Course outline

The ISACA CISA certification is mainly targeted to those candidates who want to build their career in IT Audit domain. The ISACA Certified Information Systems Auditor (CISA) exam verifies that the candidate possesses the fundamental knowledge and proven skills in the area of ISACA CISA.

Exam Price ISACA Member $575 (USD)
Exam Price ISACA Nonmember $760 (USD)
Duration 240 mins
Number of Questions 150
Passing Score 450/800

Topic Details Weights

Domain 1 (21%)

INFORMATION SYSTEMS AUDITING PROCESS - Providing audit services in accordance with standards to assist organizations in protecting and controlling information systems. Domain 1 affirms your credibility to offer conclusions on the state of an organization’s IS/IT security, risk and control solutions.

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

B. 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 (21%)

Governance and Management of IT - Domain 2 confirms to stakeholders your abilities to identify critical issues and recommend enterprise-specific practices to support and safeguard the governance of information and related technologies.

A. IT Governance

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

B. 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 (12%)

Information Systems Acquisition, Development and Implementation

A. Information Systems Acquisition and Development

Project Governance and Management

Business Case and Feasibility Analysis

System Development Methodologies

Control Identification and Design

B. Information Systems Implementation

Testing Methodologies

Configuration and Release Management

System Migration, Infrastructure Deployment, and Data Conversion

Post-implementation Review

Domain 4 (23%)

INFORMATION SYSTEMS OPERATIONS AND BUSINESS RESILIENCE -

A. 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

B. Business Resilience

Business Impact Analysis (BIA)

System Resiliency

Data Backup, Storage, and Restoration

Business Continuity Plan (BCP)

Disaster Recovery Plans (DRP)

Domain 5 (27%)

A. 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 (PKI)
Web-Based Communication Techniques
Virtualized Environments
Mobile, Wireless, and Internet-of-Things (IoT) Devices

B. 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