# *SC220-EN ISACA CISM Preparation*

**Kurzbeschreibung:**

The **SC220-EN ISACA CISM Preparation** workshop is aimed at IT professionals with technical expertise and experience in the areas of IS/IT security and control. The CISM certification proves your qualification in the planning, implementation, control and monitoring of information security concepts and is highly recognised worldwide.

This workshop **SC220-EN ISACA CISM Preparation** prepares you intensively for the content and procedure of the ISACA CISM (Certified Information Security Manager) exam. 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 **SC220-EN ISACA CISM Preparation** is aimed at information security experts who have acquired sound professional experience through extensive work in the field of information security. Professionals with five or more years of professional experience in the active organisation of corporate information security will feel addressed by the opportunity to obtain this certification.

The job titles include:

- CISO
- CSO
- IT Administrators
- Security experts
- Risk managers and consultants

**Voraussetzungen:**

To become CISM certified requires:

- Passing the CISM Exam
- Adhere to ISACA Code of Professional Ethics
- 5 years of experience in the Information Security Management field
- Verification of Work Experience

**Sonstiges:**

**Dauer:** 4 Tage

**Preis:** 2790 Euro plus Mwst.

**Ziele:**

This workshop **SC220-EN ISACA CISM Preparation** prepares you intensively for the ISACA exam to obtain

the CISM certification.

**Inhalte/Agenda:**

- ♦ **Domain 1: Information Security Governance (17%)**
- ♦ ◊ Enterprise Governance Overview
  ◊ Organizational Culture, Structures, Roles and Responsibilities
  ◊ Legal, Regulatory and Contractual Requirements
  ◊ Information Security Strategy
  ◊ Information Governance Frameworks and Standards
  ◊ Strategic Planning

- ♦ **Domain 2: Information Security Risk Management (20%)**
- ♦ ◊ Risk and Threat Landscape
  ◊ Vulnerability and Control Deficiency Analysis
  ◊ Risk Assessment, Evaluation and Analysis
  ◊ Information Risk Response
  ◊ Risk Monitoring, Reporting and Communication

- ♦ **Domain 3: Information Security Program Development and Management (33%)**
- ♦ ◊ IS Program Development and Resources
  ◊ IS Standards and Frameworks
  ◊ Defining an IS Program Road Map
  ◊ IS Program Metrics
  ◊ IS Program Management
  ◊ IS Awareness and Training
  ◊ Integrating the Security Program with IT Operations
  ◊ Program Communications, Reporting and Performance Management

- ♦ **Domain 4: Information Security Incident Management (30%)**
- ♦ ◊ Incident Management and Incident Response Overview
  ◊ Incident Management and Response Plans
  ◊ Incident Classification/Categorization
  ◊ Incident Management Operations, Tools and Technologies
  ◊ Incident Investigation, Evaluation, Containment and Communication
  ◊ Incident Eradication, Recovery and Review
  ◊ Business Impact and Continuity
  ◊ Disaster Recovery Planning
  ◊ Training, Testing and Evaluation
- ♦ ◊