Certified Information Systems Auditor (CISA) Mastery

22 November – 3 December 2027
Munich (Germany)



Certified Information Systems Auditor (CISA) Mastery

Ref: 321560_141012 **Date:** 22 November – 3 December 2027 **Location:** Munich (Germany) **Fees:** 10600 GBP

Why This Course

As organizations become increasingly dependent on digital systems, the need for robust governance, effective controls, and independent assurance has never been greater. Information Systems Auditors play a critical role in safeguarding assets, managing risk, and ensuring that IT supports business objectives.

This intensive 2-week Certified Information Systems Auditor CISA preparation program provides comprehensive coverage of all exam domains defined by ISACA. The course blends technical knowledge, audit methodology, governance frameworks, and real-world application to equip participants with both the competence to perform high-quality IS audits and the confidence to successfully pass the CISA certification exam.

Through structured lectures, applied case studies, and practical exercises, participants will build a strong foundation across audit, governance, systems development, operations, and information security.

What You'll Learn and Practice

By attending this program, you will:

- Master the five domains of the CISA exam syllabus.
- Plan, execute, and report on IS audits using internationally recognized standards.
- Evaluate IT governance structures and risk management frameworks.
- Assess systems acquisition, development, and implementation controls.
- Review IT operations, business continuity, and disaster recovery practices.
- Examine information security controls across infrastructure, applications, and cloud environments.
- Strengthen exam readiness through practice questions and structured review sessions.

The Program Flow

Day 1: Introduction to IS Auditing

- Overview of CISA certification structure and requirements
- IS audit standards, guidelines, and professional ethics
- Risk-based audit planning
- Audit evidence collection and documentation techniques



Day 2: IT Governance and Management

- IT governance frameworks, including COBIT and ITIL
- Aligning IT strategy with business objectives
- IT resource and portfolio management
- Performance measurement and reporting mechanisms

Day 3: Information Systems Acquisition Part 1

- Project management methodologies
- Feasibility analysis and business case development
- Requirements definition and validation
- Vendor evaluation and contract considerations

Day 4: Information Systems Acquisition Part 2

- System Development Life Cycle SDLC controls
- Agile and DevOps considerations from an audit perspective
- Quality assurance and testing controls
- Change management and configuration management processes

Day 5: Information Systems Implementation

- Implementation planning and control validation
- Data migration and conversion risks
- User acceptance testing UAT
- Post-implementation review practices

Day 6: IS Operations and Maintenance

- IT service management processes
- Capacity planning and performance management
- Incident and problem management
- Patch, configuration, and operational control monitoring

Day 7: Business Continuity and Disaster Recovery

- Business impact analysis BIA
- Disaster recovery planning and strategy selection
- Backup and restoration controls
- Testing and maintaining BC/DR frameworks



Day 8: Information Asset Protection Part 1

- Information security governance structures
- Identity and access management controls
- Network and infrastructure security mechanisms
- Cryptography principles and key management practices

Day 9: Information Asset Protection Part 2

- Application and database security controls
- Cloud and virtualization risk considerations
- Mobile, IoT, and emerging technology risks
- Security monitoring and incident response frameworks

Day 10: CISA Exam Preparation

- Comprehensive review of all five domains
- Practice exam questions with guided analysis
- Exam strategies, time management, and common pitfalls
- Final clarification session and readiness assessment

Individual Impact

- Strong capability to conduct risk-based IS audits aligned with global standards.
- Enhanced expertise in IT governance, systems development controls, and operational risk.
- Improved confidence in evaluating cybersecurity and information protection mechanisms.
- Structured preparation pathway to successfully achieve CISA certification.

Organizational Impact

- Stronger assurance over IT governance and control environments.
- Improved risk identification and mitigation across digital operations.
- Enhanced regulatory compliance and audit readiness.
- Better alignment between IT investments, security, and business objectives.

Training Methodology

- Instructor-led technical sessions aligned with CISA domains.
- Real-world audit scenarios and applied case discussions.
- Practice assessments with performance feedback.
- Structured exam-focused revision and strategy sessions.



Beyond the Course

Participants will leave ready to:

- Perform comprehensive IS audits with confidence and professionalism.
- Evaluate governance, risk, and control frameworks across IT environments.
- Strengthen cybersecurity and operational control oversight.
- Sit for and successfully pass the CISA certification exam.

