Certified in Risk and Information Systems Control (CRISC) – Exam Preparation

ME197

Course Overview:

This comprehensive 5-day training program is tailored for professionals seeking to attain the globally recognized CRISC (Certified in Risk and Information Systems Control) certification issued by ISACA. The course equips participants with in-depth knowledge of the four CRISC domains: Governance, IT Risk Assessment, Risk Response and Reporting, and Information Technology and Security. It is designed to strengthen participants' ability to identify, assess, and manage IT risks while establishing effective controls. Practical examples, case discussions, and exam-focused reviews are incorporated to enhance understanding and ensure readiness for the certification exam.

Course Objective:

By the end of this program, participants will be able to:

1. Understand and apply ISACA's CRISC Job Practice Domains.
2. Assess IT-related risks using structured methodologies.
3. Design and implement effective risk response strategies.
4. Align risk management practices with organizational governance.
5. Prepare comprehensively for the CRISC certification exam through simulated questions and scenarios.

Course Outline:

Day 1: CRISC Overview & Domain 1 – Governance

1. Introduction to CRISC and Exam Structure ISACA framework and certification processExam domains, format, and preparation tips
2. IT Governance Fundamentals Risk management frameworksCorporate governance and IT alignment
3. Strategic Alignment Integrating IT strategy with business objectivesDefining roles, responsibilities, and risk culture
4. Risk Appetite and Tolerance Risk appetite frameworksCommunicating acceptable risk

Day 2: CRISC Domain 2 – IT Risk Assessment (Part 1)

1. Identifying IT Risk Internal and external risk sourcesTools for risk identification
2. Risk Scenario Development Crafting risk scenarios from business functionsImpact analysis and relevance mapping
3. Emerging Risk Management Recognizing evolving threatsAdapting risk assessments dynamically

Day 3: CRISC Domain 2 – IT Risk Assessment (Part 2)

1. Risk Analysis and Evaluation Qualitative vs. quantitative risk analysisRisk matrix, heat maps, and decision-making tools
2. Risk Prioritization Criteria for ranking risksAligning with business priorities
3. Risk Documentation Best practices for reporting and trackingRisk register creation

Day 4: CRISC Domain 3 – Risk Response and Reporting

1. Risk Response Planning Response strategies: avoid, reduce, transfer, acceptDesigning mitigation controls
2. Monitoring and Key Risk Indicators Continuous control monitoringKey metrics for risk and control performance

Training Language:

English

Training Methodology:

The course combines various teaching methods, including instructor-led presentations, group discussions, case study analyses, and assessments through quizzes and a final exam to engage participants and ensure they understand and retain the material.

Venue | Date | Fees

Dubai | 22-06-2025 | 6,843 USD

3. Risk Communication and Escalation Stakeholder reportingRisk dashboards and escalation protocols

Day 5: CRISC Domain 4 – IT and Security + Exam Preparation

1. IT Operations and Information Security IT infrastructure managementConfidentiality, integrity, and availability (CIA)
2. Incident Response & Business Continuity Disaster recovery planningIncident classification and escalation
3. Mock Exam and Final Review Sample questions with rationaleExam strategies and final Q&ATips for certification application and maintenance

Who Should Attend:

-IT Risk Managers
-Systems Control Professionals
-Project Managers
-Compliance Officers
-Business Analysts
-Information Security Professionals