

CRISC Day wise TOC

Day 1:

Domain 1: IT risk Identification

- Risk capacity, risk appetite, and risk tolerance
 - Risk culture and communication
 - Elements of risk
 - Information security risk concepts and principles
 - The IT risk strategy of the business
 - IT concepts and areas of concern for the risk practitioner
 - Methods of risk identification
 - IT risk scenarios
 - Ownership and accountability
 - The IT risk register
 - RISK awareness
-
-

Day 2:

Domain 2: IT Risk Assessment

- Risk assessment techniques
 - Analyzing risk scenarios
 - Current state of controls
 - Changes in the risk environment
 - Project and program management
 - Risk and controls analysis
 - Risk analysis methodologies
 - Risk ranking
 - Documenting risk assessment
-
-

Day 3:

Domain 3: Risk Response and Mitigation

- Aligning risk response with business objectives
- Risk response options
- Analysis techniques
- Vulnerabilities associated with new controls
- Developing a risk action plan
- Business process review tools and techniques
- Control design and implementation
- Control monitoring and effectiveness
- Type of risk
- Control activities, objectives, practices and metrics

- Systems control design and implementation
 - Impact of emerging technologies on design and implementation of controls
 - Control ownership
 - Risk management procedures and documentation
-
-

Day 4:

Domain 4: Risk and Control Monitoring and Reporting

- Key risk indicators
 - Key performance Indicators
 - Data collection and extraction tools and techniques
 - Monitoring controls
 - Control assessment types
 - Results of control assessment
 - Change to the IT risk profile
-
-

Day 5:

- Exam Preparation