CRISC

Overview

The CRISC (Certified in Risk and Information Systems Control) course is designed for IT and business professionals who identify and manage risks through the development, implementation, and maintenance of Information Systems Controls. Learners gain expertise in the governance and application of risk management strategies to enhance the value of their organization's IT and business systems.Domain 1 focuses on Governance, covering strategic alignment and understanding the complex interplay between business goals and IT risk. Domain 2 dives into IT Risk Assessment, teaching learners to identify and evaluate risk to provide effective mitigation strategies. Domain 3 outlines Risk Response and Reporting, where students learn to respond and communicate risk. Finally, Domain 4 emphasizes Information Technology and Security, ensuring learners are well-versed in essential tech and security principles.By mastering these domains, participants enhance their strategic acumen, risk assessment proficiencies, response planning, and reporting abilities, making them valuable assets in an organization's effort to manage IT risk effectively. This course is essential for professionals seeking to bolster their credentials and organizations aiming to ensure robust risk management practices.

Audience Profile

The CRISC course equips professionals with skills in IT risk management, governance, and control monitoring, pivotal for organizational security and compliance.

- IT Risk Managers
- Information Security Analysts
- Compliance Officers
- IT Auditors
- Chief Information Security Officers (CISOs)
- Governance, Risk, and Compliance (GRC) Professionals
- IT Consultants specializing in risk and security
- Cybersecurity Professionals
- IT Control Professionals
- Chief Compliance Officers
- Enterprise Risk Management Consultants
- IT Project Managers
- Data Protection Officers
- Network Security Managers
- IT Directors and Managers
- Security Architects and Engineers
- Business Analysts involved in IT projects
- IT Professionals aiming for a career in Risk and Information Systems Control

Course Syllabus

DOMAIN 1—Governance 26%

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 20%

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 Reporting 32%

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 22%

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