

# CISM Exam Preparation Training

## Introduction

CISM is one of the most important 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 CISM holders have the experience and knowledge to offer effective security management and advice. This course provides an intense environment in which participants can acquire the skills and knowledge expected of a world-class information security manager.

The CISM Exam Preparation course is an intensive, four-day review program to prepare individuals who are planning to sit for the Certified Information Security Manager (CISM) exam. The course focuses on the key points covered in the CISM Review Manual 15th Edition and includes class lectures, group discussions/activities, exam practice and answer debrief. The course is intended for individuals with familiarity with and experience in information security management.

## Course Objectives

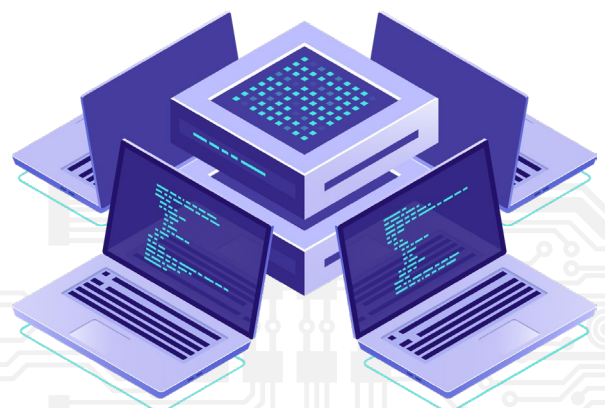
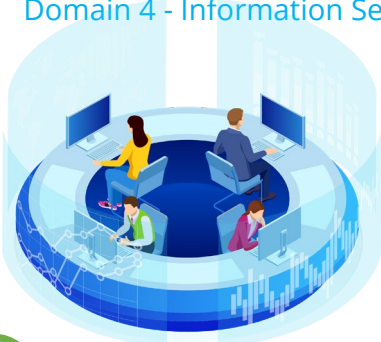
At the conclusion of this course, attendees will understand:

- The specific requirements for passing the CISM Exam and attaining your certification,
- Key concepts, tasks and knowledge related to the duties of an information security manager.
- Develop an information security strategy and plan of action to implement the strategy
- Manage and monitor information security risks
- Build and maintain an information security plan both internally and externally
- Implement policies and procedures to respond to and recover from disruptive and destructive information security events
- Successful methods evaluating exam questions and answers, including analysis and explanations.

## CISM Certification Exam Domain

The training will cover job practice domains, knowledge and supporting tasks are as follows:

- Domain 1 - Information Security Governance (17% of exam)
- Domain 2 - Information Risk Management (20% of exam)
- Domain 3 - Information Security Program (33% of exam)
- Domain 4 - Information Security Incident Management (30% of exam)



For more information contact our Academic Team

Telephone: +27 11 678 0653 | WhatsApp: +27 78 178 3979

Email: [training@naveg.co.za](mailto:training@naveg.co.za) | [www.naveg-academy.com](http://www.naveg-academy.com)

Below are the key domains, subtopics and tasks candidates will be tested:

1	Information Security Governance
A	Enterprise Governance
1A1	Organizational Culture
1A2	Legal, Regulatory, and Contractual Requirements
1A3	Organizational Structures, Roles, and Responsibilities
B	Information Security Strategy
1B1	Information Security Strategy Development
1B2	Information Governance Frameworks and Standards
1B3	Strategic Planning (e.g., budgets, resources, business case).
2	Information Security Risk Management
A	Information Security Risk Assessment
2A1	Emerging Risk and Threat Landscape
2A2	Vulnerability and Control Deficiency Analysis
2A3	Risk Assessment and Analysis
B	Information Security Risk Response
2B1	Risk Treatment / Risk Response Options
2B2	Risk and Control Ownership
2B3	Risk Monitoring and Reporting
3	Information Security Program
A	Information Security Program Development
3A1	Information Security Program Resources (e.g., people, tools, technologies)
3A2	Information Asset Identification and Classification
3A3	Industry Standards and Frameworks for Information Security
3A4	Information Security Policies, Procedures, and Guidelines
3A5	Information Security Program Metrics
B	Information Security Program Management
3B1	Information Security Control Design and Selection
3B2	Information Security Control Implementation and Integrations
3B3	Information Security Control Testing and Evaluation
3B4	Information Security Awareness and Training
3B5	Management of External Services (e.g., providers, suppliers, third parties, fourth parties)
3B6	Information Security Program Communications and Reporting
4	Incident Management
A	Incident Management Readiness
4A1	Incident Response Plan
4A2	Business Impact Analysis (BIA)
4A3	Business Continuity Plan (BCP)
4A4	Disaster Recovery Plan (DRP)
4A5	Incident Classification/Categorization
4A6	Incident Management Training, Testing, and Evaluation
B	Incident Management Operations
4B1	Incident Management Tools and Techniques
4B2	Incident Investigation and Evaluation
4B3	Incident Containment Methods
4B4	Incident Response Communications (e.g., reporting, notification, escalation)
4B5	Incident Eradication and Recovery
4B6	Post-incident Review Practices



For more information contact our Academic Team

Telephone: +27 11 678 0653 | WhatsApp: +27 78 178 3979

Email: [training@naveg.co.za](mailto:training@naveg.co.za) | [www.naveg-academy.com](http://www.naveg-academy.com)

