PURPLE GRIFFON
The IT Service Management Training & Consultancy Specialists



| | |
|---|---|
| **Course Title**: Certified In Risk & Information Systems Control (CRISC) | **Course Duration**: 4.0 Days |
| **Exam**: Included | **Exam Type**: Proctored Exam |
| **Qualification**: ISACA's Certified In Risk & Information Systems Control (CRISC) Certification | |

## Course Syllabus

Our Certified In Risk & Information Systems Control (CRISC) training course will cover the following modules:

Module 1: IT Risk Identification

- Collect and review information, including existing documentation, regarding the organisation's internal and external business and IT environments to identify potential or realised impacts of IT risk to the organisation's business objectives and operations.
- Identify potential threats and vulnerabilities to the organisation's people, processes and technology to enable IT risk analysis.
- Develop a comprehensive set of IT risk scenarios based on available information to determine the potential impact to business objectives and operations.
- Identify key stakeholders for IT risk scenarios to help establish accountability.
- Establish an IT risk register to help ensure that identified IT risk scenarios are accounted for and incorporated into the enterprise-wide risk profile.
- Identify risk appetite and tolerance defined by senior leadership and key stakeholders to ensure alignment with business objectives.
- Collaborate in the development of a risk awareness program, and conduct training to ensure that stakeholders understand risk and to promote a risk-aware culture.

Module 2: IT Risk Assessment

- Analyse risk scenarios based on organisational criteria (e.g., organisational structure, policies, standards, technology, architecture, controls) to determine the likelihood and impact of an identified risk.
- Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation.
- Review the results of risk and control analysis to assess any gaps between current and desired states of the IT risk environment.
- Ensure that risk ownership is assigned at the appropriate level to establish clear lines of accountability.
- Communicate the results of risk assessments to senior management and appropriate stakeholders to enable risk-based decision making.
- Update the risk register with the results of the risk assessment.

Module 3: Risk Response and Mitigation

- Consult with risk owners to select and align recommended risk responses with business objectives and enable informed risk decisions.
- Consult with, or assist, risk owners on the development of risk action plans to ensure that plans include key elements (e.g., response, cost, target date).
- Consult on the design and implementation or adjustment of mitigating controls to ensure that the risk is managed to an acceptable level.
- Ensure that control ownership is assigned to establish clear lines of accountability.

- Assist control owners in developing control procedures and documentation to enable efficient and effective control execution.
- Update the risk register to reflect changes in risk and management's risk response.
- Validate that risk responses have been executed according to the risk action plans.

Module 4: Risk and Control Monitoring and Reporting

- Define and establish key risk indicators (KRIs) and thresholds based on available data, to enable monitoring of changes in risk.
- Monitor and analyse key risk indicators (KRIs) to identify changes or trends in the IT risk profile.
- Report on changes or trends related to the IT risk profile to assist management and relevant stakeholders in decision making.
- Facilitate the identification of metrics and key performance indicators (KPIs) to enable the measurement of control performance.
- Monitor and analyse key performance indicators (KPIs) to identify changes or trends related to the control environment and determine the efficiency and effectiveness of controls.
- Review the results of control assessments to determine the effectiveness of the control environment.
- Report on the performance of, changes to, or trends in the overall risk profile and control environment to relevant stakeholders to enable decision making.

## Course Overview

Over 17,000 professionals are now Certified in Risk and Information Systems Control (CRISC) following the introduction of this certification by ISACA in 2010.

Professional qualifications such as CRISC are associated with higher earning potential and enhanced career development opportunities. With a growing demand for professionals with risk and control skills, it is a great time for you to gain a globally recognised certification in this field.

Our four-day Certified In Risk & Information Systems Control (CRISC) training course will help you to understand business risk, and have the technical knowledge to implement appropriate IS controls.

## Course Learning Outcomes

Our Certified In Risk & Information Systems Control (CRISC) training course will:

- Prepare for and pass the Certified Risk and Information System Controls (CRISC) exam.
- Identify the universe of IT risk to contribute to the execution of the IT risk management strategy.
- Analyse and evaluate IT risk to determine the likelihood and impact on business objectives.
- Determine risk response options and evaluate their efficiency and effectiveness to manage risk.
- Continuously monitor and report on IT risk and controls.

## Audience

Our Certified In Risk & Information Systems Control (CRISC) training course is suitable for:

- IT Professionals
- Risk Professionals
- Compliance Professionals
- Project Managers
- Control Professionals
- Business Analysts

## Entry-Level Requirements

Our Certified In Risk & Information Systems Control (CRISC) training course requires attendees to have a minimum of three years experience in the fields of risk management and IS control, per ISACA's requirements.

## Recommended Reading

It is recommended that you purchase a copy of the 'CRISC Review Manual (6th Edition)' as it is essential for anyone attempting to take the Certified In Risk & Information Systems Control (CRISC) examination.

## What's Included

Our Certified In Risk & Information Systems Control (CRISC) training course includes the following:

- 4-day instructor-led training course
- Official ISACA curriculum
- ISACA Exam Voucher included
- One-on-one after-course instructor coaching
- Pre-reading
- Course Manuel
- Quizzes
- Exercises

## Exam Information

**Certified In Risk & Information Systems Control (CRISC) Examination:**

- Duration: 4 hours
- Format: Multiple Choice
- Number of questions: 150
- Pass Mark: 450

## What's Next

Our Certified Information Systems certificates have emerged as key qualifications for Security Professionals. More and more organisations are demanding experienced Information Security Professionals with the qualifications to prove that you can protect their valuable information and assets. It is the ideal time to achieve and maintain up to date qualifications. Purple Griffon currently offer the following Certified Information Systems classroom-based training courses:

- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISSP)
- BCS Certificate In Information Security Management Principles (CISMP)

## Additional Information

If you successfully pass the examination, you will be awarded the Certified In Risk & Information Systems Control (CRISC) Qualification.