SC240-EN ISACA CRISC Preparation

Kurzbeschreibung:

CRISC (Certified in Risk and Information Systems Control) is a globally recognised management-oriented certification that prepares IT specialists for the unique challenges of IT and enterprise risk management and positions them as strategic partners for companies. The CRISC certification demonstrates your qualification as an expert in the identification and assessment of IT risks in the organisation and in the implementation and monitoring of information systems controls.

The workshop **SC240-EN ISACA CRISC Preparation** prepares you intensively for the ISACA exam to obtain the CRISC certification. The fee-based exam consists of 150 questions that must be completed within four hours. The exam can be taken online or at one of the authorised PSI test centres.

Zielgruppe:

The workshop **SC240-EN ISACA CRISC Preparation** is designed for those experienced in the management of IT risk and the design, implementation, monitoring and maintenance of IS controls.

- IT compliance managers
- IT/IS Auditors/Consultants
- Security manager/architects
- Risk manager and consultant

Voraussetzungen:

The following requirements must be met in order to obtain CRISC certification:

- Passing the CRISC Exam
- Adhere to ISACA Code of Professional Ethics
- Three (3) or more years of experience in IT risk management and IS control
- Verification of Work Experience

Sonstiges:

Dauer: 4 Tage

Preis: 2790 Euro plus Mwst.

Ziele:

This workshop **SC240-EN ISACA CISA Preparation** prepares you intensively for the ISACA exam to obtain the CRISC certification.

Inhalte/Agenda:

- ♦ **Domain 1: Governance (26%)**
  - ♦ ◊ Organizational Governance
    - ◊ · Strategy, Goals, and Objectives
    - · Organizational Structure, Roles, and Responsibilities
    - · Organizational Culture and Ethics
    - · Policies and Standards
    - · Business Processes and Resilience
    - · Organizational Asset Management
  - ◊ Risk Governance
    - ◊ · Enterprise Risk Management
    - · Lines of Defense
    - · Risk Profile
    - · Risk Appetite and Risk Tolerance
    - · Risk Frameworks, Legal, Regulatory, and Contractual Requirements
- ♦ ♦ ◊ .
- ♦ **Domain 2: Risk Assessment (22%)**
  - ♦ ◊ Risk Identification
    - ◊ · Risk Events
    - · Threat Modeling and Threat Landscape
    - · Vulnerability Management
    - · Risk Scenario Development and Evaluation
  - ◊ Risk Analysis
    - ◊ · Risk Assessment Concepts and Standards
    - · Business Impact Analysis (BIA)
    - · Risk Register
    - · Risk Analysis Methodologies
    - · Inherent, Residual, and Current Risk

- ♦ **Domain 3: Risk Response and Reporting (32%)**
  - ♦ ◊ Risk Response
    - ◊ · Risk Response Options
    - · Risk and Control Ownership
    - · Vendor/Supply Chain Risk Management
    - · Issues, Findings, Exceptions, and Exemptions Management
  - ◊ Control Design and Implementation
    - ◊ · Control Frameworks, Types, and Standards
    - · Control Design, Selection, Implementation, and Analysis
    - · Control Testing Methodologies
  - ◊ Risk Monitoring and Reporting
    - ◊ · Risk Action Plans
    - · Data Collection, Aggregation, Analysis, and Validation
    - · Risk and Control Metrics
    - · Risk and Control Monitoring and Reporting Technique
    - · Monitoring and Reporting of Emerging Risks
- ♦ ♦ ◊ .
- ♦ **Domain 4: Technology and Security (20%)**
  - ♦ ◊ Technology Principles
    - ◊ · Technology Roadmaps and Enterprise Architecture (EA)
    - · Operations Management
    - · System Development Life Cycle (SDLC)
    - · Data Lifecycle Management
    - · Portfolio and Project Management
    - · Technology Resilience and Disaster Response/Recovery
    - · Emerging Technologies
  - ◊ Information Security Principles
    - ◊ · Security Concepts, Frameworks, and Standards
    - · Security/Risk Awareness and Training
    - · Data Privacy and Data Protection Principles
  - ♦ ◊ .