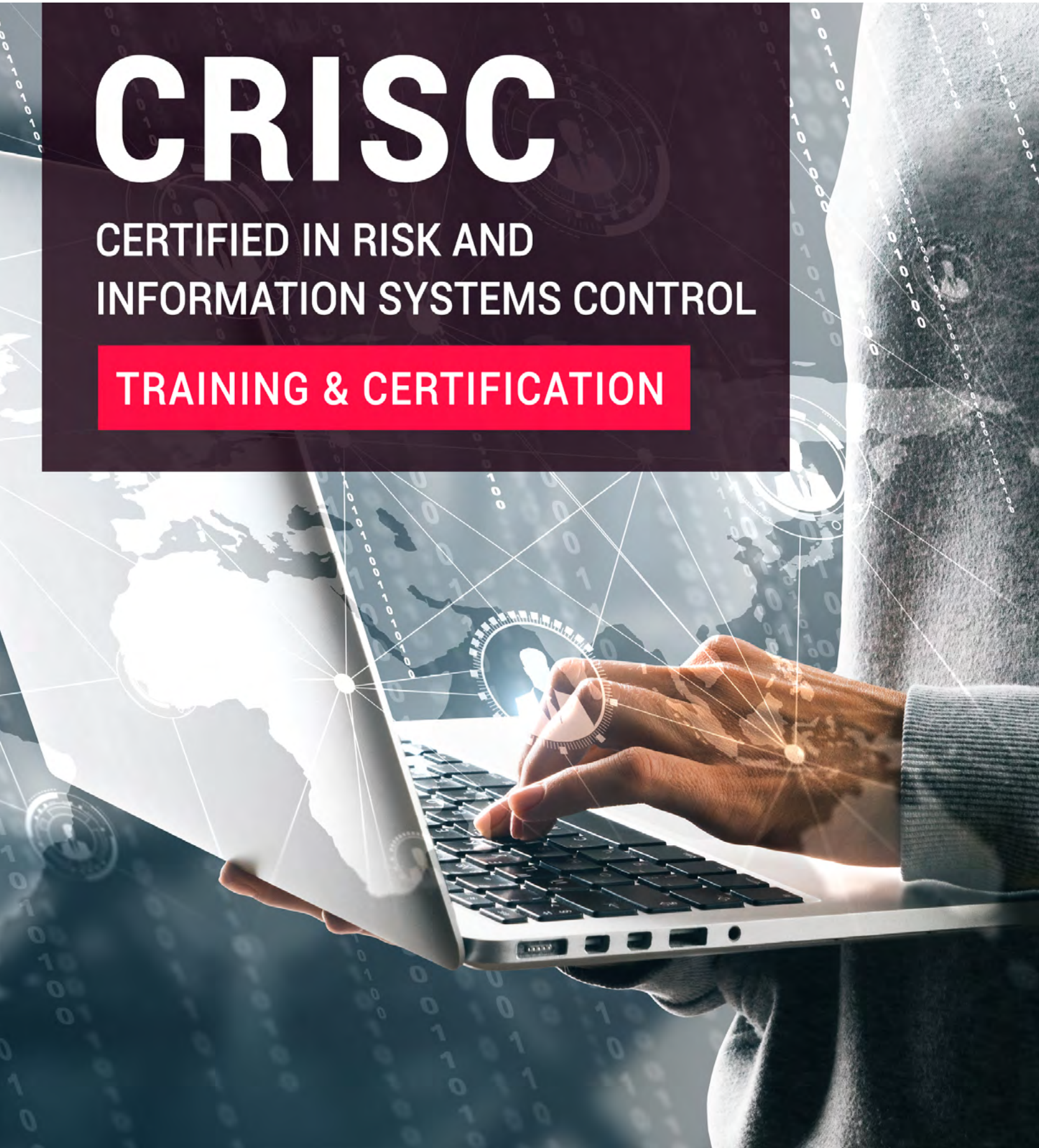
INFOSECTRAIN

CRISC

CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL

TRAINING & CERTIFICATION



INFOSECTRAIN

CRISC Introduction

Certified in Risk and Information System Control (CRISC) certification training program at Infosec Train is developed for those professionals who identify and manage the enterprise risks by implementing information system controls. The training will help you understand the impacts of IT risks and gain technical expertise in implementing proper information security controls to confront the challenges posed by these risks.

CRISC is the most current and rigorous assessment available to evaluate IT professionals' risk management proficiency and other employees within an enterprise or financial institute.

Those who earn CRISC help enterprises understand business risks and have the technical knowledge to implement appropriate IS controls.

INFOSECTRAIN

CRISC Course Highlights

32-Hrs
Instructor-led Training

Accredited
Instructors

Telegram
Discussion Group

100% Money Back Guarantee

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

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

- CEOs/CFOs
- Chief Audit Executives
- Audit Partners/Heads
- CIOs/CISOs
- Chief Compliance/ Privacy/Risk Officers
- Security Managers/ Directors/Consultants

CISM Exam Information

Certification	Certified in Risk and Information Systems Control
Exam Duration	4 Hours
Number of Questions	150
Exam Pattern	Multiple Choice
Passing Marks	450 out of 800
Languages	English, French, German, Hebrew, Italian, Japanese, Korean, Spanish, Turkish, Chinese

INFOSECTRAIN

Happy Learners Across the World

I have pursued CISSP, CRISC abd CISM from Infosectrain. The Trainers dedication and sincerity towarnds his classes is something that inspires me a lot personally.

Waseem Akram Fareed
Canada

Hey, This is Dileep from sony India. I attended the CRISC training with InfosecTrain. The session was simply wonderful. Thankyou so much.

Dileep Narayanan
Singapore

It was a good training. Thank you trainer. Please continue the good work, InfosecTrain.

Muni Prasad
United Arab Emirates

The training has been a wonderful experience. The trainer has complete knowledge about the course abd makes sure topics are covered with examples to deliver complete understanding to us.

Neha Bhardwaj
India

INFOSECTRAIN

CRISC Domains

26%
DOMAIN 1
GOVERNANCE

20%
DOMAIN 2
IT RISK ASSESSMENT

32%
DOMAIN 3
RISK RESPONSE
AND REPORTING

20%
DOMAIN 4
INFORMATION TECHNOLOGY
AND SECURITY

INFOSECTRAIN

26% DOMAIN 1

GOVERNANCE

The governance domain interrogates your knowledge of information about an organization's business and IT environments, organizational strategy, goals and objectives, and examines potential or realized impacts of IT risk to the organization's business objectives and operations, including Enterprise Risk Management and Risk Management Framework.

A—ORGANIZATIONAL GOVERNANCE

- Organizational Strategy, Goals, and Objectives
- Organizational Structure, Roles and Responsibilities
- Organizational Culture
- Policies and Standards
- Business Processes
- Organizational Assets

B—RISK GOVERNANCE

- Enterprise Risk Management and Risk Management Framework
- Three Lines of Defense
- Risk Profile
- Risk Appetite and Risk Tolerance
- Legal, Regulatory and Contractual Requirements
- Professional Ethics of Risk Management

INFOSECTRAIN

20% DOMAIN 2

IT RISK ASSESSMENT

This domain will certify your knowledge of threats and vulnerabilities to the organization's people, processes and technology as well as the likelihood and impact of threats, vulnerabilities and risk scenarios.

A—IT RISK IDENTIFICATION

- Risk Events (e.g., contributing conditions, loss result)
- Threat Modelling and Threat Landscape
- Vulnerability and Control Deficiency Analysis (e.g., root cause analysis)
- Risk Scenario Development

B—IT RISK ANALYSIS AND EVALUATION

- Risk Assessment Concepts, Standards and Frameworks
- Risk Register
- Risk Analysis Methodologies
- Business Impact Analysis
- Inherent and Residual Risk

INFOSECTRAIN

32% DOMAIN 3

RISK RESPONSE AND REPORTING

This domain deals with the development and management of risk treatment plans among key stakeholders, the evaluation of existing controls and improving effectiveness for IT risk mitigation, and the assessment of relevant risk and control information to applicable stakeholders.

A—RISK RESPONSE

- Risk Treatment / Risk Response Options
- Risk and Control Ownership
- Third-Party Risk Management
- Issue, Finding and Exception Management
- Management of Emerging Risk

B—CONTROL DESIGN AND IMPLEMENTATION

- Control Types, Standards and Frameworks
- Control Design, Selection and Analysis
- Control Implementation
- Control Testing and Effectiveness Evaluation

C—RISK MONITORING AND REPORTING

- Risk Treatment Plans
- Data Collection, Aggregation, Analysis and Validation
- Risk and Control Monitoring Techniques
- Risk and Control Reporting Techniques (heatmap, scorecards, dashboards)
- Key Performance Indicators
- Key Risk Indicators (KRIs)
- Key Control Indicators (KCIs)

INFOSECTRAIN

22% DOMAIN 4

INFORMATION TECHNOLOGY AND SECURITY

In this domain we interrogate the alignment of business practices with Risk Management and Information Security frameworks and standards, as well as the development of a risk-aware culture and implementation of security awareness training.

A—INFORMATION TECHNOLOGY PRINCIPLES

- Enterprise Architecture
- IT Operations Management (e.g., change management, IT assets, problems, incidents)
- Project Management
- Disaster Recovery Management (DRM)
- Data Lifecycle Management
- System Development Life Cycle (SDLC)
- Emerging Technologies

B—INFORMATION SECURITY PRINCIPLES

- Information Security Concepts, Frameworks and Standards
- Information Security Awareness Training
- Business Continuity Management
- Data Privacy and Data Protection Principles

www.infosectrain.com | sales@infosectrain.com