Document Generated: 11/14/2026

Learning Style: Online Instructor-Led

Technology: ISACA

Difficulty: Advanced

Course Duration: 4 Days

Certified Risk & Information Systems Control (CRISC)



The CRISC certification is designed for IT professionals who identify and manage risks through the development, implementation, and maintenance of information systems (IS) controls. It is recognized globally as a benchmark of excellence in risk management and information system control.

The course helps you build a solid understanding of risk management practices and how to align them with business goals. CRISC-certified professionals are seen as strategic partners in the enterprise, able to bridge the gap between IT risk management and business operations.

Course Objectives:

- Identify and evaluate IT risk to help organizations achieve their objectives.
- Design, implement, monitor, and maintain risk-based, efficient, and effective information systems controls.
- Develop and manage an organization's risk management framework.
- Understand and apply governance practices to align risk management with enterprise strategy.

Audience:

- IT risk management professionals with at least 3 years of relevant professional work experience in IT risk and information systems control including:Security
- Directors/Managers/Consultants
- Compliance/Risk/Privacy Directors and Managers
- IT Audit Directors/Managers/Consultants
- Compliance/Risk/Control Staff

Prerequisites:

- A minimum of three years of cumulative work experience in IT risk management and IS control in at least two of the four domains, with one domain being either Governance or Risk Response.
- Experience must be gained within the 10 years preceding the application or within five years after passing the exam.

Course Outline:

Domain 1: Governance

- Risk Assessment Concepts, Standards and Frameworks
- Organizational Strategy, Goals and Objectives
- Organizational Structure, Roles and Responsibilities
- Organizational Culture and Assets
- Policies, Standards and Business Processes
- Enterprise Risk Management, Risk Management Frameworks and Three Lines of Defense
- Risk Profile, Risk Appetite and Risk Tolerance
- Navigating Professional Ethics of Risk Management and Requirements in Laws, Regulations and Controls

Domain 2: IT Risk Assessment

- Risk Events, Threat Modeling and Threat Landscape
- Vulnerability and Control Deficiency Analysis
- Risk Scenario Development
- Risk Register
- Risk Analysis Methodologies
- Business Impact Analysis
- Inherent, Residual and Current Risk

Domain 3: Risk Response and Reporting

- Risk Treatment/Risk Response Options
- Risk and Control Ownership
- Managing Risk from Processes, Third Parties and Emerging Sources
- Control Types, Standards and Frameworks

- Control Design, Selection and Analysis
- Control Implementation, Testing and Effectiveness
- Risk Treatment Plans
- Data Collection, Aggregation, Analysis and Validation
- Risk and Control Monitoring and Reporting Techniques
- Performance, Risk and Control Metrics

Domain 4: Information Technology and Security

- Enterprise Architecture
- IT Operations Management
- Project Management
- Disaster Recovery Management
- Data Life Cycle Management
- System Development Life Cycle
- Emerging Technologies
- Information Security Concepts, Frameworks, Standards and Awareness Training
- Business Continuity Management
- Data Privacy and Protection Principles