

## Certified Information Security Auditor (CISA)

**Length:** 5 Days

**Summary:** This course employs outcome-based delivery that focuses on preparing you with the real-world skills required to pass the certification exams (and to hit the ground running in your career). The goal of our CISA certification course is to equip information professionals with the knowledge and technical skills for proficiency in IS audit, control and security skills.

**Learning Objectives:** Upon successful completion of this course, students will be able to:

- Implement information systems audit services in accordance with information systems audit standards, guidelines, and best practices.
- Evaluate an organization's structure, policies, accountability, mechanisms, and monitoring practices.
- Evaluate information systems acquisition, development, and implementation.
- Evaluate the information systems operations, maintenance, and support of an organization; and evaluate the business continuity and disaster recovery processes used to provide assurance that in the event of a disruption, IT services are maintained.
- Define the protection policies used to promote the confidentiality, integrity, and availability of information assets.

**Audience:** The intended audience for this course is information security and IT professionals, particularly internal auditors, who are interested in earning the CISA certification. The course is also applicable to individuals who are interested in learning about information security audits, controls, and security.

---

## COURSE CONTENT

### The Process of Auditing Information Systems Domain

- Some Organizations, Laws, Standards, and Frameworks
- ISAAS
- From Governance to Procedures
- KGI, CSF, KPI, and KRI
- ALE, RTO, RPO, SDO, MTO, MTD, and AIW
- Risk Appetite, Tolerance, and Capacity
- From Threats to Controls
- Risk Management
- Sampling
- IS Auditor Duties for the Process of Auditing Information Systems Domain

### The Governance and Management of IT Domain

- Security Concepts
- Roles, Responsibilities, and a RACI Matrix
- Human Resources (HR)
- Outsourcing
- Cloud Computing
- Capital Expenditures and Operational Expenditures
- BCP, DRP, and BIA
- Plan Testing
- Enterprise Architecture
- Governance
- Information Security Policy
- Information Technology Management Practices
- IT Organizational Structure Roles and

Responsibilities

- IS Auditor Duties for the Governance and Management of IT Domain

**The Information Systems Acquisition, Development, and Implementation Domain**

- Project Management
- Benefits Realization
- The Software Development Lifecycle (SDLC)
- Software Development
- E-Commerce
- EDI
- Email
- Electronic Money
- Integrated Manufacturing System (IMS)
- Industrial Control Systems (ICS)
- Artificial Intelligence and Expert Systems
- Business Intelligence (BI)
- Decision Support System (DSS)
- Re-Engineering
- Other Business Applications
- Infrastructure
- Managing Change, Configuration, Patches, and Releases
- Application Controls
- IS Auditor Duties for the Information Systems Acquisition, Development, and Implementation Domain

**The Information Systems Operations, Maintenance, and Service Management Domain**

- Information Systems Operations
- Hardware Architecture
- Operating Systems
- Database Management
- Third-Party Software
- Network Infrastructure
- Internet Concepts
- Telecommunications
- IS Auditor Duties for the Information Systems Operations, Maintenance, and Service Management Domain

**The Protection of Information Assets Domain**

- Asset Classification
- Security Awareness and Training
- External Parties
- Computer Crime
- Logical Access
- Remote Connectivity
- Media Handling
- Network Security
- Firewalls
- Intrusion Detection
- Encryption
- Penetration Testing
- Environmental Issues
- Data Leakage Prevention (DLP)
- Physical Access
- IS Auditor Duties for the Protection of Information Assets Domain