INFOSECTRAIN

# CISA

## Certified Information Systems Auditor

In a World Full of Auditors, be a CISA

### KEY FEATURES

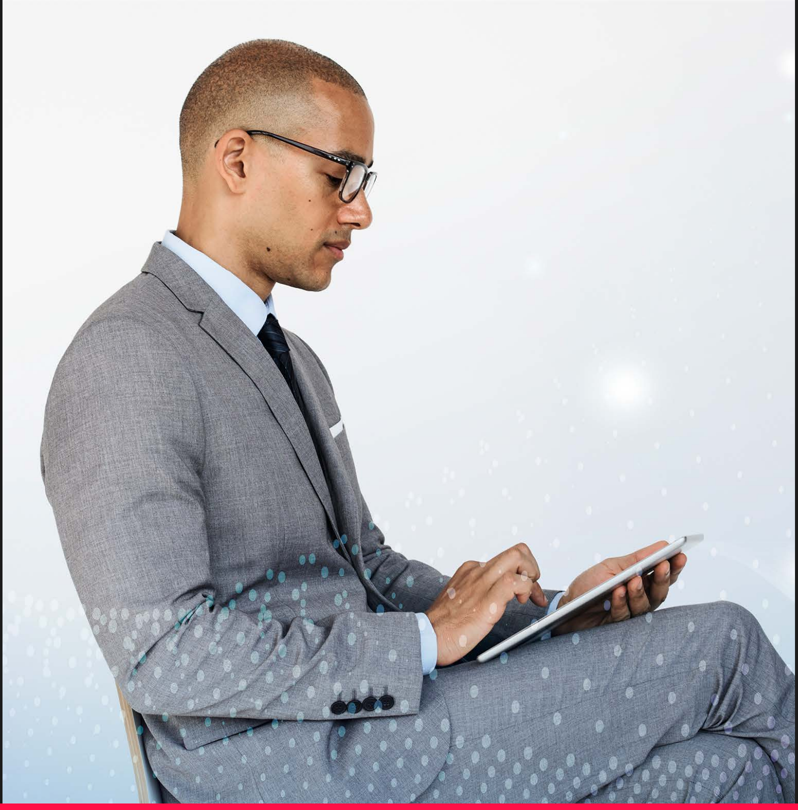
- ISACA Premium Training Partner
- Access to the recorded sessions
- Certified & Experienced Trainers

ISACA ACCREDITED PARTNER CISA

Validate your expertise and get the leverage you need to move up in your career. With ISACA's Certified Information Systems Auditor (CISA) certification, you can do just that. CISA is world-renowned as the standard of achievement for those who audit, control, monitor and assess an organization's information technology and business systems.

# Overview

The CISA is a globally reputed certification for security professionals who audit, monitor, and assess organizations' information systems and business operations. The certification showcases the candidate's auditing experience, knowledge, and skills to evaluate vulnerabilities, report on compliance, and institute controls within the enterprise. Organizations require audit professionals who possess the knowledge and expertise to identify critical issues and security challenges. The skills and practices that CISA promotes and evaluates are the building blocks of success in the field. Possessing the CISA demonstrates proficiency and is the basis for measurement in the profession.



# Target Audience

- Individuals who are willing to learn in Information Systems Auditing
- Professionals who are Auditors or working in an Audit environment
- The professionals who are willing to make a Career in Information Systems Auditing
- IT managers
- Security Managers
- System Analysts
- Consultants

# Pre-Requisite

A minimum of 5 years of professional information systems auditing, control or security work experience (as described in the CISA job practice areas) is required for certification. Substitutions and waivers of such experience, to a maximum of 3 years, maybe obtained as follows:

- A maximum of 1 year of information systems experience OR 1 year of non-IS auditing experience can be substituted for 1 year of experience.
- 60 to 120 completed university semester credit hours (the equivalent of a 2-year or 4-year degree) not limited by the 10-year preceding restriction can be substituted for 1 or 2 years, respectively, of experience.
- A master's degree in information security or information technology from an accredited university can be substituted for 1 year of experience.

## Exam Information

| | |
|---|---|
| Duration | 4 hours |
| Number of Questions | 150 |
| Question format | Multiple Choice |
| Passing grade | 450 out of 800 |
| Languages available | English, French, German, Hebrew, Italian, Japanese, Korean, Spanish, Turkish, Chinese |

## Why Infosec Train?

Certified & Experienced Instructor

Flexible Schedule

Access to the recorded sessions

Post Training Support

Tailor Made Training

Telegram Discussion Group

# Our Expert Instructors

"

Certified Security specialist having several years of experience in Information Security across all domains including application security, vulnerability assessment, ethical hacking, pen testing and IT risk and compliance and more

### PRABH NAIR

CISSP I CCSP I CSSLP I CRISC I CISM I CISA I CGEIT

"

Ajit has more than 15 years of experience which include Consulting, Network and InfoSec training ( CISA, CISM, CISSP, CCSP, Security+, SSCP), Content development, Assessments and auditing and more

### AJIT

CISSP I CCSP I CRISC I CISA I CGEIT

"

8+ years' experience as an IT Information Security analyst. Compatible team player through complete project cycles, testing and final implementation.

### JEEVAN K

CISA | CISSP | CRISC | ECSA | CEH

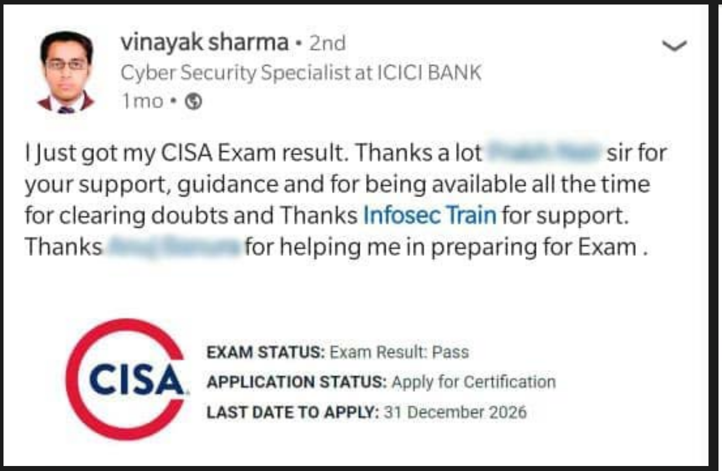
"

Chartered Accountant from Institute of CA of India with over 10 years of experience in Financial Reporting, auditing and taxation across CA Practice and corporate. Certified Information Security Auditor (CISA) accreditation from ISACA ( Rank - 2, ISACA Chennai Chapter, June 2019 ).

### ASWINI S

CA | CISA | Dip-IFR (UK)

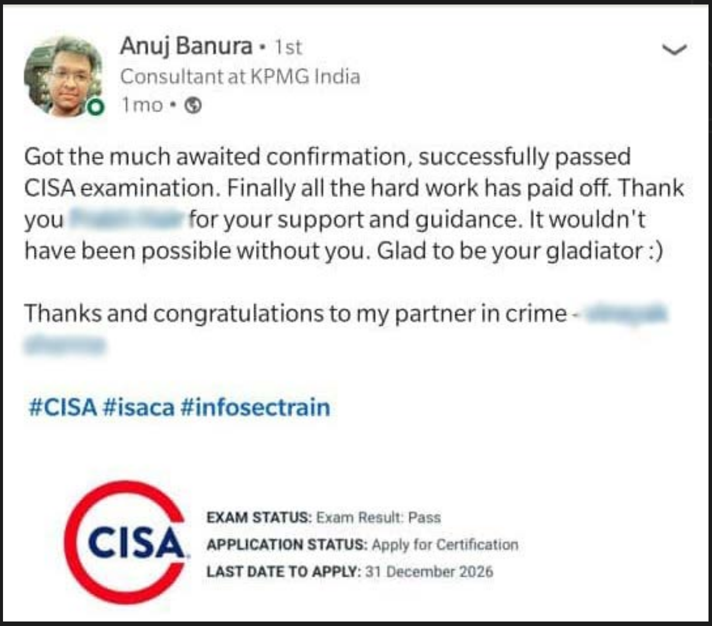
# Happy Learners from LinkedIn



vinayak sharma • 2nd
Cyber Security Specialist at ICICI BANK
1mo •

I Just got my CISA Exam result. Thanks a lot [redacted] sir for your support, guidance and for being available all the time for clearing doubts and Thanks Infosec Train for support. Thanks [redacted] for helping me in preparing for Exam .

**EXAM STATUS:** Exam Result: Pass
**APPLICATION STATUS:** Apply for Certification
**LAST DATE TO APPLY:** 31 December 2026



Anuj Banura • 1st
Consultant at KPMG India
1mo •

Got the much awaited confirmation, successfully passed CISA examination. Finally all the hard work has paid off. Thank you [redacted] for your support and guidance. It wouldn't have been possible without you. Glad to be your gladiator :)

Thanks and congratulations to my partner in crime - [redacted]

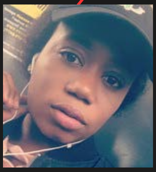
#CISA #isaca #infosectrain

**EXAM STATUS:** Exam Result: Pass
**APPLICATION STATUS:** Apply for Certification
**LAST DATE TO APPLY:** 31 December 2026

# HAPPY LEARNERS FROM THE WORLD

**Prabhav**
CISA | India

I had the opportunity to take CISA lessons. The Trainer has been consistently giving me a lot of mental and material support. I would recommend his mentorship for any aspirant.



**Fatimah Akintola**
CISA | USA

I made the right choice, and every session was worth it. Thank you once again. I would highly recommend my friends, the professor has immense knowledge and the subject and was very logical and practical.

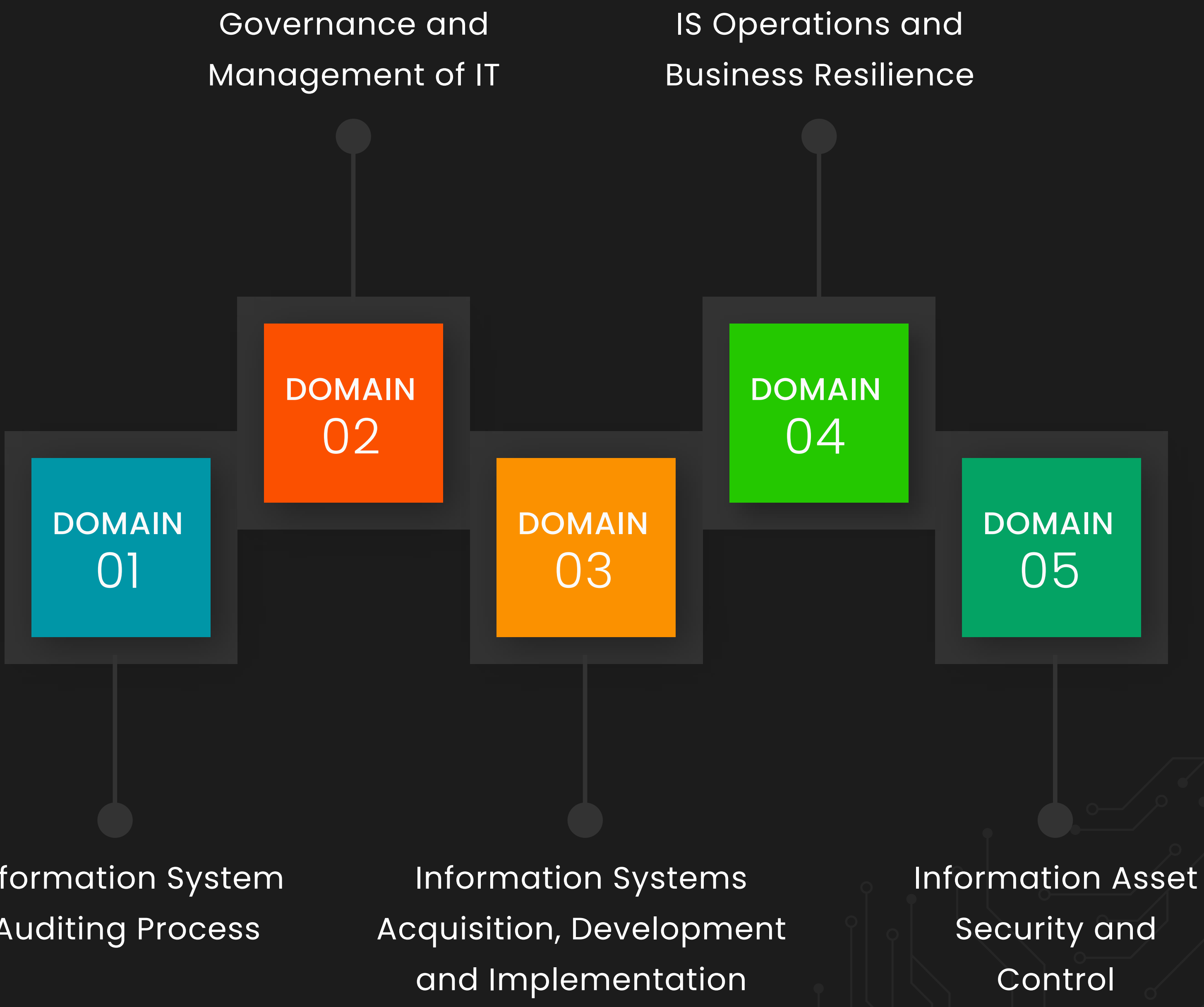
**Wahidullah Badri**
CISA | India

The session was very productive and informative, understood many concepts. Talented and knowledgeable trainer, explained the concepts clearly and practicing questions in topic.

INFOSECTRAIN

# CISA Course Outline

The five domains in CISA include



DOMAIN 01

Information System Auditing Process

DOMAIN 02

Governance and Management of IT

DOMAIN 03

Information Systems Acquisition, Development and Implementation

DOMAIN 04

IS Operations and Business Resilience

DOMAIN 05

Information Asset Security and Control

## Domain 1: Information System Auditing Process

1.1 Planning

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

1.2 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

2.1 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

2.2 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

3.1 Information Systems Acquisition and Development

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

3.2 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

4.1 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 Manageme

4.2 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

5.1 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

5.2 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

INFOSECTRAIN

www.infosectrain.com | sales@infosectrain.com