Course Description

General Information:

CISA is the globally recognized gold standard for IS audit, control, and assurance, in demand and valued by leading global brands. It's often a mandatory qualification for employment as an IT auditor. CISA holders have validated ability to apply a risk-based approach to planning, executing and reporting on audit engagements.

There are 150 Questions on the exam which must be completed in 4 hours. It is available online via remote proctoring and at in-person testing centers where available.

The CISA certification is intended for:

Early to mid-career professionals looking to gain recognition and enhanced credibility in interactions with internal and external stakeholders, regulators, and customers. Job roles include:

- IT Audit Directors/Managers/Consultants
- IT and Internal Auditors
- Compliance/Risk/Privacy Directors
- IT Directors/Managers/Consultants

CPE Overview:

To maintain your CISA, you must earn and report a minimum of 120 CPE hours every 3-year reporting cycle and at least 20 hours annually. CISA awards up to 1 hour of CPE for every 1 hour of instructor led training. Online review course earns 28 CPEs and Virtual Instructor-Led Training (VILT) earns 14 CPEs.

Course Duration:

Online Course: Approximately 22 hours

In-person training or VILT: 2-4 days

Course Topics:

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

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

Business Resilience

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

Domain 5: 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
- 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