# Certified in Risk and Information Systems Control

## Duration: 3 Days  Course Code: CRISC

### Overview:

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.

### 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:

- Risk Identification, Assessment and Evaluation (31%)
- Risk Response (17%)
- Risk Monitoring (17%)
- Information Systems Control Design and Implementation (17%)
- IS Control Monitoring and Maintenance (18%)

### 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

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.

## Content:

Domain 1—Risk Identification, Assessment and Evaluation

- Collect information and review documentation to ensure that risk scenarios are identified and evaluated
- Identify legal, regulatory and contractual requirements and organizational policies and standards related to information systems to determine their potential impact on the business objectives.
- Identify potential threats and vulnerabilities for business processes, associated data and supporting capabilities to assist in the evaluation of enterprise risk.
- Create and maintain a risk register to ensure that all identified risk factors are accounted for.
- Assemble risk scenarios to estimate the likelihood and impact of significant events to the organization.
- Analyze risk scenarios to determine their impact on business objectives.
- Develop a risk awareness program and conduct training to ensure that stakeholders understand risk and contribute to the risk management process and to promote a risk-aware culture.
- Correlate identified risk scenarios to relevant business processes to assist in identifying risk ownership.
- Validate risk appetite and tolerance with senior leadership and key stakeholders to ensure alignment

Domain 2—Risk Response

Identify and evaluate risk response options and provide management with information to enable risk response decisions.

- Review risk responses with the relevant stakeholders for validation of efficiency, effectiveness and economy.
- Apply risk criteria to assist in the development of the risk profile for management approval.

Assist in the development of risk response action plans to address risk factors identified in the organizational risk profile.

- Assist in the development of business cases supporting the investment plan to ensure risk responses are aligned with the identified business objectives.

Domain 3—Risk Monitoring

- Collect and validate data that measure key risk indicators (KRIs) to monitor and communicate their status to relevant stakeholders.
- Monitor and communicate key risk indicators (KRIs) and management activities to assist relevant stakeholders in their decision-making process.
- Facilitate independent risk assessments and risk management process reviews to ensure they are performed efficiently and effectively.
- Identify and report on risk, including compliance, to initiate corrective action and meet business and regulatory requirements.

Domain 4—Information Systems Control Design and Implementation

- Interview process owners and review process design documentation to gain an understanding of the business process objectives.
- Analyze and document business process objectives and design to identify required information systems controls.
- Design information systems controls in consultation with process owners to ensure alignment with business needs and objectives.
- Facilitate the identification of resources (e.g., people, infrastructure, information, architecture) required to implement and operate information systems controls at an optimal level.
- Monitor the information systems control design and implementation process to ensure that it is implemented effectively and within time, budget and scope.
- Provide progress reports on the implementation of information systems controls to inform stakeholders and to ensure that deviations are promptly addressed.
- Test information systems controls to verify effectiveness and efficiency prior to implementation.
- Implement information systems controls to mitigate risk.
- Facilitate the identification of metrics and key performance indicators (KPIs) to

Domain 5—IS Control Monitoring and Maintenance

- Plan, supervise and conduct testing to confirm continuous efficiency and effectiveness of information systems controls.
- Collect information and review documentation to identify information systems control deficiencies.
- Review information systems policies, standards and procedures to verify that they address the organization's internal and external requirements.
- Assess and recommend tools and techniques to automate information systems control verification processes.
- Evaluate the current state of information systems processes using a maturity model to identify the gaps between current and targeted process maturity.
- Determine the approach to correct information systems control deficiencies and maturity gaps to ensure that deficiencies are appropriately considered and remediated.
- Maintain sufficient, adequate evidence to support conclusions on the existence and operating effectiveness of information systems controls.
- Provide information systems control status reporting to relevant stakeholders to enable informed decision making.

enable the measurement of information systems control performance in meeting business objectives.
- Assess and recommend tools to automate information systems control processes.
- Provide documentation and training to ensure information systems controls are effectively performed.
- Ensure all controls are assigned control owners to establish accountability.
- Establish control criteria to enable control life cycle management

## Further Information:

For More information, or to book your course, please call us on 353-1-814 8200

info@globalknowledge.ie

www.globalknowledge.com/en-ie/

Global Knowledge, 3rd Floor Jervis House, Millennium Walkway, Dublin 1