Certified Information Systems Auditor (CISA) Training

Course: **00053**
Filter: **Beginner**
Duration: **20 hours**
Category:: **Cyber Security**
Price: **3000,00 €**

About Course

An ISACA CISA (Certified Information Systems Auditor) is recognized as one of the leading authorities in the areas of IS (Information Systems) auditing, control, and information security. This official CISA training course provides in-depth coverage of the five CISA domains covered on the CISA certification exam. These domains include auditing information systems; IT (Information Technology) governance and management of IT; information systems acquisition, development, and implementation; information systems operations, maintenance, and support; and protection of information assets. In addition to meeting ISACA's certification requirements, passing the CISA Certification Exam meets U.S. DoD Directive 8140/8570.01 Technical (IAT) Level-III and CSSP Auditor requirements.

What you'll learn

- Prepare for and pass the Certified Information Systems Auditor (CISA) Exam.
- Develop and implement a risk-based IT audit strategy in compliance with IT audit standards.
- Evaluate the effectiveness of an IT governance structure.
- Ensure that the IT organizational structure and human resources (personnel) management support the organization's strategies and objectives.
- Review the information security policies, standards, and procedures for completeness and alignment with generally accepted practices

Targeted audience

- This ISACA certification prep course is specifically designed for experienced information security professionals who are preparing to take the ISACA CISA exam.

Pre-requisites

- IT professionals must have 5 years or more of IS audit, control, assurance, and security experience.

Curriculum

Module 1: The Process of Auditing Information Systems

- Develop and implement a risk-based IT audit strategy
- Plan specific audits
- Conduct audits in accordance with IT audit standards
- Report audit findings and make recommendations to key stakeholders
- Conduct follow-ups or prepare status reports

Module 2: Governance and Management of IT

- Evaluate the effectiveness of the IT governance
- Evaluate IT organizational structure and human resources (personnel) management
- Evaluate the organization's IT policies, standards, and procedures
- Evaluate the adequacy of the quality management
- Evaluate IT management and monitoring of controls
- Evaluate IT contracting strategies and policies, and contract management
- Evaluate risk management practices
- Evaluate the organization's business continuity plan

Module 3: Information Systems Acquisition, Development, and Implementation

- Evaluate the business case for proposed investments in information
- Evaluate the project management practices and controls

- Conduct reviews to determine whether a project is progressing in accordance with project
- Evaluate controls for information systems
- Evaluate the readiness of information systems for implementation and migration into production
- Conduct post-implementation reviews of systems

Module 4: Information Systems Operations, Maintenance, and Support

- Conduct periodic reviews of information systems
- Evaluate service-level management practices
- Evaluate third-party management practices
- Evaluate data administration practices
- Evaluate the use of capacity and performance monitoring tools and techniques
- Evaluate change, configuration, and release management practices

Module 5: Protection of Information Assets

- Evaluate the information security policies, standards, and procedures
- Evaluate the design, implementation, and monitoring of system and logical security
- Evaluate the design, implementation, and monitoring of physical access and environmental controls
- Evaluate the processes and procedures used to store, retrieve, transport, and dispose of information assets