountability
- Security Metrics
- Managing Internal and External Resources

4. Information Security Incident Management

- Implementing Effective Information Security Management
- Security Controls and Policies
- Standards and Procedures
- Trading Partners and Service Providers
- Security Metrics and Monitoring
- The Change Management Process
- Vulnerability Assessments
- Due Diligence
- Resolution of Non-Compliance Issues
- Culture, Behaviour and Security Awareness