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: 3 Tage

Preis: 2390 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%)**
  - ♦ ◊ Organisation management
    - ◊ · Organizational Strategy, Goals and Objectives
    - · Organizational Structure, Roles and Responsibilities
    - · Organizational Culture and Assets
    - · Policies, Standards and Business Process Review
  - ◊ Risk Governance
    - ◊ · Enterprise Risk Management, Risk Management
    - · Frameworks and Three Lines of Defense
    - · Risk Profile
    - · Risk Appetite and Risk Tolerance
    - · Professional Ethics, Laws, Regulations and Contracts

- ♦ **Domain 2: IT Risk Assessment (20%)**
  - ♦ ◊ Identify Risk Events
    - ◊ · Risk Events
    - · Threat Modeling and Threat Landscape
    - · Vulnerability and Control Deficiency Analysis
    - · Risk Scenario Development
  - ◊ Risk Assessment and Analysis
    - ◊ · 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
    - · Managing Risk from Processes, Third Parties and Emergent Sources
  - ◊ Control Design and Implementation
    - ◊ · Control Types, Standards and Frameworks
    - · Control Design, Selection and Analysis
    - · Control Implementation, Testing and Effectiveness Evaluation
  - ◊ Risk Monitoring and Reporting Overview
    - ◊ · Risk Treatment Plans
    - · Data Collection, Aggregation, Analysis and Validation
    - · Risk and Control Monitoring and Reporting Techniques
    - · Performance, Risk and Control Metrics

- ♦ **Domain 4: Information Technology and Security (22%)**
  - ♦ ◊ Information Technology Principles
    - ◊ · Enterprise Architecture
    - · IT Operations Management
    - · Project Management
    - · Disaster-Recovery-Management (DRM)
    - · Data Life Cycle Management
    - · System Development Life Cycle
    - · Emerging Technologies
  - ◊ Information Security Principles
    - ◊ · Information Security Frameworks and Standards
    - · Information Security Awareness Training
    - · Business Continuity Management
    - · Data Privacy and Data Protection Principles
  - ♦ ◊