INFOSECTRAIN

CISM

Certified Information Security Manager
Training & Certification

www.infosectrain.com

INFOSECTRAIN

CISM Introduction

The CISM is a management-focused certification that promotes international security practices and validates individuals' skills to manage designs, oversee, and assess an enterprise's information security. The CISM training course at InfosecTrain helps candidates develop an understanding of risk management, information security governance, and drafting security policies and strategies to achieve the organizational goals.

The CISM certification is a worldwide recognized benchmark of excellence in this field, and the demand for skilled information security management experts is on the rise.Organizations require Information Security Managers who possess the knowledge and expertise to identify critical issues and security challenges. The skills and practices that CISM promotes and evaluates are the building blocks of success in the field.

Learn by Practice

Experience Immersive Learning with highly interactive sessions and hands-on labs

Take Regular Assessments

Bridge knowledge-gaps with our free mock exams and high intensity skill assessments

Earn CPEs

Complete your CPE target by getting CPEs and accessing our library of most trending courses

INFOSECTRAIN

CISM Course Highlights

- **32-Hrs** Instructor-led Training
- **Online Test** Simulations
- Accredited **Instructors**
- **Scenario-Based** Learning

100% Satisfaction Guarantee

Not satisfied with your training on Day 1?
You can get a refund or enroll in a different course.

Access Recorded Sessions

Revisit your lectures, revise your concepts, and retain your knowledge From anywhere, whenever you want.

Extended Post Training

Get extended support even after you finish your training.
We're here for you until you reach your certification goals.

INFOSECTRAIN

Who Should Attend

- Security Consultants and Managers
- Security Auditors and Architects
- Information Security Managers
- IT Directors and Managers
- Security Systems Engineers
- IS/IT Consultants

CISM Exam Information

Certification	Certified Information Security Manager (CISM)
Exam Duration	4 Hours
Number of Questions	150
Exam Pattern	Multiple Choice
Passing Marks	450 out of 800
Languages	English, Japanese, Korean, Spanish

INFOSECTRAIN

Happy Learners Across the World

Vattikooti Venkata Phani Raju

Singapore

Training was based on concepts and techniques required to answer CISM questions. It was very good and glad that I ve been able to get the CISM knowledge to clear the exam.

Saurabh Harjai

India

Holistically the complete training module is comprehensive and has comprehended the CISM concept throughly and boosted our confidence to clear CISM.

Mohammed Rehaan Khan

India

It was the best course I have ever attended. The trainer was highly skilled and professional.

Ashish Aggarwal

India

A very good learning experience with Infosec Train. The trainer is equipped with adequate knowledge of CISM.

INFOSECTRAIN

CISM Domains

- 17% DOMAIN 1 – INFORMATION SECURITY GOVERNANCE
- 20% DOMAIN 2 – INFORMATION SECURITY RISK MANAGEMENT
- 33% DOMAIN 3 – INFORMATION SECURITY PROGRAM
- 30% DOMAIN 4 – INCIDENT MANAGEMENT

INFOSECTRAIN

17% DOMAIN 1 INFORMATION SECURITY GOVERNANCE

This domain will provide you with a thorough insight into the culture, regulations and structure involved in enterprise governance, as well as enabling you to analyze, plan and develop information security strategies. Together, this will affirm high-level credibility in information security governance to stakeholders.

A–ENTERPRISE GOVERNANCE

- Organizational Culture
- Legal, Regulatory and Contractual Requirements
- Organizational Structures, Roles and Responsibilities

B–INFORMATION SECURITY STRATEGY

- Information Security Strategy Development
- Information Governance Frameworks and Standards
- Strategic Planning (e.g., Budgets, Resources, Business Case)

20% DOMAIN 2 INFORMATION SECURITY RISK MANAGEMENT

This domain empowers you to analyze and identify potential information security risks, threats and vulnerabilities as well as giving you all the information about identifying and countering information security risks you will require to perform at management level.

A–INFORMATION SECURITY RISK ASSESSMENT

- Emerging Risk and Threat Landscape
- Vulnerability and Control Deficiency Analysis
- Risk Assessment and Analysis

B–INFORMATION SECURITY RISK RESPONSE

- Risk Treatment / Risk Response Options
- Risk and Control Ownership
- Risk Monitoring and Reporting

INFOSECTRAIN

33% DOMAIN 3 INFORMATION SECURITY PROGRAM

This domain covers the resources, asset classifications and frameworks for information security as well as empowering you to manage information security programs, including security control, testing, comms and reporting and implementation.

A–INFORMATION SECURITY PROGRAM DEVELOPMENT

- Information Security Program Resources (e.g., People, Tools, Technologies)
- Information Asset Identification and Classification
- Industry Standards and Frameworks for Information Security
- Information Security Policies, Procedures and Guidelines
- Information Security Program Metrics

B–INFORMATION SECURITY PROGRAM MANAGEMENT

- Information Security Control Design and Selection
- Information Security Control Implementation and Integrations
- Information Security Control Testing and Evaluation
- Information Security Awareness and Training
- Management of External Services (e.g., Providers, Suppliers, Third Parties, Fourth Parties)
- Information Security Program Communications and Reporting

INFOSECTRAIN

30% DOMAIN 4 INCIDENT MANAGEMENT

This domain provides in-depth training in risk management and preparedness, including how to prepare a business to respond to incidents and guiding recovery. The second module covers the tools, evaluation and containment methods for incident management.

A–INCIDENT MANAGEMENT READINESS

- Incident Response Plan
- Business Impact Analysis (BIA)
- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- Incident Classification/Categorization
- Incident Management Training, Testing and Evaluation

B–INCIDENT MANAGEMENT OPERATIONS

- Incident Management Tools and Techniques
- Incident Investigation and Evaluation
- Incident Containment Methods
- Incident Response Communications (e.g., Reporting, Notification, Escalation)
- Incident Eradication and Recovery
- Post-Incident Review Practices

www.infosectrain.com | sales@infosectrain.com