CISA: CERTIFIED INFORMATION SYSTEMS AUDITOR

Course Introduction:

Globally recognized, **ISACA's Certified Information Systems Auditor (CISA)** is the gold standard for IT professionals seeking to practice in information security, audit control and assurance. Ideal candidates are able to identify and assess organizational threats and vulnerabilities, assess compliance, and provide guidance and organizational security controls.

CISA-Certified Professionals are able to demonstrate knowledge and skill across the **CISA** job practice areas of auditing, governance and management, acquisition, development and implementation, maintenance and service management, and asset protection.

An **ISACA Certified Information Systems Auditor** is recognized as one of the leading authorities in the areas of IS auditing, control, and information security. This **CISA** training course provides you with in-depth coverage of the five **CISA** domains that are covered on the **CISA** exam. These domains include auditing information systems; IT governance and management; information systems acquisition, development, and implementation; information systems operations, maintenance, and support; and protection of information assets.

What You'll Learn:

- **Prepare for passing 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

Prerequisites:

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

Who should attend?:

Individuals seeking **CISA Certification**.

CISA: CERTIFIED INFORMATION SYSTEMS AUDITOR

Course Outline:

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: IT Governance and Management of IT

- Evaluate the effectiveness of the IT governance structure
- 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 system
- Evaluate IT management and monitoring of controls
- Evaluate IT contracting strategies and policies, and contract management practices
- 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 plans
- 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