CISM Certified Information Security Manager

Course Duration: 4 day; / 28 hours; Instructor-led/ remote online training
Time: 9.00am – 5.00pm
Break: 10.15am – 10.30am /3.15pm – 3.30pm
Lunch: 1.00pm – 2.00pm

OVERVIEW
The ISACA® Certified Information Security Manager™ is the fastest growing and arguably the most prestigious qualification available for Information Security managers today.

CISM properly recognises that security is first and foremost a management rather than a technical issue. 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 5-day training program provides an intense environment in which participants will acquire the skills and knowledge needed to meet the requirements of the CISM certification.

AUDIENCE
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
PREREQUISITES

Who Should Earn the CISM Designation?

CISM is more than an entry-level certification. It is specifically developed for the information security professional who has acquired experience working on the front lines of information security. Individuals with three years or more of experience managing the information security function of an enterprise or performing such duties will find CISM tailored to their knowledge and skills.

The Exam is held twice per year in June and December and exam registrations close around 2 months prior. Refer to www.isaca.org for exam dates and exam registration.

METHODOLOGY
This program will be conducted with interactive lectures, PowerPoint presentations, discussions and practical exercises

COURSE OUTLINES

Module 1: Information Security Governance and Strategy

Lesson
- 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

Practice Questions; Review of Practice Questions;
Reference Materials and Glossary

Module 2: Information Security Risk Management and Compliance

Lesson
- 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

Practice Questions; Review of Practice Questions; Reference Materials and Glossary

Module 3: Information Security Program Development and Management

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

Practice Questions; Review of Practice Questions;
Reference Materials and Glossary

Module 4: Information Security Incident Management

Lesson
- 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, Behavior and Security Awareness