Training Course on Auditing and Monitoring Data Protection Compliance

Professional Development Training Course Outline

Category	Data Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s digital-first world, data protection compliance has become a cornerstone of organizational integrity and consumer trust. As data privacy regulations like the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) continue to evolve, businesses must adapt by implementing robust auditing and monitoring protocols. Training Course on Auditing and Monitoring Data Protection Compliance provides participants with the essential tools to understand, implement, and evaluate data protection frameworks, empowering professionals to ensure organizational accountability and legal compliance.

This training program targets professionals in compliance, IT governance, cybersecurity, and risk management roles. It addresses the increasing demand for real-time monitoring, compliance auditing tools, and privacy impact assessments (PIA) to ensure lawful processing of personal data. Participants will engage in hands-on learning, analyze real-life case studies, and apply best-in-class frameworks to identify risks and close compliance gaps effectively.

Programme Curriculum

Training Course on Auditing and Monitoring Data Protection Compliance

Introduction

In today’s digital-first world, data protection compliance has become a cornerstone of organizational integrity and consumer trust. As data privacy regulations like the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) continue to evolve, businesses must adapt by implementing robust auditing and monitoring protocols. Training Course on Auditing and Monitoring Data Protection Compliance provides participants with the essential tools to understand, implement, and evaluate data protection frameworks, empowering professionals to ensure organizational accountability and legal compliance.

This training program targets professionals in compliance, IT governance, cybersecurity, and risk management roles. It addresses the increasing demand for real-time monitoring, compliance auditing tools, and privacy impact assessments (PIA) to ensure lawful processing of personal data. Participants will engage in hands-on learning, analyze real-life case studies, and apply best-in-class frameworks to identify risks and close compliance gaps effectively.

Course Objectives

1. Understand key principles of data protection regulations (GDPR, CCPA, etc.)
2. Conduct comprehensive privacy audits and internal compliance assessments.
3. Analyze data flows to detect privacy risks and vulnerabilities.
4. Learn audit trail creation and log monitoring techniques.
5. Develop and evaluate privacy compliance dashboards.
6. Implement effective data lifecycle management strategies.
7. Understand roles of Data Protection Officers (DPOs) in audit readiness.
8. Evaluate and improve vendor data processing practices.
9. Apply automated tools for privacy monitoring and auditing.
10. Conduct and document Data Protection Impact Assessments (DPIA).
11. Use compliance scorecards for ongoing regulatory benchmarking.
12. Respond to and document data breaches and incidents effectively.
13. Integrate continuous monitoring for proactive compliance management.

Target Audience

1. Data Protection Officers (DPOs)
2. Compliance and Risk Managers
3. IT Auditors and Internal Auditors
4. Cybersecurity Professionals
5. Legal and Regulatory Advisors
6. Data Governance Specialists
7. Privacy Consultants
8. Information Security Officers

Course Duration: 10 days

Course Modules

Module 1: Introduction to Data Protection Laws

- Overview of GDPR, CCPA, LGPD, and global frameworks
- Core principles of data protection
- Roles and responsibilities in compliance
- Personal data vs. sensitive data
- Lawful basis for data processing
- **Case Study**: GDPR Violation – Google France €50M Fine

Module 2: Understanding Audit Frameworks

- What is a privacy audit?
- Internal vs. external audits
- Risk-based audit planning
- Mapping compliance to business processes
- Tools for privacy audits
- **Case Study**: Facebook’s Data Audit Failures

Module 3: Building Audit Checklists

- Audit checklist templates
- Data mapping essentials
- Consent management review
- Third-party vendor audits
- Audit sampling and evidence collection
- **Case Study**: Marriott International Breach Audit

Module 4: Monitoring Tools and Technologies

- Real-time monitoring platforms
- Log management systems
- Alerts and automated triggers
- Integration with SIEM tools
- Key performance indicators (KPIs)
- **Case Study**: Capital One Cloud Monitoring Gaps

Module 5: Conducting Data Protection Impact Assessments

- When to conduct a DPIA
- Steps of a DPIA
- Stakeholder involvement
- DPIA report structure
- Tools for automated DPIA
- **Case Study**: NHS COVID-19 App DPIA

Module 6: Vendor and Third-Party Compliance Audits

- Vendor risk classification
- Privacy clauses in contracts
- Due diligence questionnaires
- Monitoring subcontractor compliance
- Breach liability assessment
- **Case Study**: Zoom and Third-Party Data Sharing

Module 7: Role of the Data Protection Officer (DPO)

- DPO responsibilities in audits
- Independence and reporting lines
- Documentation and recordkeeping
- Cross-border data transfer oversight
- Balancing DPO with business needs
- **Case Study**: DPO Role in LinkedIn’s Compliance

Module 8: Managing Data Subject Rights (DSARs)

- Overview of DSAR obligations
- Verification and response timelines
- Redaction and data extraction tools
- DSAR workflow automation
- Challenges in large-scale DSARs
- **Case Study**: Uber’s Response to DSAR Complaints

Module 9: Audit Trails and Data Logs

- Importance of audit logs

- Log retention policies
- Detecting anomalies
- Logging for different platforms
- Compliance documentation from logs
- **Case Study**: Equifax Breach Audit Trail Analysis

Module 10: Developing Compliance Dashboards

- What makes a good compliance dashboard
- Metrics for privacy compliance
- Role-based access to dashboards
- Integration with BI tools
- Visualization of risk levels
- **Case Study**: Microsoft 365 Compliance Center

Module 11: Breach Management and Response

- Identifying a data breach
- Notification obligations
- Root cause analysis
- Communication strategy
- Remediation actions
- **Case Study**: T-Mobile Breach Response Protocol

Module 12: Documentation and Reporting Standards

- Record of Processing Activities (RoPA)
- Retention schedules
- Training logs and compliance reports
- Incident documentation
- Preparing for regulatory inspections
- **Case Study**: British Airways ICO Report

Module 13: Internal Communication and Culture

- Privacy awareness programs
- Creating a culture of compliance
- Training vs. accountability
- Reporting mechanisms
- Cross-department collaboration
- **Case Study**: Apple’s Internal Privacy Culture Shift

Module 14: Certification and Industry Standards

- ISO/IEC 27701, SOC 2, and NIST
- Benefits of privacy certifications
- Compliance gap analysis
- Certification process overview
- Leveraging standards in audits
- **Case Study**: Shopify’s SOC 2 Certification Journey

Module 15: Future Trends and Emerging Risks

- AI and data privacy compliance
- Biometrics and facial recognition
- Smart devices and IoT monitoring

- Global harmonization of laws
- Predictive compliance analytics
- **Case Study**: TikTok and Facial Recognition Risks

Training Methodology

- Interactive presentations using real-world examples
- Group activities and role-playing audit scenarios
- Hands-on demonstrations of auditing tools
- Quizzes and knowledge checks per module
- Breakout sessions for brainstorming audit solutions
- Practical assignments with guided feedback

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

Start Date	End Date	Location	Price
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