Certified in Risk and Information System Controls (CRISC)

Course Duration: 4 Days

Course Overview

The CRISC 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 6th 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.

Target Audience

This course is intended for:

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

Prerequisites

There are no prerequisites for taking the CRISC course or the CRISC exam; however, in-order-to apply for the CRISC certification, the candidate must meet the following requirements a determined by ISACA:

- Three (3) years of work experience managing IT risk by designing and implementing IS controls, including experience 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

Course Objectives

On completion of this program, participants will be able to:

- Identify risks
- ssess current and potential risks
- Respond and Mitigate risks
- Ensure risk and control monitoring as risk reporting
- An understanding of the format and structure of the CRISC certification exam
- A knowledge of the various topics and technical areas covered by the exam
- Practice with specific strategies, tips and techniques for taking and passing the exam

Course Content

Domain 1 – Governance

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

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 Mitigation

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

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