ISACA Certified in Risk and Information Systems Control incl QAE

Duration: 4 Days Course Code: CRISC

Overview:

Prepare the CRISC - Certified Risk and Information System Control certification
This CRISC training course, in association with ISACA, prepares IT professionals for real-world threats with relevant tools to assess, govern and mitigate risk, and is targeting certification preparation.
The CRISC - Certified Risk and Information System Control - certificate gives you international recognition (from ISACA) as a security professional. The CRISC extensive set of online practice questions (QAE) are included in the courseprice.
The CRISC designation will not only certify professionals who have knowledge and experience identifying and evaluating entity-specific risk, but also aid them in helping enterprises accomplish business objectives by designing, implementing, monitoring and maintaining risk-based, efficient and effective IS controls. **Continuing Professional Education (CPE) :** 31**Practice questions (QAE = Questions, Answers and Explanations) :** 6 month access

Updated 9/2026

Target Audience:

CRISC is designed for IT professionals, risk professionals, business analysts, and project manager and/or compliance professionals and anyone who has job responsibilities in the following areas: Risk identification, assessment, evaluation, risk response, monitoring and IS control design/monitoring and implementation/maintenance.

Objectives:

- After this course participants should be able to:
- **Understand Master Governance Frameworks:** Understand organizational structures, policies, and accountability principles required to govern enterprise IT risk.
- **Assess IT Risk**: Identify threats, vulnerabilities, and impacts on business objectives to evaluate risk scenarios and assign accurate ratings.
- **Implement Risk Responses**: Formulate and execute practical risk treatment plans (mitigate, transfer, avoid, or accept) and monitor their performance.
- **Optimize Security Controls:** Design, implement, and maintain effective information systems controls to safeguard modern enterprise assets.
- **Align IT with Business Goals:** Translate technical risk data into meaningful business metrics to help leadership make informed strategic decisions

Prerequisites:

There is no prerequisite to take the CRISC exam; however, in order to apply for CRISC certification you must meet the necessary experience requirements as determined by ISACA (see below).

Testing and Certification

The CRISC exam lasts **4 hours** and consists of **150 multiple-choice questions in English**.

Exam Domains:

- **Governance** – 26%
- **IT Risk Assessment** – 22%
- **Risk Response and Reporting** – 32%
- **Information Technology and Security** – 20%

Exam Voucher

Please note that the exam voucher for the official CRISC exam is **not included in the course price**. However, the exam voucher can be purchased when attending the associated training.

The exam voucher is available **only to Global Knowledge course**

attendees and cannot be purchased as a standalone product.

Certification Requirements

To obtain the CRISC certification, candidates must:

- Pass the official **CRISC exam**.
- Have **three (3) or more years of cumulative work experience** performing the tasks of a CRISC professional across at least **two (2) CRISC domains**, with at least one year of experience in **Domain 1 or Domain 2**. There are **no substitutions or experience waivers**.

Follow-on-Courses:

Management & Governance Paths

- **CISM (Certified Information Security Manager):** Focuses on security program management, strategy, and incident management.
- **CDPSE (Certified Data Privacy Solutions Engineer):** Focuses on privacy governance, privacy by design, and technical privacy controls.

Audit & Compliance Paths

- **CISA (Certified Information Systems Auditor):** Focuses on evaluating IT controls, compliance, and safeguarding information assets.
- **ISO 27001LI - ISO27001LA Lead Implementer / Auditor:** Provides hands-on operational training for building and auditing information security management systems (ISMS).

Content:

Domain 1: Governance

A. Organizational Governance

- Strategy, Goals, and Objectives
- Organizational Structure, Roles, and Responsibilities
- Organizational Culture and Ethics
- Policies and Standards
- Business Processes and Resilience (e.g., DRP, BCP)
- Organizational Asset Management

B. Risk Governance

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

Domain 2: Risk Assessment

A. Risk Identification

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

B. Risk Analysis

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

Domain 3: Risk Response and Reporting

A. Risk Response

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

B. Control Design and Implementation

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

C. Risk Monitoring and Reporting

- Risk Action Plans Data Collection, Aggregation, Analysis, and Validation
- Risk and Control Metrics (e.g., KRIs, KCIs, KPIs)
- Risk and Control Monitoring Techniques
- Risk and Control Reporting Techniques (e.g., heatmaps, scorecards, dashboards)
- Monitoring and Reporting of Emerging Risks

Domain 4: Technology and Security

A. Technology Principles

- Technology Roadmaps and Enterprise Architecture (EA)
- Operations Management (e.g., change management, assets, DevOps, problems, incidents)
- System Development Life Cycle (SDLC)
- Data Lifecycle Management
- Portfolio and Project Management (e.g., Agile)
- Technology Resilience and Disaster Response/Recovery
- Emerging Technologies

B. Information Security Principles

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

Additional Information:

QAE (Questions, Answers and Explanations) is online available, via a voucher which is part of the courseware Official course book provided to participants

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK