Information Assurance and Security Policy Auditing Training Course

Professional Development Training Course Outline

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

Course Introduction

In today's hyper-connected digital economy, robust Information Assurance (IA) is non-negotiable for business continuity and regulatory compliance. Organizations face a constantly escalating barrage of cyber threats and complex regulatory frameworks like GDPR, HIPAA, and NIST. Information Assurance and Security Policy Auditing Training Course is specifically designed to bridge the critical gap between written Security Policy and real-world Security Controls implementation. Participants will gain the advanced, practical skills necessary to perform comprehensive, risk-based security audits, evaluate the effectiveness of an organization's security posture, and ensure data governance integrity. A successful audit function is the cornerstone of Cyber Resilience, transforming security from a cost center into a strategic competitive advantage.

This highly in-demand certification courses focuses on the auditor?ÇÖs role in assessing and validating an organization's Information Security Management System (ISMS). Through a blend of theoretical knowledge and hands-on case studies, learners will master IT audit methodologies, scrutinize the design and operating effectiveness of security policies, and generate high-impact audit reports. Key areas of focus include Third-Party Risk Management, Cloud Security Auditing, and the critical evaluation of Incident Response capabilities. Completing this program empowers security, risk, and compliance professionals to drive organizational maturity, achieve ISO 27001 compliance, and confidently navigate the evolving landscape of cyber risk management.

Programme Curriculum

Information Assurance and Security Policy Auditing Training Course

Introduction

In today's hyper-connected digital economy, robust Information Assurance (IA) is non-negotiable for business continuity and regulatory compliance. Organizations face a constantly escalating barrage of cyber threats and complex regulatory frameworks like GDPR, HIPAA, and NIST. Information Assurance and Security Policy Auditing Training Course is specifically designed to bridge the critical gap between written Security Policy and real-world Security Controls implementation. Participants will gain the advanced, practical skills necessary to perform comprehensive, risk-based security audits, evaluate the effectiveness of an organization's security posture, and ensure data governance integrity. A successful audit function is the cornerstone of Cyber Resilience, transforming security from a cost center into a strategic competitive advantage.

This highly in-demand certification courses focuses on the auditor?ÇÖs role in assessing and validating an organization's Information Security Management System (ISMS). Through a blend of theoretical knowledge and hands-on case studies, learners will master IT audit methodologies, scrutinize the design and operating effectiveness of security policies, and generate high-impact audit reports. Key areas of focus include Third-Party Risk Management, Cloud Security Auditing, and the critical evaluation of Incident Response capabilities. Completing this program empowers security, risk, and compliance professionals to drive organizational maturity, achieve ISO 27001 compliance, and confidently navigate the evolving landscape of cyber risk management.

Course Duration

5 days

Course Objectives

1. Master the Risk-Based Auditing methodology for Information Security Management Systems (ISMS).
2. Evaluate the design and operating effectiveness of Security Controls against frameworks like NIST CSF and ISO 27001.
3. Develop and implement a comprehensive Security Policy Auditing program.
4. Analyze and ensure compliance with major Data Privacy regulations, including GDPR and CCPA.
5. Identify and assess risks related to Cloud Security and DevSecOps pipelines.
6. Conduct Third-Party Risk Management (TPRM) audits of vendors and supply chain partners.
7. Apply practical Digital Forensics and Log Analysis techniques in an audit context.
8. Formulate high-impact Audit Findings and evidence-based recommendations to enhance Cyber Resilience.
9. Assess the maturity and effectiveness of an organization's Incident Response and Business Continuity Planning (BCP).
10. Validate Identity and Access Management (IAM) and Zero Trust Architecture controls.
11. Utilize automated GRC and Security Auditing Tools for continuous monitoring.
12. Communicate complex Cyber Risk to executive leadership and non-technical stakeholders.
13. Prepare for globally recognized certifications, such as CISA and ISO 27001 Lead Auditor.

Target Audience

1. IT Auditors
2. Information Security Managers and Analysts
3. Governance, Risk, and Compliance (GRC) Professionals
4. Chief Information Security Officers (CISOs) and Security Directors
5. Consultants specializing in Cybersecurity and Compliance
6. IT Operations and System Administrators with security responsibilities

7. Data Protection Officers (DPOs) and Privacy Officers
8. Internal Audit Staff.

Course Modules

Module 1: Foundational Principles of Information Assurance and Audit

- CIA Triad (Confidentiality, Integrity, Availability) and the pillars of Information Assurance.
- Risk-Based Audit planning and scoping: Identifying high-risk areas.
- Understanding the Security Policy Lifecycle and its direct link to controls.
- Key Audit Methodologies and standards
- Case Study: Auditing a corporate Acceptable Use Policy for clarity, enforceability, and employee awareness training.

Module 2: Security Governance and Regulatory Compliance

- IT Governance Frameworks and their role in the audit.
- In-depth review of ISO 27001 and NIST Cybersecurity Framework
- Auditing for Regulatory Compliance
- Control Mapping and testing.
- Case Study: A financial services firm facing a penalty for PCI-DSS non-compliance due to inadequate audit trails.

Module 3: Security Policy Evaluation and Control Assessment

- Best practices for evaluating the completeness and suitability of a Security Policy Suite.
- Auditing Access Control Policies
- Testing Data Classification and Data Handling Policies effectiveness.
- Assessment of Configuration Management and Vulnerability Management policies.
- Case Study: Evaluating a healthcare provider?ÇÖs HIPAA policies concerning encryption and access to ePHI.

Module 4: Auditing Network and Cloud Security

- Reviewing Network Security Architecture.
- Cloud Security Auditing in AWS/Azure/GCP.
- Evaluating Third-Party/Vendor Risk and supply chain security policies.
- Auditing Wireless and Remote Access security policies and controls.
- Case Study: A company's data breach resulting from an un-audited, vulnerable cloud storage bucket

Module 5: Identity, Access Management, and Data Protection

- Auditing Identity and Access Management systems, including MFA and SSO.
- Evaluating the implementation of the Principle of Least Privilege.
- Technical auditing of Data Encryption policies.
- Assessing controls around Data Loss Prevention and Data Masking.
- Case Study: Auditing a new Zero Trust implementation and its impact on employee workflows.

Module 6: Incident Management and Business Continuity Auditing

- Auditing the organization's Incident Response Plan and testing procedures.
- Reviewing Disaster Recovery and Business Continuity Planning.

- Assessing the effectiveness of Security Information and Event Management and log analysis.
- Audit of the Security Awareness Training program for human risk mitigation.
- Case Study: Post-mortem audit of a simulated Ransomware incident to find gaps in the IR plan.

Module 7: Audit Tools, Reporting, and Communication

- Introduction to key Security Auditing Tools
- Developing clear, evidence-based Audit Findings and Risk Ratings.
- Structuring and writing the final Security Audit Report for executive management.
- Techniques for effectively communicating Cyber Risk and gaining buy-in for remediation.
- Case Study: Preparing a detailed Executive Summary for the Board of Directors following a critical infrastructure audit.

Module 8: Professional Ethics, Legal, and Future Trends

- Professional ethics and the IS Auditor's Code of Conduct.
- Legal and liability issues in Information Assurance.
- Introduction to auditing AI/Machine Learning and IoT security.
- Continuous Auditing and security maturity model development.
- Case Study: Ethical considerations when discovering a colleague's violation of the Code of Professional Ethics during an internal audit.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com 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
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

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

Register Online Now

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