INFOSECTRAIN
Educate. Excel. Empower.

ISACA ACCREDITED PARTNER

CRISC 2025

Certified in Risk and Information Systems Control

Certification Training

Course Highlights

32-Hour LIVE
Instructor-Led
Training

ISACA
Premium
Training Partner

Immersive
Learning

Highly Interactive
and **Dynamic
Sessions**

98%
Exam
Pass Rate

Experienced
Industry
Experts

Practice with
**Online Test
Engine**

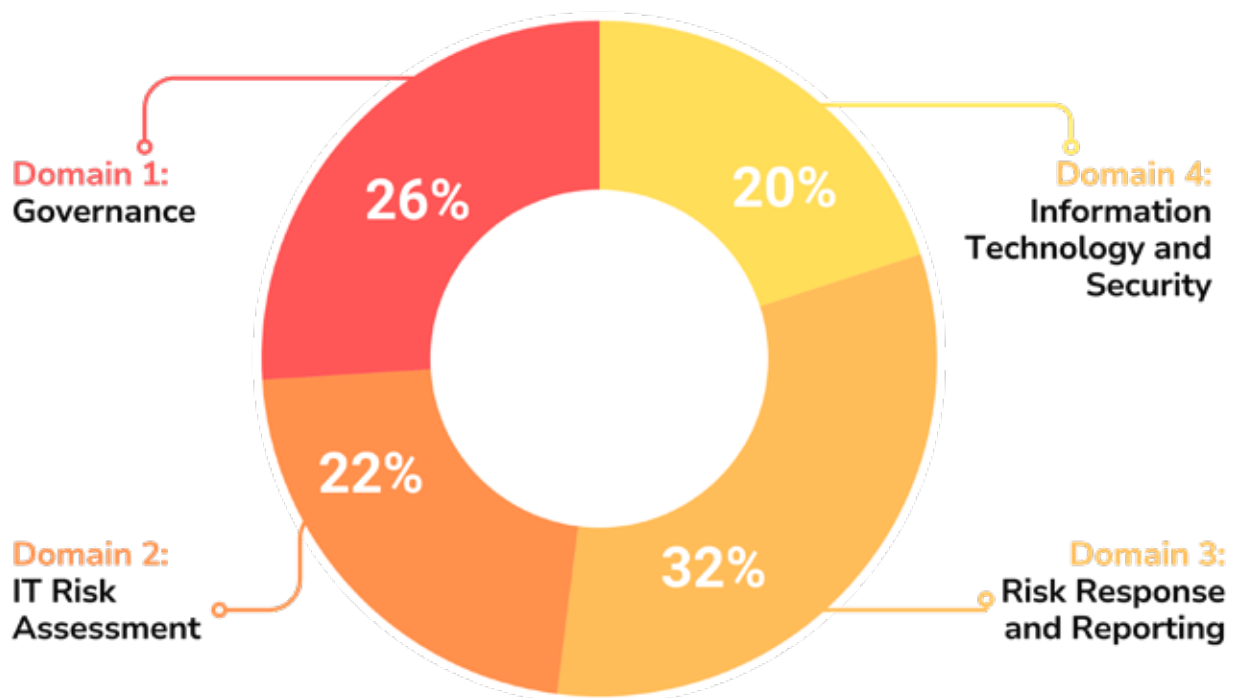Post **Training
Support** Till
Exam

Telegram Group
for Exam
Practice

About Course

The CRISC 2025 Certification Training with InfosecTrain equips IT professionals to tackle the unique challenges of enterprise risk management, preparing them to serve as strategic partners within their organizations. As the industry's leading certification in risk management, CRISC provides a rigorous, up-to-date evaluation of professional expertise in managing risk and implementing IS controls. By earning CRISC, individuals demonstrate their ability to assess, understand, and address business risks effectively, empowering enterprises and financial institutions to strengthen their risk resilience and safeguard their operations.

CRISC domains & Weightage

Domain 1:
Governance
26%

Domain 4:
Information
Technology and
Security
20%

Domain 2:
IT Risk
Assessment
22%

Domain 3:
Risk Response
and Reporting
32%

Course Objectives

- Identify the IT risk management strategy in support of business objectives and alignment with the Enterprise Risk Management (ERM) strategy.

- Analyze and evaluate IT risk to determine the likelihood and impact on business objectives to enable risk-based decision making.

- Determine risk response options and evaluate their efficiency and effectiveness to manage risk in alignment with business objectives.

- Continuously monitor and report on IT risk and controls to relevant stakeholders to ensure the continued efficiency and effectiveness of the IT risk management strategy and its alignment with business objectives.

Target Audience

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

Pre-requisites

- A minimum 3 years of work experience across at least two of the four CRISC domains.
- Pass the CRISC Exam within the last five years.

INFOSECTRAIN

Exam Information

Certification	Certified in Risk and Information Systems Control
Exam Duration	240 minutes
Number of Questions	150 Questions
Exam Pattern	Multiple Choice
Passing Marks	450 out of 800
Exam Languages	English, French, German, Hebrew, Italian, Japanese, Korean, Spanish, Turkish, Chinese

Course Content

Domain 1   Governance (26%)

Part A: Organizational Governance

- Strategy, Goals, and Objectives
- Organizational Structure, Roles, and Responsibilities
- Organizational Culture and Ethics
- Policies and Standards
- Business Processes and Resilience
- Organizational Asset Management

Part B: Risk Governance

- Enterprise Risk Management
- Lines of Defense
- Risk Profile
- Risk Appetite and Risk Tolerance
- Risk Frameworks, Legal, Regulatory, and Contractual Requirements

Domain 2 **IT Risk Assessment** (22%)

Part A: Risk Identification

- Risk Events
- Threat Modeling and Threat Landscape
- Vulnerability Management
- Risk Scenario Development and Evaluation

Part B: Risk Analysis

- Risk Assessment Concepts and Standards
- Business Impact Analysis (BIA)
- Risk Register
- Risk Analysis Methodologies
- Inherent, Residual, and Current Risk

Domain 3 — Risk Response and Reporting (32%)

Part A: Risk Response

- Risk Response Options
- Risk and Control Ownership
- Vendor/Supply Chain Risk Management
- Issues, Findings, Exceptions, and Exemptions Management

Part B: Control Design and Implementation

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

Part C: Risk Monitoring and Reporting

- Risk Action Plans
- Data Collection, Aggregation, Analysis, and Validation
- Risk and Control Metrics
- Risk and Control Monitoring and Reporting Techniques
- Monitoring and Reporting of Emerging Risks

Domain 4 — Information Technology and Security (20%)

Part A: Information Technology Principles

- Technology Roadmaps and Enterprise Architecture (EA)
- Operations Management
- System Development Life Cycle (SDLC)
- Data Lifecycle Management
- Portfolio and Project Management
- Technology Resilience and Disaster Response/Recovery
- Emerging Technologies

Part B: Information Security Principles

- Security Concepts, Frameworks, and Standards
- Security/Risk Awareness and Training
- Data Privacy and Data Protection Principles

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on