

Certified Information Systems Auditor (CISA)  
Certification Training

**Course Agenda**

## **Index**

Domain 01 - Process of Auditing Information Systems

Domain 02 - Governance and Management of IT

Domain 03 - Information Systems Acquisition, Development, and Implementation

Domain 04 - Information Systems Operations, Maintenance, and Support

Domain 05 - Protection of Information Assets

## **Course Curriculum**

### **Domain 1: Information System Auditing Process**

- Planning

IS Audit Standards, Guidelines and Codes of Ethics  
Business Processes  
Types of Controls  
Risk-based Audit Planning  
Types of Audits and Assessments

- Execution

Audit Project Management  
Sampling Methodology  
Audit Evidence Collection Techniques  
Data Analytics  
Reporting and Communication Techniques  
Quality Assurance and Improvement of the Audit Process

### **Domain 2: Governance and Management of IT**

- IT Governance and IT Strategy

IT-related Frameworks  
IT Standards, Policies and Procedures  
Organizational Structure  
Enterprise Architecture  
Enterprise Risk Management  
Maturity Models  
Laws, Regulations and Industry Standards Affecting the Organization

- IT Management

IT Resource Management  
IT Service Provider Acquisition and Management  
IT Performance Monitoring and Reporting  
Quality Assurance and Quality Management of IT

### **Domain 3: Information Systems Acquisition, Development and Implementation**

- Information Systems Acquisition and Development

Project Governance and Management  
Business Case and Feasibility Analysis  
System Development Methodologies  
Control Identification and Design

- Information Systems Implementation

Testing Methodologies  
Configuration and Release Management  
System Migration, Infrastructure Deployment and Data Conversion  
Post-implementation Review

### **Domain 4: IS Operations and Business Resilience**

- Information Systems Operations

Common Technology Components  
IT Asset Management  
Job Scheduling and Production Process Automation  
System Interfaces  
End-user Computing  
Data Governance  
Systems Performance Management  
Problem and Incident Management  
Change, Configuration, Release and Patch Management  
IT Service Level Management  
Database Management

- Business Resilience

Business Impact Analysis  
System Resiliency  
Data Backup, Storage and Restoration  
Business Continuity Plan  
Disaster Recovery Plans

## **Domain 5: Information Asset Security and Control**

- Information Asset Security Frameworks, Standards and Guidelines

Privacy Principles

Physical Access and Environmental Controls

Identity and Access Management

Network and End-point Security

Data Classification

Data Encryption and Encryption-related Techniques

Public Key Infrastructure

Web-based Communication Technologies

Virtualized Environments

Mobile, Wireless and Internet-of-things Devices

- Security Event Management

Security Awareness Training and Programs

Information System Attack Methods and Techniques

Security Testing Tools and Techniques

Security Monitoring Tools and Techniques

Incident Response Management

Evidence Collection and Forensics