Auditing of Information Security Controls Training Course

Professional Development Training Course Outline

Category	Quality Assurance and ISO standards	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today?ÇÖs rapidly evolving digital landscape, organizations face an increasing number of cyber threats and regulatory compliance requirements. Auditing of information security controls Training Course is a critical process that ensures systems, data, and networks remain secure, reliable, and compliant. This training course provides participants with essential knowledge on conducting effective audits of information security controls, applying international standards, and implementing best practices for risk mitigation. The course emphasizes trending topics such as cybersecurity frameworks, ISO/IEC 27001, compliance auditing, and cloud security assurance, helping participants develop the skills needed to assess and enhance organizational resilience.

By combining theory with practical case studies, this course equips participants to evaluate security controls in diverse environments and industries. Attendees will gain insights into identifying vulnerabilities, testing system controls, and preparing detailed audit reports for executive decision-making. The program is designed to enhance skills in audit planning, control testing, incident response, and compliance validation. This training is ideal for professionals seeking to strengthen their expertise in governance, risk, and compliance while aligning with the latest trends in information security auditing.

Programme Curriculum

Auditing of Information Security Controls Training Course

Introduction

In today?ÇÖs rapidly evolving digital landscape, organizations face an increasing number of cyber threats and regulatory compliance requirements. Auditing of information security controls Training Course is a critical process that ensures systems, data, and networks remain secure, reliable, and compliant. This training course

provides participants with essential knowledge on conducting effective audits of information security controls, applying international standards, and implementing best practices for risk mitigation. The course emphasizes trending topics such as cybersecurity frameworks, ISO/IEC 27001, compliance auditing, and cloud security assurance, helping participants develop the skills needed to assess and enhance organizational resilience.

By combining theory with practical case studies, this course equips participants to evaluate security controls in diverse environments and industries. Attendees will gain insights into identifying vulnerabilities, testing system controls, and preparing detailed audit reports for executive decision-making. The program is designed to enhance skills in audit planning, control testing, incident response, and compliance validation. This training is ideal for professionals seeking to strengthen their expertise in governance, risk, and compliance while aligning with the latest trends in information security auditing.

Course Objectives

1. Understand the fundamentals of auditing information security controls
2. Apply international standards such as ISO/IEC 27001 and NIST frameworks
3. Identify and assess risks within IT and cloud-based environments
4. Conduct effective compliance audits for regulatory requirements
5. Enhance skills in cybersecurity auditing and digital forensics
6. Evaluate internal controls for data protection and privacy management
7. Develop strategies for vulnerability testing and remediation
8. Prepare detailed and actionable audit reports for management
9. Strengthen capabilities in IT governance and risk management
10. Implement audit methodologies for incident detection and response
11. Apply trending tools and technologies in audit automation
12. Build resilience against emerging cyber threats through control validation
13. Gain practical knowledge through real-world case studies of IS audits

Organizational Benefits

- Strengthened information security governance across the enterprise
- Improved compliance with international standards and regulations
- Enhanced risk management practices through effective auditing
- Increased awareness of vulnerabilities and corrective actions
- Streamlined audit processes with modern tools and automation
- Improved resilience against cyberattacks and data breaches
- Stronger incident detection and faster response mechanisms
- Increased stakeholder confidence in security systems
- Cost reduction from minimizing compliance violations
- Alignment of audit practices with organizational objectives

Target Audiences

1. Information Security Auditors
2. IT Risk and Compliance Officers
3. Cybersecurity Professionals
4. Internal and External Auditors
5. IT Managers and Administrators
6. Data Privacy Officers
7. Governance and Risk Consultants

8. Security Operations Center (SOC) Analysts

Course Duration: 10 days

Course Modules

Module 1: Introduction to Information Security Auditing

- Overview of information security and audit fundamentals
- Understanding governance, risk, and compliance frameworks
- Introduction to auditing standards (ISO, NIST, COBIT)
- Role of auditors in protecting organizational data
- Tools and technologies in IS auditing
- Case study: Successful IS audit in a financial institution

Module 2: Audit Planning and Risk Assessment

- Key steps in planning an IS audit
- Risk-based audit approach explained
- Identifying risks in IT infrastructure and processes
- Prioritizing controls based on impact analysis
- Audit scope and resource allocation
- Case study: Risk-based audit planning in healthcare

Module 3: IT Governance and Security Policies

- Role of governance in IS auditing
- Development of effective IT policies and standards
- Aligning controls with business objectives
- Evaluating governance maturity models
- Auditing policy compliance and effectiveness
- Case study: IT governance audit in a telecom company

Module 4: Access Controls and Identity Management

- Types of access control mechanisms
- Role-based access and least privilege principles
- Auditing identity management systems
- Evaluating authentication and authorization processes
- Detecting anomalies in user access patterns
- Case study: Access control audit in cloud infrastructure

Module 5: Network Security Controls Auditing

- Components of secure network architecture
- Firewalls, IDS/IPS, and monitoring systems
- Auditing network segmentation and configuration
- Assessing VPNs and wireless network security
- Testing resilience of perimeter defenses
- Case study: Network audit in a multinational company

Module 6: Application Security Controls

- Security measures in application development
- Auditing secure coding practices
- Assessing software vulnerabilities and patching
- Web application firewalls and their audit scope
- Testing APIs and mobile applications
- Case study: Application security audit in e-commerce

Module 7: Cloud Security and Virtualization Auditing

- Cloud deployment models and risks
- Evaluating cloud service provider compliance
- Security challenges in virtualized environments
- Auditing SaaS, PaaS, and IaaS infrastructures
- Shared responsibility model in cloud auditing
- Case study: Cloud audit in a government agency

Module 8: Data Protection and Privacy Controls

- Understanding data privacy regulations (GDPR, HIPAA, CCPA)
- Auditing data lifecycle management practices
- Encryption, tokenization, and masking audits
- Compliance with data subject rights
- Techniques for auditing data retention policies
- Case study: Data privacy audit in healthcare services

Module 9: Incident Response and Business Continuity Auditing

- Role of auditors in incident management
- Business continuity planning and disaster recovery
- Testing effectiveness of incident response plans
- Auditing backup and recovery processes
- Gap analysis in business continuity frameworks
- Case study: Audit of incident response in manufacturing

Module 10: Vulnerability and Penetration Testing Audits

- Differences between vulnerability scanning and penetration testing
- Integrating penetration test results into audits
- Tools for vulnerability assessment
- Compliance implications of unpatched systems
- Risk prioritization of identified vulnerabilities
- Case study: Penetration testing audit in banking sector

Module 11: Compliance Auditing and Regulatory Requirements

- Key compliance regulations (SOX, PCI DSS, HIPAA)
- Methods for auditing regulatory frameworks
- Evidence collection for compliance validation
- Challenges in multi-jurisdictional audits
- Preparing compliance audit reports
- Case study: Compliance audit in retail industry

Module 12: Digital Forensics and Evidence Collection

- Role of digital forensics in IS audits
- Tools for forensic data collection and analysis
- Chain of custody and evidence preservation
- Integration of forensic techniques in audits
- Legal and ethical considerations in evidence handling
- Case study: Digital forensics audit in law enforcement

Module 13: Audit Reporting and Documentation

- Structure of effective audit reports
- Techniques for documenting audit findings
- Presenting results to executive management
- Communicating audit recommendations effectively
- Importance of follow-up audits
- Case study: Audit reporting in government sector

Module 14: Emerging Trends in IS Auditing

- AI and machine learning in audit automation
- Blockchain-based auditing applications
- Cloud-native security control audits
- Zero Trust architecture and audit requirements
- Cybersecurity maturity model certification (CMMC)
- Case study: Emerging trends audit in IT industry

Module 15: Capstone Case Studies and Practical Audit Workshop

- Group exercise: Planning an IS audit from scratch
- Hands-on auditing with real-world scenarios
- Analyzing gaps in organizational controls
- Simulating incident response and control validation
- Peer review and feedback on audit reports
- Case study: End-to-end IS audit for multinational organization

Training Methodology

- Interactive instructor-led sessions
- Real-world case studies and simulations
- Group discussions and peer learning
- Hands-on exercises with auditing tools
- Continuous assessments and feedback
- Practical workshops for skill application

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com