Certified in Risk and InformationSystems Control (CRISC)

Introduction

Certified in Risk and Information Systems Control (CRISC) certification is an ideal credential for mid-career professionals who perform various roles in enterprise risk management and control.

It is developed by one of the globally renowned certification body ISACA to upscale your career in IT.

Moreover, this certification course prepares the candidate for dealing with real-world threats with relevant tools to assess, govern, and mitigate risk.

After qualifying this certification, a professional can be hired as a senior IT auditor, security engineer architect, IT security analyst, or information assurance program manager.

Course Highlights

This course teaches you about core aspects such as:

- Risk and Information Systems Control
- Understanding enterprise risk
- Plan, execute, scrutinize, and retain information systems controls.
- Risk: identification, evaluation, assessment, response, and monitoring
- IS control design and execution
- IS control maintenance and monitoring

Course Outline

MODULE 1: Risk Identification

- Risk Identification Objectives
- Risk Identification Overview
- Concepts of IT Risk
- Risk Management Standards
- Risk Identification Frameworks
- Assets
- Threats
- Vulnerabilities
- Elements of Risk
- Penetration Testing
- COBIT 5
- ISO
- Risk Scenarios
- Communicating Risk
- Risk Awareness
- Organizational Structures and Culture
- Risk within the Enterprise
- Compliance
- Principles of Risk
- Conclusion

MODULE 2: Risk Assessment

- Risk Assessment Objectives
- Risk Assessment Overview
- Risk Assessment Techniques
- Risk Assessment Analysis
- Methodologies
- Control Assessment
- Risk Evaluation and Impact Assessment
- Risk and Control Analysis
- Third-Party Management
- System Development Lifecycle
- Developing Technologies
- Enterprise Architecture
- Conclusion

MODULE 3: Risk Response and Mitigation

- Risk Response and Mitigation Objectives
- Risk Response and Mitigation Overview
- Risk Response Options
- Response Analysis
- Risk Response Plans
- Control Objectives and Practices
- Control Ownership
- Systems Control Design Implementation
- Control and Countermeasures
- Business Continuity
- Disaster Recovery
- Risk Accountability
- Inherent and Residual Risk
- Conclusion

MODULE 4: Risk and Control Monitoring and Reporting

- Risk and Control Monitoring and Reporting Objectives
- Risk and Control Monitoring and Reporting Overview
- Key Risk Indicators (KRIs)
- Data Collection
- Monitoring Controls
- Control Assessments
- Penetration Testing
- Vulnerability Assessments
- Third-Party Assurance
- Maturity Model Assessment
- Techniques for Improvement
- Capability Maturity Model
- IT Risk Profile
- Conclusion

Prerequisites

The course itself has no prerequisites, but you should be familiar with the CRISC job practice domains. To receive CRISC certification, you must meet the work experience requirements of 3 years of experience across at least 2 of the four CRISC domains, some of which must be in either Domain 1 or 2. The four domains are as follows:

- IT Risk Identification
- IT Risk Assessment
- Risk Response and Mitigation
- Risk and Control Monitoring and Reporting

Target Audience

Anyone who manages IT risk and information security controls within their job role and would like to prepare for the CRISC exam.

Duration

- 40 hours certification course