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 in Risk and Information Systems Control (CRISC) Training

Eng. Mansour Quzmar

Certified in Risk and Information Systems Control (CRISC) Training

Overview

- Introduction to IT Risk Management and Information Systems Controls based on ISACA CRISC framework
- Understanding enterprise risk management concepts, methodologies, and governance principles
- Learning how to identify, assess, analyze, respond to, and monitor IT and business risks
- Understanding the design, implementation, and management of information systems controls
- Developing practical skills in risk assessment, control evaluation, and risk response planning
- Understanding cybersecurity risks, compliance requirements, and operational resilience
- Introduction to governance frameworks, risk reporting, and control monitoring techniques
- Preparation for the ISACA CRISC certification examination

Training Objectives

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

- Understand the principles of IT Risk Management and Information Systems Control
- Identify and assess organizational and technology-related risks
- Apply risk analysis and risk response methodologies
- Understand risk governance and enterprise risk management concepts
- Design and evaluate information systems controls
- Understand control monitoring and performance measurement techniques
- Assess cybersecurity, operational, and compliance risks
- Understand risk ownership, accountability, and communication processes

- Integrate risk management into organizational decision-making
- Improve organizational resilience and control effectiveness
- Understand governance, compliance, and audit considerations
- Prepare for the CRISC certification examination

Training Outline

Module 1: Introduction to CRISC and IT Risk Management

- Overview of CRISC certification
- Role of the Risk and Control Professional
- Fundamentals of IT risk management
- Enterprise risk management concepts
- Governance, risk, and compliance (GRC)
- Risk terminology and principles

Module 2: Governance and Risk Management

- IT governance concepts
- Risk governance structure
- Organizational roles and responsibilities
- Risk appetite and tolerance
- Policies, standards, and procedures
- Compliance and regulatory requirements
- Risk culture and awareness

Module 3: Risk Identification

- Identifying organizational risks
- Business and technology risks

- Threats, vulnerabilities, and risk events
- Internal and external risk factors
- Emerging technology risks
- Third-party and vendor risks
- Risk scenario development

Module 4: Risk Assessment and Analysis

- Risk assessment methodologies
- Qualitative and quantitative risk analysis
- Likelihood and impact analysis
- Risk prioritization techniques
- Business impact analysis (BIA)
- Root cause analysis
- Risk evaluation and reporting

Module 5: Risk Response and Treatment

- Risk response strategies
    - Risk mitigation
    - Risk transfer
    - Risk acceptance
    - Risk avoidance
- Developing risk treatment plans
- Control selection and implementation
- Residual risk management
- Risk monitoring and review

Module 6: Information Systems Controls

- Types of controls
  - Preventive controls
  - Detective controls
  - Corrective controls
- Administrative, technical, and physical controls
- Access control management
- Change management controls
- Network and infrastructure security controls
- Data protection and backup controls

Module 7: Control Design and Assessment

- Control design principles
- Control testing and evaluation
- Control effectiveness assessment
- Key Risk Indicators (KRIs)
- Key Performance Indicators (KPIs)
- Monitoring and reporting mechanisms
- Audit and assurance considerations

Module 8: Cybersecurity and Emerging Risks

- Cybersecurity risk management
- Security incident management
- Cloud computing risks
- Third-party security risks
- Data privacy and protection

- Business continuity and disaster recovery
- Emerging technology threats

Module 9: Risk Monitoring and Reporting

- Continuous risk monitoring
- Risk dashboards and metrics
- Executive and management reporting
- Communication and escalation procedures
- Incident reporting
- Compliance monitoring
- Continuous improvement practices

Module 10: Practical Risk Management Scenarios

- Enterprise risk assessment workshops
- Control evaluation exercises
- Cybersecurity risk scenarios
- Compliance and audit case studies
- Incident response and risk mitigation examples
- Real-world governance and risk management discussions

Module 11: CRISC Certification Preparation

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