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 Security Manager (CISM) Training

Eng. Mansour Quzmar

class JO

Certified Information Security Manager (CISM) Training

Overview

- Introduction to Information Security Management and Governance
- Understanding the role of the Information Security Manager in organizations
- Learning how to establish, manage, and maintain an enterprise information security program
- Understanding information security governance, risk management, and compliance principles
- Developing knowledge in incident management and security program development
- Understanding how to align information security strategies with business objectives
- Introduction to security controls, frameworks, policies, and best practices
- Preparation for the ISACA CISM certification exam

Training Objectives

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

- Understand the core concepts of Information Security Management
- Explain the principles of information security governance
- Align security strategies with organizational goals and objectives
- Understand enterprise risk management and risk assessment methodologies
- Develop and manage information security programs
- Understand information security policies, standards, and procedures
- Identify and manage information security incidents
- Understand incident response planning and business continuity concepts
- Implement security management best practices and governance frameworks
- Understand compliance, legal, regulatory, and audit requirements
- Improve organizational security posture and operational resilience
- Prepare for the CISM certification examination

Training Outline

Module 1: Introduction to CISM and Information Security Management

- Overview of CISM certification
- Role of the Information Security Manager
- Information security concepts and principles
- Governance vs management
- Information security frameworks and standards
- Enterprise security objectives

Module 2: Information Security Governance

- Governance principles and structures
- Aligning security with business objectives
- Security governance frameworks
- Roles and responsibilities
- Organizational culture and security awareness
- Security policies, standards, and procedures
- Legal, regulatory, and compliance requirements

Module 3: Information Security Risk Management

- Risk management concepts
- Risk identification and assessment
- Risk analysis methodologies
- Risk treatment and mitigation
- Risk appetite and tolerance
- Third-party and vendor risks

- Risk monitoring and reporting
- Business impact analysis (BIA)

Module 4: Information Security Program Development and Management

- Developing an information security program
- Security program objectives and scope
- Security architecture and controls
- Resource and budget management
- Security metrics and performance measurement
- Security awareness and training programs
- Security operations management
- Security technologies and tools

Module 5: Information Security Incident Management

- Incident management lifecycle
- Incident response planning
- Incident detection and analysis
- Containment, eradication, and recovery
- Digital forensics basics
- Communication and escalation procedures
- Lessons learned and continual improvement
- Crisis management coordination

Module 6: Business Continuity and Disaster Recovery

- Business continuity concepts
- Disaster recovery planning

- Recovery objectives (RTO/RPO)
- Continuity testing and exercises
- Resilience and recovery strategies
- Integration with incident management

Module 7: Security Governance Frameworks and Standards

- ISO/IEC 27001 overview
- NIST Cybersecurity Framework
- COBIT integration
- IT governance alignment
- Compliance management
- Audit and assurance considerations

Module 8: Security Operations and Control Management

- Access control management
- Identity and access management (IAM)
- Security monitoring and logging
- Vulnerability management
- Security incident and event management (SIEM)
- Security operations center (SOC) concepts

Module 9: Practical Scenarios and Case Studies

- Security governance scenarios
- Risk assessment workshops
- Incident response simulations
- Security program implementation examples

- Compliance and audit scenarios
- Real-world security management case studies

Module 10: Certification Preparation

- CISM exam structure and domains
- Exam question techniques
- Practice questions and assessments
- Study guidance and exam preparation tips
- Review sessions and discussions