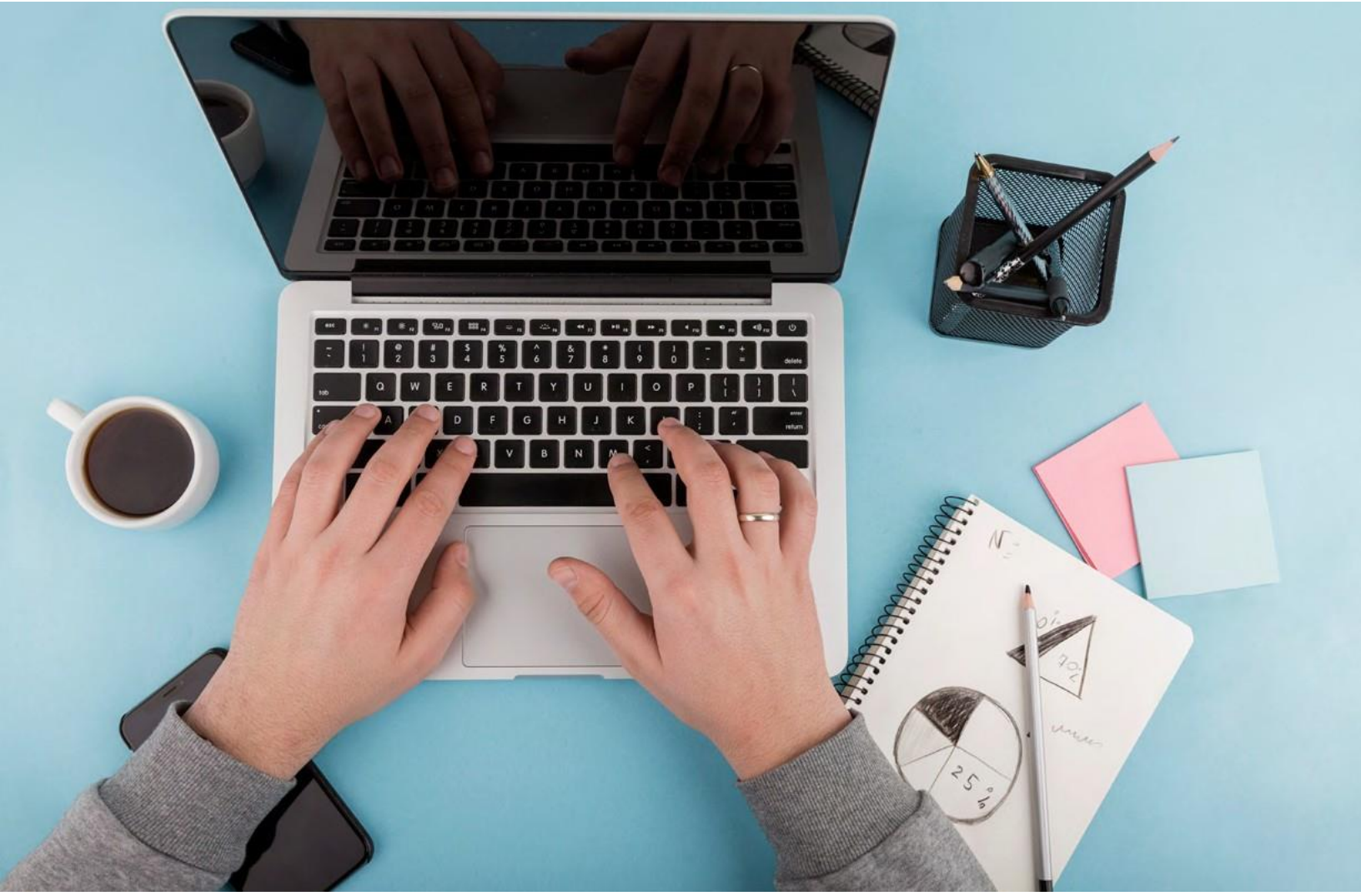

CISA 2024

28th Edition

Certified Information Systems Auditor

Training & Certification

Introduction

CISA is a globally recognized certification meticulously designed for the professionals responsible for monitoring, managing, and protecting an organization's IT and business environment. The latest 28th edition of the CISA certification training course validates the certification holder's skills and expertise to assess vulnerabilities, report compliance issues, and successfully implement IT security controls for an organization.

Why **CISA** with Beyond Boundariez?

Access to
Recorded Sessions

Accredited
Instructors

Whatsapp
Discussion Group

CISA Course Highlights

40-Hrs LIVE
Instructor-led Training

Highly Interactive
and Dynamic Sessions

Learn from
Industry Experts

Post Training
Support

Access to Recorded Sessions

Revisit your lectures, revise your concepts, and retain yourknowledge from anywhere, whenever you want

Extended Post Training

Get extended support even after you finish your training.
We're here for you until you reach your certification goals.

Target Audience

- Individuals who are willing to learn about IS auditing
- Professionals who are auditors or working in an audit environment
- Professionals who are willing to make a career in information systems auditing
- IT Managers
- Security Managers
- System Analysts
- Consultants

CISA Exam Information

Exam Name	CISA 2019	CISA 2024
Launch Date	June 2019	Effective from August 1, 2024
Exam Duration	4 Hours	
Number of Questions	150	
Exam Format	Multiple Choice Questions	
Passing Score	450 out of 800	

CISA Domains 2019 Vs 2024

Domains	2019	2024
Information System AuditingProcess	21%	18%
Governance and Managementof IT	17%	18%
Information Systems Acquisition, Development, andImplementation	12%	12%
Information Systems Operations and BusinessResilience	23%	26%
Protection of InformationAssets	27%	26%

Course Content

Domain 1
Information System Auditing Process (18%)

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
Governance and Management of IT(18%)

A:IT Governance and IT Strategy

- 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

Information Systems Acquisition, Development and Implementation (12%)

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

Information Systems Operations and Business Resilience (26%)

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)

A: Information Asset Security and Controls

- 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