INFOSECTRAIN

ISACA ACCREDITED PARTNER CRISC

CRISC

CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL

TRAINING & CERTIFICATION

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.

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.

Pre-requisites

- Take the CRISC exam to demonstrate your information security knowledge. Even without meeting experience requirements, passing qualifies you to apply for certification within five years once experience criteria are met.
- Complete a minimum of 3 years in information systems auditing, control, or security within the CRISC job practice areas, with experience gained within the last 10 years. Candidates have up to 5 years from the passing date to apply for certification.
- Fulfill 120 Continuing Professional Education (CPE) hours every three years, with at least 20 hours per year. CPE hours may also count toward other ISACA certifications if requirements align.
- Uphold ISACA's Code of Professional Ethics as a CRISC-certified professional, ensuring ethical conduct in both professional and personal activities.

CRISC Course Highlights

32-Hour LIVE
Instructor-led Training

Online Test
Simulations

Accredited Instructors
(18+ Years of Experience)

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.

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.

Who Should Attend

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

CRISC 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

Our Expert Instructors

PRABH NAIR

18+ Years Of Experience

CISSP-ISSAP | CGRC | CCSP | CSSLP | CCISO | CISM | CISA | CRISC | CGEIT | CIPM CIPPE | CDPSE

18+ years of IT industry experience, specializing in Information Security. Expertise spans Vulnerability Assessment & Penetration Testing, Application Security, IT Governance, Risk & Compliance, and Security Solutions. Led global Information Security operations for a US-based IT Service Provider with a presence in the US, Canada, India, and Sri Lanka. Delivered services to 250+ organizations across 25+ countries through diverse assignments.

KHALID

20+ Years Of Experience

CRISC | CISM | CISA | ISO 27001 Lead Implementer | CC | ITIL V4 Foundation | PMP ITIL Intermediate – Service Operations | Network+ | A+

Khalid Duduke has over twenty years of experience as an IT Management professional in various sectors such as Telecom, Banking, and Government organizations in the Middle East. He has a solid understanding of IT Project Management, Service Operation, Delivery, and Audit/Compliance. Khalid is known for his excellent organizational skills, effective interpersonal communication, and collaborative teamwork abilities. His skills are adaptable to executive roles, making him a valuable addition to any leadership team.

Khalid Duduke, an experienced trainer, demonstrates exceptional skill in simplifying complex ideas. His clear communication style helps learners grasp difficult concepts easily. Khalid's friendly approach encourages open discussions and sharing of knowledge. He adjusts training sessions to suit different learning styles. Khalid's engaging teaching techniques create a rewarding learning environment for everyone involved.

KK SINGH

18+ Years Of Experience

C|CISO | CISSP | CCSP | CISM | CRISC | CISA | CCSK | CCAK | CDPSE | CEH | RHCSA GRCA | GRCP | CPP | PSP | PCI | AZ-900 | GDPR

With 18+ years of experience, KK is a seasoned Cyber Security Professional with a stellar record in developing and executing cybersecurity strategies for global organizations. He is an expert dedicated to safeguarding sensitive data and ensuring the integrity and availability of critical systems. He has extensive experience in the evolving cybersecurity landscape, excelling in areas such as risk management, incident response, security architecture, and both network and cloud security. His expertise also covers identity and access management, digital transformation security, DevSecOps, and compliance with standards like GDPR and ISO 27001. Equipped with advanced knowledge in blockchain, AI/ML security, and frameworks like Archer GRC, he is committed to staying ahead of emerging threats and delivering comprehensive protection for today's complex digital environment. Holding certifications such as C|CISO, CISSP, CCSP, CISM, CRISC, CISA, CCSK, CCAK, CDPSE, CEH, RHCSA, GRCA, GRCP, CPP, PSP, and PCI, KK is a recognized Cloud & Cybersecurity Strategist and a prominent CyberSec Leader, Speaker, and Mentor. He is committed to staying ahead of emerging threats and ensuring robust protection in today's complex digital world.

JEEVAN

8+ Years Of Experience

CISA | CISM | CISSP | CRISC | ECSA | CGEIT | CEH

With 8+ years of experience as an IT Information Security Analyst, Jeevan also possesses expertise in IT SOX compliance, proficiency in General IT Controls, Business Continuity Management, Application Controls and performing SOC1 and SOC2 reviews. He has also conducted application security assessments, business cycle controls (BCCs) review, general computer controls (GCCs), and carried out IT strategy reviews and assisted in implementation of an IT governance framework.

INFOSECTRAIN

ISACA ACCREDITED PARTNER CRISC

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 and makes sure topics are covered with examples to deliver complete understanding to us.

Neha Bhardwaj
India

CRISC Domains

26%
DOMAIN 1
GOVERNANCE

20%
DOMAIN 2
IT RISK ASSESSMENT

32%
DOMAIN 3
RISK RESPONSE
AND REPORTING

22%
DOMAIN 4
INFORMATION TECHNOLOGY
AND SECURITY

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

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

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)

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

INFOSECTRAIN

www.infosectrain.com I sales@infosectrain.com