Document Generated: 11/15/2026

Learning Style: Online Instructor-Led

Technology: ISACA

Difficulty: Advanced

Course Duration: 4 Days

Certified Information Systems Auditor (CISA)

This comprehensive prep course aims to provide participants with a deep understanding of information systems auditing processes while thoroughly preparing them for the CISA exam. Attendees will learn to evaluate organizational policies, procedures, and infrastructures to ensure that information systems are adequately controlled and aligned with business objectives. The curriculum emphasizes risk management, governance, and the implementation of robust security measures to protect information assets effectively. Additionally, participants will gain exam-focused insights, practice with exam-style questions, and develop the confidence needed to pass the CISA certification exam successfully.

Course Objectives:

- This comprehensive prep course aims to provide participants with a deep understanding of information systems auditing processes while thoroughly

preparing them for the CISA exam. Attendees will learn to evaluate organizational policies, procedures, and infrastructures to ensure that information systems are adequately controlled and aligned with business objectives. The curriculum emphasizes risk management, governance, and the implementation of robust security measures to protect information assets effectively. Additionally, participants will gain exam-focused insights, practice with exam-style questions, and develop the confidence needed to pass the CISA certification exam successfully.

Audience:

- This course is ideal for IT professionals, internal and external auditors, compliance officers, and individuals responsible for ensuring the integrity, confidentiality, and availability of information systems. It's also beneficial for those aspiring to roles in IT auditing, security management, and governance.

Prerequisites:

- No formal prerequisites to take the exam
- To become certified, candidates must have at least 5 years of professional experience in information systems auditing, control, or security (waivers available for up to 3 years based on education or experience)

Course Outline:

Domain 1. Information Systems Auditing Process

Planning

- IS Audit Standards, Guidelines and Codes of Ethics
- Business Proces 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 Organization

Information Systems Implementation

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

Domain 4. Information Systems 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
- Control Identification and DesignOrganization

Business Resilience

- Business Impact Analysis
- System Resiliency

- Data Backup, Storage and Restoration
- Business Continuity Plan
- Disaster Recovery Plans

Protection of Information Assets

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

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