

Course Title: CISM - Certified Information Security manager

Course Introduction

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 or managing those who do. Individuals with five years or more of experience managing information security will find CISM[®] tailored to their expertise and the increasing global demand for high standards of certified professionalism.

CISM[®] certification is for the individual who manages, designs, oversees and/or assesses an enterprise's information security (IS). The CISM[®] certification promotes international practices and provides executive management with assurance that those earning the designation have the required experience and knowledge to provide effective security management and consulting services.

Course Objectives

- Obtain the skills and knowledge of the core competencies required of an information security professional, to be gained in a structured learning environment.
- Gain the knowledge required for, and have thoroughly prepared for the certification examination in systematic way.

What you will learn

On completion of the course, delegates will be able to enhance their preparation for the CISM[®] exam by learning about:

- Information Security Governance
- Information Risk Management
- Information Security Program Development
- Creating and maintaining a program to implement the information security governance strategy
- Information Security Program Management
- Information security activities to execute the information security program
- Incident Management and Response

Course Prerequisites

- Prior handling of Information security tasks will be an added advantage. Knowledge or experience of Managerial level of at least 3 years is required. Knowledge or equivalent experience of information security fundamentals is required.

Target Group

- Security professionals with 3-5 years of front-line experience
- Information security managers or those with management responsibilities
- Information security staff and other information security assurance providers who

require and in-dept understanding of information security management including CIOs, CISOs, CSOs, risk managers, compliance personnel and security auditors

Learning Level

Advanced

Course Duration

5 days

Benefits of becoming a CISM

- Recognition of attainment of advanced job skills as required for an information security professional
- Worldwide recognition as an information security manager
- Opportunity to build upon existing certifications/credentials already earned
- Provides tangible evidence of career growth
- Potential for a salary increase and/or promotion

Course Outline

Chapter 1 – Information Security Strategy

Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations.

- Understanding information security governance concepts and issues
- Examining the scope and charter of information security governance
- Pinpointing information governance metrics
- Overcoming common pitfalls when creating and information systems strategy
- Determining your organisation's current state of security
- Identifying strategy resources and constraints
- Detailing an appropriate action plan

Chapter 2 –Risk Management

Identify and manage information security risks to achieve business objectives.

- Outlining the principles of effective information security risk management
- Assessing integration into the life cycle processes
- Practical steps to implement risk management
- Evaluating risk identification and analysis methods
- Implementing mitigation strategies and prioritisation
- Methods to reporting changes to management

Chapter 3 – Information Security Program Management

Design and develop an information security program to implement the information security governance framework.

- Applying project management practices
- Planning and business processes
- Infrastructure
- Life cycles processes
- Impact on end users
- Managing internal and external resources

Chapter 4 – Information Security Management

Oversee and direct information security activities to execute the information security program.

- Understanding information systems operations
- Identifying appropriate security controls and policies
- Applying standards and procedures
- Pinpointing trading partners and service providers
- Outlining security metrics and monitoring
- Assessing the change management process
- Undertaking vulnerability assessments and due diligence
- Examining culture, behaviour and security awareness

Chapter 5 – Response Management

Develop and manage a capability to respond to and recover from disruptive and destructive information security events.

- Assessing the role of business continuity and disaster recovery planning
- Conducting the auditing process of business continuity and disaster recovery
- Performing a business impact analysis
- Developing response and recovery plans
- Identifying incident response processes
- Testing response and recovery plans
- Executing response and recovery plans