CRISC CERTIFICATION

Content

DOMAIN 1—Governance 26%

Organizational Governance

- Organizational Strategy, Goals, and Objectives
- Organizational Structure, Roles, and Responsibilities
- Organizational Culture
- Policies and Standards
- Business Processes
- Organizational Assets

Risk Governance

- 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

- 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

- 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

- 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

- Control Types, Standards, and Frameworks
- Control Design, Selection, and Analysis
- Control Implementation
- Control Testing and Effectiveness Evaluation

Risk Monitoring and Reporting

- 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

- 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

- Information Security Concepts, Frameworks, and Standards
- Information Security Awareness Training
- Business Continuity Management
- Data Privacy and Data Protection Principles