Certified Information Security Manager (CISM)

Course Objectives

In-depth coverage of the four domains required to pass the CISM exam:

- Information Security Governance
- Information Risk Management and Compliance
- Information Security Program Development and Management
- Information Security Incident Management

Description

Information Systems Audit and Control Association (ISACA) provides three testing opportunities each year, so we developed this Certified Information Security Manager (CISM) exam prep course to help you get it right the first time. The course focuses on advanced risk management and specific compliance and security management operations.

Target Audience

The training programme is designed for **Senior Executives, IT managers, information security professionals, IT software system and application developers and IT auditors.**

Training Outline

Testing-Taking Tips and Study Techniques

- Preparation for the CISM exam
- Submitting Required Paperwork
- Resources and Study Aids
- Passing the Exam, the First Time

Information Security Governance

- Asset Identification
- Risk Assessment
- Vulnerability Assessments
- Asset Management

Information Risk Management

- Asset Classification and Ownership
- Structured Information Risk Assessment Process
- Business Impact Assessments
- Change Management

Information Security Program Development

- Information Security Strategy
- Program Alignment of Other Assurance Functions
- Development of Information Security Architectures
- Security Awareness, Training, and Education
- Communication and Maintenance of Standards, Procedures, and Other Documentation
- Change Control
- Lifecycle Activities
- Security Metrics

Information Security Program Management

<ulstyle="padding-left: 5%;">

- Security Program Management Overview
- Planning
- Security Baselines
- Business Processes
- Security Program Infrastructure
- Lifecycle Methodologies
- Security Impact on Users
- Accountability
- Security Metrics
- Managing Resources

Incident Management and Response

- Response Management Overview
- Importance of Response Management
- Performing a Business Impact Analysis
- Developing Response and Recovery Plans
- The Incident Response Process
- Implementing Response and Recovery Plans
- Response Documentation
- Post-Event Reviews

Review and Q&A Session

- Test Review and Test Prep

Prerequisite

- Five years of experience with audit, IT systems, and security of information systems; systems administration experience; familiarity with TCP/IP; and an 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.

+60 16 223 9422
contact@quandatics.com