€TRAINING

CISA Certified Information Systems Auditor

14 - 18 October 2024
Rome (Italy)

CISA Certified Information Systems Auditor

REF: A1677 DATE: 14 - 18 October 2024 Venue: Rome (Italy) - Fee: 5940 Euro

Introduction

The Certified Information Security Auditor CISA certification is a widely recognized credential that relies on the prior expertise of IS professionals to create valued personnel with superior knowledge of information systems auditing, control, and security.

Delegates will learn about the Five Domains of Information Security Auditing during this CISA training course. To pass the CISA exam and use their certification in the workplace, delegates must have a thorough understanding of these domains, which make up the CISA foundations. Each of these domains has a number of subjects that, when taken together, give a thorough overview of the subject area.

Course Objectives

At the end of this course the participants will be able to:

- Get knowledge of the domains:
- The Process of Auditing Information Systems
- Governance & Management of IT
- Information Systems Acquisition, Development, and Implementation
- Information Systems Operations, Maintenance, and Support
- Protection of Information Assets

Targeted Audience

This course is ideal for those looking to advance their careers and learn more about Information Systems Auditing, Control, and Security.

Course Outline

Unit 1: Information Systems Audit Process

- creating a risk-based approach to IT auditing
- preparing particular audits
- auditing in accordance with IS audit standards
- putting risk management and control methods into practice

Unit 2: IT Governance and Management:

- IT governance structure's efficiency
- Organizational design for IT and personnel administration
- IT rules, standards, and processes inside the organization
- Whether the Quality Management System is adequate
- controls for IT management and supervision
- investment in IT resources

- IT contracting tactics and regulations
- Organizational management hazards associated to IT
- techniques for surveillance and assurance
- Business continuity strategy for an organization

Unit 3: Information Systems Acquisition, Development, and Implementation:

- Business case development for IS acquisition, development, maintenance, and retirement
- Controls and procedures for project management
- evaluating the methods used in project management
- controls for the phases of specifications, procurement, development, and testing
- Information Systems Readiness
- Reviewing the Project Plan and Post-implementation System Reviews

Unit 4: Information Systems Operations, Maintenance, and Support:

- Review the organization's goals on a regular basis.
- Service level administration
- techniques used by third parties
- Procedures for end users and operations
- procedure for maintaining information systems
- The integrity and optimization of databases are determined by data administration methods.
- Utilization of monitoring tools and methods for capacity and performance
- Techniques for managing issues and incidents
- Practices in change, configuration, and release management
- Provisions for backup and restoration are adequate.
- In the case of a crisis, an organization's disaster recovery plan

Unit 5: Protection of Information Assets:

- policies, guidelines, and practices for information security
- System and logical security controls design, implementation, and monitoring
- Processes and procedures for designing, executing, and tracking data classification
- Design, implementation, and oversight of environmental and physical access controls
- Information assets' storage, retrieval, transportation, and disposal processes and procedures