Cybersecurity Auditing Training Course

Professional Development Training Course Outline

Category	ACCOUNTING & FINANCE	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Cybersecurity Auditing Training Course is a comprehensive, industry-aligned program designed to equip learners with advanced skills in cybersecurity risk assessment, IT governance, compliance auditing, and digital security frameworks. In today’s rapidly evolving digital landscape, organizations face increasing threats such as data breaches, ransomware attacks, insider threats, and cloud security vulnerabilities. This course provides deep insights into cybersecurity audit methodologies, ISO 27001 standards, NIST cybersecurity framework, penetration testing awareness, and enterprise security controls to ensure robust organizational protection.

This training is essential for professionals seeking to strengthen their expertise in cybersecurity auditing, risk management, and information assurance. It integrates practical auditing techniques, real-world cyber threat analysis, compliance evaluation strategies, and security governance practices. Learners will gain hands-on understanding of how to identify system vulnerabilities, evaluate security policies, and implement audit-driven cybersecurity improvements across enterprise IT infrastructures.

Programme Curriculum

Cybersecurity Auditing Training Course

Introduction

Cybersecurity Auditing Training Course is a comprehensive, industry-aligned program designed to equip learners with advanced skills in cybersecurity risk assessment, IT governance, compliance auditing, and digital security frameworks. In today’s rapidly evolving digital landscape, organizations face increasing threats such as data breaches, ransomware attacks, insider threats, and cloud security vulnerabilities. This course provides deep insights into cybersecurity audit methodologies, ISO 27001 standards, NIST cybersecurity framework, penetration testing awareness, and enterprise security controls to ensure robust organizational protection.

This training is essential for professionals seeking to strengthen their expertise in cybersecurity auditing, risk management, and information assurance. It integrates practical auditing techniques, real-world cyber threat analysis, compliance evaluation strategies, and security governance practices. Learners will gain hands-on understanding of how to identify system vulnerabilities, evaluate security policies, and implement audit-driven cybersecurity improvements across enterprise IT infrastructures.

Course Objectives

1. Understand cybersecurity auditing principles and information security governance frameworks
2. Develop expertise in risk-based auditing methodologies for IT environments
3. Apply ISO 27001 and NIST cybersecurity framework in audit processes
4. Identify and assess vulnerabilities in network, cloud, and application systems
5. Evaluate organizational cybersecurity policies and compliance standards
6. Perform internal and external cybersecurity audits effectively
7. Strengthen knowledge in ethical hacking and penetration testing fundamentals
8. Analyze cybersecurity threats, malware behavior, and attack vectors
9. Implement audit reporting and cybersecurity documentation techniques
10. Enhance incident response auditing and digital forensics awareness
11. Improve governance, risk, and compliance (GRC) capabilities
12. Integrate cybersecurity controls within enterprise systems
13. Develop strategic cybersecurity risk mitigation recommendations

Organizational Benefits

- Improved cybersecurity risk detection and mitigation capabilities
- Enhanced compliance with global cybersecurity regulations and standards
- Strengthened data protection and information security governance
- Reduced risk of cyberattacks, data breaches, and system vulnerabilities
- Increased operational resilience against cyber threats
- Better audit transparency and accountability across departments
- Strengthened IT infrastructure security posture
- Improved incident response and disaster recovery readiness
- Enhanced stakeholder trust and organizational reputation
- Cost reduction from prevented cybersecurity incidents

Target Audiences

- IT Security Analysts and Engineers
- Cybersecurity Auditors and Compliance Officers
- Network and System Administrators
- Risk Management Professionals
- Information Security Managers
- Internal and External Auditors
- IT Governance Professionals
- Cloud Security Specialists

Course Duration: 5 days

Course Modules

Module 1: Foundations of Cybersecurity Auditing

- Introduction to cybersecurity auditing concepts and principles
- Overview of IT governance and security frameworks
- Understanding audit lifecycle in cybersecurity environments
- Cyber risk identification and classification methods
- Audit planning techniques and documentation standards
- Case Study: Global financial institution cybersecurity audit failure analysis

Module 2: Cyber Risk Management and Assessment

- Cyber risk identification and evaluation techniques
- Risk scoring and prioritization models
- Threat intelligence and vulnerability assessment basics
- Asset classification and risk mapping strategies
- Risk mitigation planning and control implementation
- Case Study: Healthcare sector ransomware attack risk breakdown

Module 3: ISO 27001 and Security Compliance Auditing

- ISO 27001 standard structure and requirements
- Information Security Management System (ISMS) auditing
- Compliance evaluation techniques and gap analysis
- Policy and control effectiveness assessment
- Certification readiness and audit reporting
- Case Study: European data protection compliance audit failure

Module 4: Network and Infrastructure Security Auditing

- Network architecture security assessment techniques
- Firewall, IDS/IPS configuration auditing
- Server and endpoint security evaluation methods
- Cloud infrastructure security auditing basics
- Wireless network vulnerability analysis
- Case Study: Major telecom network breach investigation

Module 5: Application and Database Security Auditing

- Web application security testing principles
- Secure coding audit and OWASP standards
- Database security controls and encryption auditing
- API security evaluation techniques
- Application vulnerability scanning methods
- Case Study: Global e-commerce SQL injection attack analysis

Module 6: Incident Response and Digital Forensics

- Cyber incident detection and response processes
- Digital forensics investigation fundamentals
- Evidence collection and chain of custody management
- Malware analysis and breach investigation techniques
- Incident reporting and recovery planning
- Case Study: International cyber espionage investigation

Module 7: Ethical Hacking and Penetration Testing Awareness

- Ethical hacking concepts and methodologies
- Penetration testing lifecycle and tools overview
- Social engineering attack simulations
- System exploitation and vulnerability testing basics
- Security loophole identification techniques
- Case Study: Global banking penetration test simulation report

Module 8: Cybersecurity Governance and Audit Reporting

- Cybersecurity governance frameworks and policies
- Audit reporting structure and documentation standards
- KPI and cybersecurity metrics evaluation
- Continuous monitoring and improvement strategies
- Strategic cybersecurity decision-making support
- Case Study: Multinational enterprise cybersecurity governance transformation

Training Methodology

- Instructor-led classroom and virtual training sessions
- Hands-on practical cybersecurity auditing exercises
- Real-world case study analysis and discussions
- Interactive group workshops and simulations
- Industry-standard cybersecurity tools demonstrations
- Continuous assessment and knowledge evaluations

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	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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