Certified in Risk and Information Systems Control + Practice questions (QAE)

Duration: 4 Days **Course Code: CRISC** **Delivery Method: Virtual Learning**

Overview:

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. **Continuing Professional Education (CPE) :** 31**Practice questions (QAE = Questions, Answers and Explanations) :** 6 month access

Updated 4/2026

Target Audience:

CRISC is 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:

- The Certified in Risk and Information Systems Control certification is designed for IT professionals who have hands-on experience with risk identification, assessment, and evaluation; risk response; risk monitoring; IS control design and implementation; and IS control monitoring and maintenance.
- 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.
- Governance (25%)
- IT Risk Assessment (20%)
- Risk Response and Reporting (32%)
- Information Technology and Security (22%)

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

Testing and Certification

QAE (Questions, Answers and Explanations) is online available via a voucher which is part of the courseware.

The requirements for certification are:

- Pass the official CRISC-exam
- Three (3) or more years of cumulative work experience performing the tasks of a CRISC professional across at least two (2) CRISC domains, of which one must be in Domain 1 or 2, is required for certification. There are no substitutions or experience waivers.

The exam lasts 4 hours and consists of 150 English Multiple Choice questions.

The examenvoucher for the official CRISC exam is not included in the price.

Content:

DOMAIN 1—Governance 26%

Organizational Governance A

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

Risk Governance B

- 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 ManagementDOMAIN 2—IT Risk Assessment 20%

IT Risk Identification A

- 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

IT Risk Analysis and Evaluation B

- Risk Assessment Concepts, Standards, and Frameworks
- Risk Register
- Risk Analysis Methodologies
- Business Impact Analysis
- Inherent and Residual RiskDOMAIN 3—Risk Response and Reporting 32%

Risk Response A

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

Control Design and Implementation B

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

Risk Monitoring and Reporting C

- 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)DOMAIN 4—Information Technology and Security 22%

Information Technology Principles A

- 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

Information Security Principles B

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

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/