BLUEMARK ACADEMY

CISA (Certified Information Systems Auditor) Training

Duration: 5 Days · **Training format:** Virtual Classroom / Online

Description

This CISA training aims to provide participants with a comprehensive and exam-focused understanding of information systems auditing, IT governance, risk management, and information security controls. The training is designed in alignment with the CISA domain structure defined by ISACA and aims to enable participants to both prepare effectively for the CISA certification exam and acquire practical knowledge and competencies that add value to information systems audit processes within their organizations.

Throughout the training, key topics such as the risk-based audit approach, IT governance, system development and operational processes, business continuity, disaster recovery, and controls for the protection of information assets are covered and reinforced through case studies, sample scenarios, and exam-style practice questions.

Audience

- Information Systems Auditors (IS Auditors)
- Internal and External Auditors
- IT Audit and IT Control teams
- Information Security and Cybersecurity professionals
- Risk, Compliance, and Internal Control professionals
- IT Managers and IT Governance professionals
- Professionals preparing for the CISA certification exam

Outline

Day 1 – Information Systems Auditing Fundamentals & Domain 1

- Introduction to CISA certification and ISACA framework
- Role and responsibilities of the Information Systems Auditor
- ISACA Code of Professional Ethics and auditing standards
- Audit planning and risk-based audit approach
- Audit evidence types, collection techniques, and sampling

- Audit reporting, communication, and follow-up activities
- Practice questions and group discussions

Day 2 – Governance and Management of IT (Domain 2)

- IT governance concepts, structures, and frameworks
- Alignment of IT strategy with business objectives
- IT policies, standards, and procedures
- IT resource management and performance measurement
- Risk management and internal control frameworks
- Case study: Evaluating IT governance effectiveness
- Domain-based practice questions

Day 3 – IS Acquisition, Development & Implementation (Domain 3)

- Project management fundamentals and controls
- System Development Life Cycle (SDLC) methodologies
- Requirements definition and solution acquisition
- Application controls and system configuration reviews
- Change, release, and implementation management
- Post-implementation review and audit considerations
- Scenario-based exercises and exam-style questions

Day 4 – IS Operations & Business Resilience (Domain 4)

- IT operations management and service delivery models
- Incident, problem, and change management processes
- IT service continuity and availability management
- Business Continuity Planning (BCP) fundamentals
- Disaster Recovery Planning (DRP) and testing methods
- Backup, recovery, and resilience controls
- Hands-on case study and domain review questions

Day 5 – Protection of Information Assets & Exam Review (Domain 5)

- Information security governance and risk management
- Logical access controls and identity management
- Physical and environmental security controls
- Cybersecurity threats, vulnerabilities, and mitigation
- Data classification, privacy, and regulatory considerations
- Full CISA exam review and mock questions
- Exam strategies, time management, and final Q&A

Prerequisites

Basic knowledge of information technologies, information systems, or auditing concepts and familiarity with IT processes, internal control, or risk management concepts