

Certified Information Systems Auditor (CISA)

Course Overview

This four-session, exam-prep course brings together the knowledge and practice to give learners the knowledge and concepts necessary to successfully take and pass the CISA exam.

CISA Exam Preparation

Topics:

- About the CISA Exam
- CISA Certification
- Basis of the CISA Exam
- Exam Scoring
- Preparing for the Exam

Domain 1 - Information System Auditing Process

Learning Objectives:

- Plan an audit to determine whether information systems are protected, controlled, and provide value to the enterprise.
- Conduct an audit following IS audit standards and a risk-based IS audit strategy.
- Communicate audit progress, findings, results, and recommendations to stakeholders.
- Conduct audit follow-up to evaluate whether risks have been sufficiently addressed.
- Evaluate IT management and monitoring of controls.
- Utilize data analytics tools to streamline audit processes.
- Provide consulting services and guidance to the enterprise to improve the quality and control of information systems.
- Identify opportunities for process improvement in the enterprise's IT policies and practices.

Topics:

- IS Audit Standards, Guidelines, Functions, and Codes of Ethics
- Types of Audits, Assessments, and Reviews
- Risk-based Audit Planning
- Types of Controls and Considerations
- Audit Project Management

- Audit Testing and Sampling Methodology
- Audit Evidence Collection Techniques
- Audit Data Analytics
- Reporting and Communication Techniques
- Quality Assurance and Improvement of Audit Process

Domain 2 – Governance and Management of IT

Learning Objectives:

- Evaluate the IT strategy for alignment with the enterprise's strategies and objectives.
- Evaluate the effectiveness of IT governance structure and IT organizational structure.
- Evaluate the enterprise's management of IT policies and practices.
- Evaluate the enterprise's IT policies and practices for compliance with regulatory and legal requirements.
- Evaluate IT resource and portfolio management for alignment with the enterprise's strategies and objectives.
- Evaluate the enterprise's risk management policies and practices.
- Evaluate IT management and monitoring of controls.
- Evaluate the monitoring and reporting of IT key performance indicators (KPIs).
- Evaluate whether IT supplier selection and contract management processes align with business requirements.
- Evaluate whether IT service management practices align with business requirements.
- Conduct periodic review of information systems and enterprise architecture. Evaluate data governance policies and practices.
- Evaluate the information security program to determine its effectiveness and alignment with the enterprise's strategies and objectives.
- Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices.

Topics

- Laws, Regulations, and Industry Standards
- Organizational Structure, IT Governance, and IT Strategy
- IT Policies, Standards, Procedures, and Guidelines
- Enterprise Architecture and Considerations
- Enterprise Risk Management (ERM)
- Privacy Program and Principles

- Data Governance and Classification
- IT Resource Management
- IT Vendor Management
- IT Performance Monitoring and Reporting
- Quality Assurance and Quality Management of IT

Domain 3 – Information Systems Acquisition, Development, and Implementation

Learning Objectives:

- Evaluate whether the business case for proposed changes to information systems meet business objectives.
- Evaluate the enterprise's project management policies and practices.
- Evaluate controls at all stages of the information systems development lifecycle.
- Evaluate the readiness of information systems for implementation and migration into production.
- Conduct post-implementation review of systems to determine whether project deliverables, controls, and requirements are met.
- Evaluate change, configuration, release, and patch management policies and practices.

Topics:

- Project Governance and Management
- Business Case and Feasibility Analysis
- System Development Methodologies
- Control Identification and Design
- System Readiness and Implementation Testing
- Implementation Configuration and Release Management
- System Migration, Infrastructure Deployment, and Data Conversion
- Postimplementation Review

Domain 4 – Information Systems Operations and Business Resilience

Learning Objectives:

- Evaluate the enterprise's ability to continue business operations.
- Evaluate whether IT service management practices align with business requirements.
- Conduct periodic review of information systems and enterprise architecture.
- Evaluate IT operations to determine whether they are controlled effectively and continue to support the enterprise's objectives.

- Evaluate IT maintenance practices to determine whether they are controlled effectively and continue to support the enterprise's objectives.
- Evaluate database management practices.
- Evaluate data governance policies and practices.
- Evaluate problem and incident management policies and practices.
- Evaluate change, configuration, release, and patch management policies and practices.
- Evaluate end-user computing to determine whether the processes are effectively controlled.
- Evaluate policies and practices related to asset lifecycle management.

Topics:

- IT Components
- IT Asset Management
- Job Scheduling and Production Process Automation
- System Interfaces
- End-user Computing and Shadow IT
- Systems Availability and Capacity Management
- Problem and Incident Management
- IT Change, Configuration, and Patch Management
- Operational Log Management
- IT Service Level Management
- Database Management
- Business Impact Analysis
- System and Operational Resilience
- Data Backup, Storage, and Restoration
- Business Continuity Plan
- Disaster Recovery Plans

Domain 5 – Protection of Information Assets

Learning Objectives:

- Conduct audit in accordance with IS audit standards and a risk-based IS audit strategy.
- Evaluate problem and incident management policies and practices.
- Evaluate the enterprise's information security and privacy policies and practices.
- Evaluate physical and environmental controls to determine whether information assets are adequately safeguarded.

- Evaluate logical security controls to verify the confidentiality, integrity, and availability of information.
- Evaluate data classification practices for alignment with the enterprise's policies and applicable external requirements.
- Evaluate policies and practices related to asset lifecycle management.
- Evaluate the information security program to determine its effectiveness and alignment with the enterprise's strategies and objectives.
- Perform technical security testing to identify potential threats and vulnerabilities.
- Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices.

Topics:

- Information Asset Security Policies, Frameworks, Standards, and Guidelines
- Physical and Environmental Controls
- Identity and Access Management
- Network and End-Point Security
- Data Loss Prevention
- Data Encryption
- Public Key Infrastructure (PKI)
- Cloud and Virtualized Environments
- Mobile, Wireless, and Internet-of-Things Devices
- Security Awareness Training and Programs
- Information System Attack Methods and Techniques
- Security Testing Tools and Techniques
- Security Monitoring Logs, Tools, and Techniques
- Security Incident Response Management
- Evidence Collection and Forensics

CISA Exam Preparation

- CISA Exam Rules
- Exam Tips
- Day of the Exam
- CISA Certification Steps