# *SC230-EN ISACA CISA Preparation*

**Kurzbeschreibung:**

**Certified Information Systems Auditor (CISA)** is recognised worldwide as the gold standard for those who audit, control, monitor and evaluate a company's IT and business systems. CISA is often a mandatory qualification for employment as an IT auditor. The holder of the CISA title has a proven ability to apply a risk-based approach to the planning, execution and reporting of audit engagements.

This workshop **SC230-EN ISACA CISA Preparation** prepares you intensively for the ISACA exam to obtain the CISA certification. The paid exam consists of 150 questions that must be completed within four hours. The questions relate to five areas that ISACA has identified as part of its current analysis of CISA professional practice. The exam can be taken online or at one of the authorised PSI test centres.

**Zielgruppe:**

Do you have a desire to improve your professional performance or advance to a new position? Obtaining the title of CISA will set you apart from other candidates and give you a competitive edge. The workshop **SC230-EN ISACA CISA Preparation** is aimed at anyone who wants to successfully pass the CISA certification.

- 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 CISA certification:

Passing the CISA Exam
Adhere to ISACA Code of Professional Ethics
5 years of information systems auditing, control or security work experience
Verification of Work Experience

**Sonstiges:**

**Dauer:** 4 Tage

**Preis:** 2790 Euro plus Mwst.

**Ziele:**

This workshop **SC230-EN ISACA CISA Preparation** prepares you intensively for the ISACA exam to obtain the CISA certification.

**Inhalte/Agenda:**

- ♦ **Domain 1: Information Systems Auditing Process (18%)**
  - ♦ ◊ Planning
    - ◊ · IS Audit Standards, Guidelines, Functions, and Codes of Ethics
    - · Types of Audits, Assessments, and Reviews
    - · Risk-based Audit Planning
    - · Types of Controls and Considerations
  - ◊ Execution
    - ◊ · Audit Project Management
    - · Audit Testing and Sampling Methodology
    - · Audit Evidence Collection Techniques
    - · Data Analytics
    - · Reporting and Communication Techniques
    - · Quality Assurance and Improvement of the Audit Process

- ♦ **Domain 2: Governance and Management of IT (18%)**
  - ♦ ◊ IT Governance
    - ◊ · Laws, Regulations, and Industry Standards
    - · Organizational Structure, IT Governance, and IT Strategy
    - · IT Policies, Standards, Procedures, and Guidelines
    - · Enterprise Architecture and Considerations
    - · Enterprise Architecture
    - · Enterprise Risk Management (ERM)
    - · Data Privacy Program and Principles
    - · Data Governance and Classification
  - ◊ IT Management
    - ◊ · IT Resource Management
    - · IT Vendor Management
    - · IT Performance Monitoring and Reporting
    - · Quality Assurance and Quality Management of IT

- ♦ **Domain 3: Information Systems Acquisition Development and Implentation (12%)**
  - ♦ ◊ Information Systems Acquisition and Development
    - ◊ · Project Governance and Management
    - · Business Case and Feasibility Analysis
    - · System Development Methodologies
    - · Control Identification and Design
  - ◊ Information System Implementation
    - ◊ · System Readiness and Implementation Testing
    - · Implementation Configuration and Release Management
    - · System Migration, Infrastructure Deployment, and Data Conversion
    - · Postimplementation Review

- ♦ **Domain 4: Information Systems Operations and Business Resilience (26%)**
  - ♦ ◊ Information System Operations
    - ◊ · IT Components
    - · IT Asset Management
    - · Job Scheduling and Production Process Automation
    - · System Interfaces
    - · End-user Computing and Shadow IT
    - · Systems Availability and Capacity Management
    - · Problem and Incident Management
    - · IT Change, Configuration, and Patch Management
    - · Operational Log Management
    - · IT Service Level Management
    - · Database Management
  - ◊ Business Resilience
    - ◊ · Business Impact Analysis
    - · System and Operational Resilience
    - · Data Backup, Storage, and Restoration
    - · Business Continuity Plan
    - · Disaster Recovery Plans

- ♦ ◊ ·

- **Domain 5: Protection of Information Assets (26%)**
  - Information Asset Security and Control
    - Information Asset Security Policies, Frameworks, Standards, and Guidelines
    - Physical and Environmental Controls
    - Identity and Access Management
    - Physical Access and Environmental Controls
    - Identity and Access Management
    - Network and End-Point Security
    - Data Loss Prevention
    - Data Encryption
    - Public Key Infrastructure (PKI)
    - Cloud and Virtualized Environments
    - Mobile, Wireless, and Internet-of-Things Devices
  - Security Event Management
    - Security Awareness Training and Programs
    - Information System Attack Methods and Techniques
    - Security Testing Tools and Techniques
    - Security Monitoring Logs, Tools, and Techniques
    - Security Incident Response Management
    - Evidence Collection and Forensics

- **Practice Questions/Review/CISA Exam Prep**