INFOSECTRAIN

CISM

Certified Information Security Manager

KEY FEATURES

- ISACA Premium Training Partner
- Access to the recorded sessions
- Certified & Experienced Trainers

ISACA ACCREDITED PARTNER CISM

Overview

The CISM certification, which is focused on management, promotes worldwide security practices and acknowledges the professional who manages, designs, oversees, and assesses an organization's information security. The CISM certification is the worldwide recognized benchmark of excellence in this field, and the demand for skilled information security management experts is on the rise.

Target Audience

- Security Consultants and Managers
- IT directors and managers
- Security auditors and architects
- Security systems engineers
- Chief Information Security Officers (CISOs)
- Information security managers
- IS/IT consultants
- Chief Compliance/Privacy/Risk Officers

Pre-Requisite

Submit verified evidence of a minimum of five years of information security work experience, with a minimum of three years of work experience in three or more job practice analysis areas of information security management. The work experience must be gained within the 10 years preceding the application date for certification or within 5 years from the exam's passing date.

The following security-related certifications and information systems management experience can be used to substitute the indicated amount of information security work experience.

TWO YEARS

- Certified Information Systems Auditor (CISA) in good standing
- Certified Information Systems Security Professional (CISSP) in good standing
- Post-graduate degree in information security or a related field (e.g., business administration, information systems, information assurance)

ONE YEAR

- One full year of information systems management experience
- One full year of general security management experience
- Skill-based security certifications (e.g., SANS Global Information Assurance Certification (GIAC), Microsoft Certified Systems Engineer (MCSE), CompTIA Security +, Disaster Recovery Institute Certified Business
- Continuity Professional (CBCP), ESL IT Security Manager)

Completion of an information security management program at an institution aligned with the Model Curriculum

Exam Information

Duration	4 hours
Number of Questions	150
Question format	Multiple Choice
Passing grade	450 out of 800
Languages available	English, Japanese, Korean, Spanish

Why Infosec Train?

- Certified & Experienced Instructor
- Flexible Schedule
- Access to the recorded sessions
- Post Training Support
- Tailor Made Training
- Telegram Discussion Group

Our Expert Instructors

"

Certified Security specialist having several years of experience in Information Security across all domains including application security, vulnerability assessment, ethical hacking, pen testing and IT risk and compliance and more

PRABH NAIR

CISSP I CCSP I CSSLP I CRISC I CISM I CISA I CGEIT

"

Rahul have 19+ years of experience in Information Technology industry with specialization in Information Security. Worked with 100+ clients across 25+ countries through various short-term and long-term assignments. Certified as CISSP, CISM and 10+ more certification

RAHUL

CISSP I CISM I CITP I CMGR I MCMI I MIET I MBCS

"

An IT leader with almost 2 decades of experience in multiple industries, I have conducted over 500 training sessions to over 10000+ Some of the courses that I have taught over the years: CISSP, CCSP, CISM, CISA, CGEIT, CCSK, CompTIA securitY+, cysA+

S. RAI

CISSP I CISM I CCSP I CISA I CASP I MCA I CGEIT I PMP

HAPPY LEARNERS FROM THE WORLD

Puneet Sharma

CISM | India

Trainer explained the key concepts and practiced sample questions as well which would really help us to complete our exam successfully. Important topics were discussed in detail.

Yaqoob Kath

CISM | Canada

The trainer covered many concepts apart from exam perspective which helped in gaining much knowledge.

Shefali Shetty

CISM | India

It was a great learning experience. Instructor is highly knowledgeable and connects well with class citing real life examples. The full team is very helpful and flexible. I recommend Infosectrain for anyone looking forward to take on CISM.

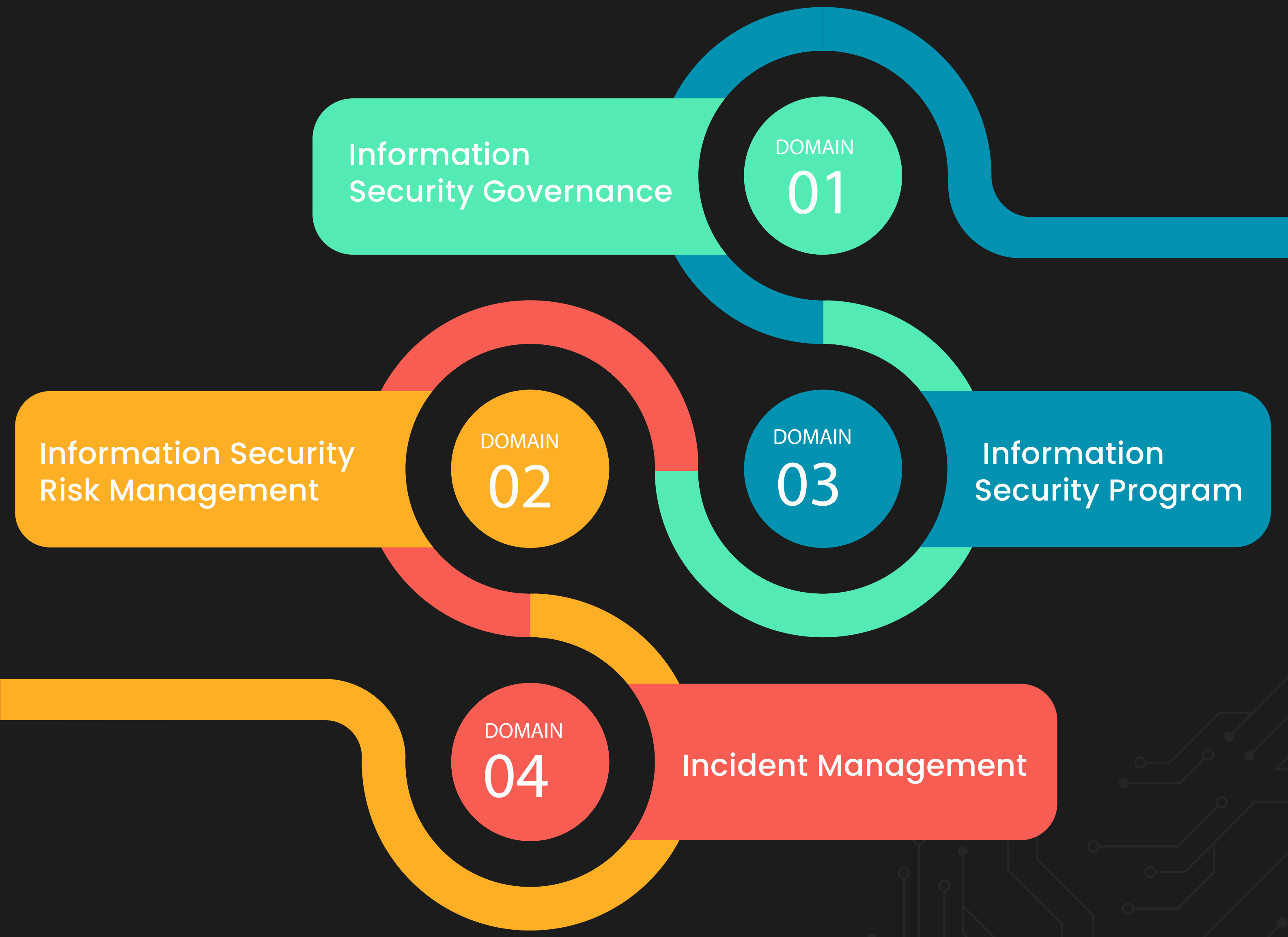
Ravi Prakash Basavaraja

CISM | India

The trainer was excellent in teaching the necessary concepts in the right way. The training will will give anyone a clear picture on the subject, as well as the tips required to face the certification exam.

CISM Course Outline

The four domains in CISM include



DOMAIN 01
Information Security Governance

DOMAIN 02
Information Security Risk Management

DOMAIN 03
Information Security Program

DOMAIN 04
Incident Management

Domain 1: Information Secuirty Governance (17%)

PART A: ENTERPRISE GOVERNANCE

- Importance of Information Security Governance
- Organizational Culture
- Legal, Regulatory and Contractual Requirements
- Organizational Structures, Roles and Responsibilities

PART B: INFORMATION SECURITY STRATEGY

- nformation Security Strategy Development
- Information Governance Frameworks and Standards
- Strategic Planning

Domain 2: Information Security Risk Management (20%)

PART A: INFORMATION RISK ASSESSMENT

- Risk and Threat Landscape
- Vulnerability and Control Deficiency Analysis
- Risk Analysis, Evaluation and Assessment

PART B: INFORMATION RISK RESPONSE

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

Domain 3: Information Security Program (33%)

PART A: INFORMATION SECURITY PROGRAM DEVELOPMENT

- Information Security Program Overview
- Information Security Program Resources
- Information Asset Identification and Classification
- Industry Standards and Frameworks for Information Security

- > Information Security Policies, Procedures and Guidelines
- > Defining an Information Security Program Road Map
- > Information Security Program Metrics

PART B: INFORMATION SECURITY PROGRAM MANAGEMENT

- > Information Security Control Design and Selection
- > Information Security Control Implementation and Integration
- > Information Security Control Testing and Evaluation
- > Information Security Awareness and Training
- > Integration of the Security Program with IT Operations >
- > Management of External Services and Relationships
- > Information Security Program Communications and Reporting

Domain 4: Incident Management (30%)

PART A: INCIDENT MANAGEMENT READINESS

- > Incident Management and Incident Response Overview
- > Incident Management and Incident Response Plans
- > Business Impact Analysis
- > Business Continuity Plan
- > Disaster Recovery Plan
- > Incident Classification/Categorization
- > Incident Management Training, Testing and Evaluation

PART B: INCIDENT MANAGEMENT OPERATIONS

- > Incident Management Tools and Technologies
- > Incident Investigation and Evaluation
- > Incident Containment Methods
- > Incident Response Communications
- > Incident Eradication and Recovery
- > Post-Incident Review Practices

INFOSECTRAIN

www.infosectrain.com | sales@infosectrain.com