Certified in Risk and Information Systems Control

Duration: 365 Days Course Code: CRISC Delivery Method: Elearning (Self-paced)

Overview:

CRISC is the only certification that prepares and enables IT professionals for the unique challenges of IT and enterprise risk management, and positions them to become strategic partners to the enterprise helping enterprises accomplish business objectives by designing, implementing, monitoring and maintaining risk-based, efficient and effective IS controls.

The CRISC Exam Preparation course is an intensive, Four-day review program to prepare individuals who are planning to sit for the Certified in Risk and Information System Controls™ (CRISC) exam. The course focuses on the key points covered in the CRISC Review Manual 7th Edition and includes class lectures, group discussions, exam practice and answer debriefs. The course is intended for individuals with familiarity with and experience in IT and enterprise risk management.

E-learning (Self-paced)

Interactive self-paced content that provides flexibility in terms of pace. place and time to suit individuals and organizations. These resources also consist of online books, educational podcasts and vodcasts, and video-based learning.

Target Audience:

Individuals who are looking to build a greater understanding of the impact of IT risk and how it relates to their organization. It is for mid-career IT/IS audit, risk and security professionals.

Objectives:

- **After completing this course you should be able to:**
- 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.

Prerequisites:

Attendees should meet the following prerequisites:

- There are 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

Recommended as preparation for the following exam:

- ISACA CRISC Certification Exam

Please Note: Three (3) or more years of experience in IT risk management and IS control. No experience waivers or Substitutions.

Content:

This update to the CRISC exam content outline is based on changes in the work practices of IT risk professionals as well as market dynamics and trends that have placed an increased focus on organizational governance, continuous risk monitoring and reporting, information security and data privacy considerations for effective ITRM. These statements and domains are the results of extensive research, feedback, and validation from IT risk and control subject matter experts and prominent industry leaders from around the globe.

Below are the key domains, subtopics and tasks candidates will be tested on:

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 Management

DOMAIN 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 Risk

DOMAIN 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

Secondary Classifications

Supporting Tasks

- Collect and review existing information regarding the organization's business and IT environments.
- Identify potential or realized impacts of IT risk to the organization's business objectives and operations.
- Identify threats and vulnerabilities to the organization's people, processes, and technology.
- Evaluate threats, vulnerabilities, and risk to identify IT risk scenarios.
- Establish accountability by assigning and validating appropriate levels of risk and control ownership.
- Establish and maintain the IT risk register, and incorporate it into the enterprise-wide risk profile.
- Facilitate the identification of risk appetite and risk tolerance by key stakeholders.
- Promote a risk-aware culture by contributing to the development and implementation of security awareness training.
- Conduct a risk assessment by analyzing IT risk scenarios and determining their likelihood and impact.
- Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation.
- Review the results of risk analysis and

control analysis to assess any gaps between current and desired states of the IT risk environment.
- Facilitate the selection of recommended risk responses by key stakeholders.
- Collaborate with risk owners on the development of risk treatment plans.
- Collaborate with control owners on the selection, design, implementation, and maintenance of controls.
- Validate that risk responses have been executed according to risk treatment plans.
- Define and establish key risk indicators (KRIs).
- Monitor and analyze key risk indicators (KRIs).
- Collaborate with control owners on the identification of key performance indicators (KPIs) and key control indicators (KCIs).
- Monitor and analyze key performance indicators (KPIs) and key control indicators (KCIs).
- Review the results of control assessments to determine the effectiveness and maturity of the control environment.
- Report relevant risk and control information to applicable stakeholders to facilitate risk-based decision-making.
- Evaluate alignment of business practices with risk management and information security frameworks and standards.

Additional Information:

Courseware is provided in a digital format, the voucher for courseware access is distributed prior to the start of the class
The CRISC exam is not included in this training course and candidates must book their Computer-Based Testing (CBT) exam session directly with ISACA. Our experience shows that delegates have the highest chance of success if they sit the exam approximately two to four weeks after completing the training course.

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