



Auditing Information Security

Course Introduction:

In today's digital age, organizations face increasing risks related to cyber threats, data breaches, and regulatory non-compliance. Auditing information security is essential to ensure that security policies, controls, and risk management strategies are effectively implemented to protect sensitive information and maintain business continuity. This five-day training program provides a comprehensive theoretical foundation for conducting information security audits, covering industry best practices, risk assessment frameworks, and compliance requirements.

Participants will explore methodologies for evaluating security policies, assessing vulnerabilities, and ensuring adherence to regulatory standards such as ISO 27001, NIST, GDPR, and other cybersecurity frameworks. The course will also cover the principles of security governance, risk management, incident response, and auditing tools. By the end of this training, attendees will have the knowledge required to conduct thorough information security audits, identify weaknesses, and recommend improvements to enhance an organization's security posture.

Course Objectives:

Upon completion of this course, participants will:

- Understand the principles and objectives of information security auditing.
- Learn about risk management frameworks and security governance models.
- Explore key regulatory and compliance requirements for information security.
- Identify security risks, vulnerabilities, and control deficiencies.
- Assess the effectiveness of security policies and incident response plans.
- Learn methodologies for auditing IT infrastructure, networks, and data protection measures.
- Analyze audit findings and develop actionable recommendations.
- Gain insights into emerging trends and technologies in security auditing.

Who Should Attend?

This course is designed for professionals and individuals such as IT auditors and compliance professionals, Information security officers and risk managers, Cybersecurity professionals and analysts, Internal and external auditors, IT managers and governance specialists, Incident response and SOC team members, and Government and regulatory compliance officers.

Course Outline:

Day 1: Introduction to Information Security Auditing

- Importance of auditing in information security management
- Overview of security audit methodologies and frameworks
- Understanding security governance and risk management principles
- Compliance standards: ISO 27001, NIST, GDPR, PCI-DSS, etc.

Day 2: Security Risk Assessment and Vulnerability Management

- Identifying risks and threats to information systems
- Risk assessment methodologies and classification
- Evaluating security controls and risk mitigation strategies
- Reviewing case studies on security failures and vulnerabilities

Day 3: IT Infrastructure and Network Security Auditing

- Auditing network security configurations and firewall policies
- Assessing endpoint security, access controls, and authentication mechanisms
- Monitoring security logs and analyzing system events
- Evaluating cloud security and third-party risks

Day 4: Incident Response, Business Continuity, and Compliance Auditing

- Reviewing incident response and disaster recovery plans
- Auditing security awareness training and user compliance
- Assessing business continuity and disaster recovery measures
- Legal, ethical, and regulatory considerations in security audits

Day 5: Reporting, Recommendations, and Future Trends

- Documenting audit findings and preparing audit reports
- Presenting recommendations for improving security posture
- Emerging trends in security auditing: AI, automation, and Zero Trust
- Course review, Q&A session, and discussion on audit best practices

Course Methodology:

A variety of methodologies will be used during the course that including:

- (30%) Based on Case Studies
- (30%) Techniques
- (30%) Role Play
- (10%) Concepts

- Pre-test and Post-test
- Variety of Learning Methods
- Lectures
- Case Studies and Self Questionnaires
- Group Work
- Discussion
- Presentation

Course Certificate:

International Center for Training & Development (ICTD) will award an internationally recognized certificate(s) for each delegate on completion of training.

Course Fees:

To be advised as per course location. This rate includes participant's manual, Hand-Outs, buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Course Timings:

Daily Course Timings:

08:00 - 08:20	Morning Coffee / Tea
08:20 - 10:00	First Session
10:00 - 10:20	Coffee / Tea / Snacks
10:20 - 12:20	Second Session
12:20 - 13:30	Lunch Break & Prayer Break
13:30 - 15:00	Last Session