



classJO

PROFESSIONAL LEARNING PLATFORM

LEARN TODAY... LEAD TOMORROW

Professional Courses • Expert Instructors • Flexible Learning



PROFESSIONAL COURSES

Up-to-date content aligned with industry needs.



FLEXIBLE LEARNING

Online and in-person options that fit your schedule.



EXPERT INSTRUCTORS

Learn from professionals with real-world experience.



CERTIFICATES & SUPPORT

Earn certificates and get continuous support.

Certified Information Systems Auditor (CISA) Training

Eng. Mansour Quzmar

Certified Information Systems Auditor (CISA) Training

Overview

- Introduction to Information Systems Auditing, Control, and Assurance
 - Understanding the role and responsibilities of Information Systems Auditors
 - Learning audit methodologies, governance frameworks, and risk-based auditing approaches
 - Understanding IT governance, IT operations, systems acquisition, and information security controls
 - Developing knowledge in audit planning, execution, reporting, and follow-up activities
 - Understanding compliance, regulatory requirements, and control assessment techniques
 - Introduction to cybersecurity, risk management, and business continuity from an audit perspective
 - Preparation for the ISACA CISA certification exam
-

Training Objectives

By the end of this training, participants will be able to:

- Understand the principles and practices of Information Systems Auditing
- Explain audit standards, guidelines, and professional ethics
- Plan, conduct, and manage IT audits effectively
- Assess IT governance structures and management processes
- Evaluate IT operations, systems development, and infrastructure controls
- Identify and assess information security risks and controls
- Understand business continuity and disaster recovery audit requirements
- Evaluate compliance with policies, standards, and regulations

- Develop audit findings, recommendations, and reports
 - Apply risk-based auditing techniques and control assessment methodologies
 - Understand cybersecurity concepts from an audit and assurance perspective
 - Prepare for the CISA certification examination
-

Training Outline

Module 1: Introduction to CISA and Information Systems Auditing

- Overview of CISA certification
 - Role of the Information Systems Auditor
 - Audit concepts and terminology
 - Types of audits
 - Risk-based auditing approach
 - Audit standards, guidelines, and ethics
 - Internal controls overview
-

Module 2: The Process of Auditing Information Systems

- Audit planning and preparation
 - Audit scope and objectives
 - Risk assessment techniques
 - Audit evidence collection
 - Sampling methods
 - Audit testing procedures
 - Audit documentation and working papers
 - Audit reporting and follow-up
-

Module 3: Governance and Management of IT

- IT governance principles
 - Organizational structure and responsibilities
 - Policies, standards, and procedures
 - IT strategy alignment with business objectives
 - Risk management frameworks
 - IT performance monitoring
 - Compliance and regulatory requirements
 - Third-party and vendor management
-

Module 4: Information Systems Acquisition, Development, and Implementation

- System development life cycle (SDLC)
 - Project management controls
 - Business requirements and feasibility analysis
 - Change management controls
 - Testing and quality assurance
 - System implementation and migration controls
 - Post-implementation review
 - Agile and DevOps considerations
-

Module 5: Information Systems Operations and Business Resilience

- IT operations management
- Service management concepts
- Incident and problem management
- Backup and recovery controls

- Business continuity planning (BCP)
 - Disaster recovery planning (DRP)
 - IT asset management
 - Capacity and performance management
-

Module 6: Protection of Information Assets

- Information security principles
 - Access control management
 - Identity and access management (IAM)
 - Network security concepts
 - Endpoint and infrastructure security
 - Data protection and privacy
 - Cryptography basics
 - Security monitoring and logging
 - Security incident management
-

Module 7: Cybersecurity and Emerging Technologies

- Cybersecurity threats and attack vectors
 - Cloud computing risks and controls
 - Virtualization and container security
 - Mobile and remote access security
 - Artificial intelligence and emerging technologies
 - Security governance and compliance
-

Module 8: Audit Tools, Techniques, and Reporting

- Computer-assisted audit techniques (CAATs)
 - Data analysis and audit automation
 - Control assessment methodologies
 - Vulnerability and configuration assessments
 - Audit findings and recommendations
 - Reporting best practices
 - Communication with stakeholders
-

Module 9: Practical Audit Scenarios and Case Studies

- IT governance audit scenarios
 - Risk assessment exercises
 - Security control review examples
 - Compliance audit case studies
 - Business continuity audit examples
 - Real-world audit findings and remediation discussions
-

Module 10: Certification Preparation

- CISA exam structure and domains
- Exam question analysis techniques
- Practice questions and mock exams
- Study guidance and exam preparation tips
- Review sessions and discussions