CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL

CRISC

Duration: 4 days; Instructor-led

OVERVIEW

The only globally accepted IT risk management certification for professionals with three or more years of experience.

This credential demonstrates expertise in identifying and managing enterprise IT risk and implementing and maintaining information systems controls. CRISC can enhance your IT team's credibility with stakeholders and clients.

In this course, you'll cover all four domains of the Certified in Risk and Information Systems Control (CRISC) exam and gain the knowledge and concepts required to obtain CRISC certification. Since its inception in 2010, the CRISC certification is for IT and business professionals who identify and manage risks through the development, implementation, and maintenance of appropriate information systems (IS) controls.

OBJECTIVES

Students will master the four CRISC domains:
- Governance
- IT Risk Assessment
- Risk Response and Reporting
- Information Technology and Security

PREREQUISITES

IT risk management professionals with at least 3 years of relevant professional work experience in IT risk and information systems control.

AUDIENCE

The CRISC certification is designed for:
- IT Managers
- IT Risk Analysts
- IT Consultants
- IT Risk/Security Advisory Managers
- IT Compliance Managers
- IT Risk Assessment Specialists

COURSE CONTENTS

Module 1:   Governance
- Risk Assessment Concepts, Standards and Frameworks
- Organizational Strategy, Goals and Objectives
- Organizational Structure, Roles and Responsibilities
- Organizational Culture and Assets
- Policies, Standards and Business Processes
- Enterprise Risk Management, Risk Management Frameworks and Three Lines of Defense
- Risk Profile, Risk Appetite and Risk Tolerance
- Navigating Professional Ethics of Risk Management and Requirements in Laws, Regulations and Controls

Module 2:   IT Risk Assessment
- Risk Events, Threat Modeling and Threat Landscape
- Vulnerability and Control Deficiency Analysis
- Risk Scenario Development
- Risk Register
- Risk Analysis Methodologies
- Business Impact Analysis
- Inherent, Residual and Current Risk

Module 3:   Risk Response and Reporting
- Risk Treatment/Risk Response Options
- Risk and Control Ownership
- Managing Risk from Processes, Third Parties and Emerging Sources
- Control Types, Standards and Frameworks
- Control Design, Selection and Analysis
- Control Implementation, Testing and Effectiveness
- Risk Treatment Plans
- Data Collection, Aggregation, Analysis and Validation
- Risk and Control Monitoring and Reporting Techniques
- Performance, Risk and Control Metrics

Module 4:   Information Technology and Security
- Enterprise Architecture
- IT Operations Management
- Project Management
- Disaster Recovery Management
- Data Life Cycle Management
- System Development Life Cycle
- Emerging Technologies
- Information Security Concepts, Frameworks, Standards and Awareness Training
- Business Continuity Management
- Data Privacy and Protection Principles