Training Course on Legal and Regulatory Aspects of Incident Response

Professional Development Training Course Outline

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

Course Introduction

In today’s hyper-connected digital landscape, data breaches and cyber incidents are not just technological threats—they are serious legal liabilities. With global regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) setting the tone for stringent compliance standards, organizations must be equipped with legal knowledge and regulatory strategies to manage and respond to incidents effectively. Training Course on Legal and Regulatory Aspects of Incident Response is designed to help professionals align incident response plans with regulatory requirements, ensuring both proactive risk mitigation and rapid legal compliance when breaches occur.

This specialized training delves into the legal and regulatory frameworks governing data protection and cybersecurity, focusing on how organizations must respond under pressure. From breach notification obligations to consumer rights, cross-border data transfer laws, and litigation risks, you’ll learn how to navigate high-stakes incidents within the scope of laws such as GDPR, CCPA, HIPAA, and global data protection acts. Equip yourself with actionable strategies, real-world case studies, and compliance playbooks essential for every data privacy officer, legal counsel, CISO, and IT security leader.

Programme Curriculum

Training Course on Legal and Regulatory Aspects of Incident Response

Course Introduction

In today’s hyper-connected digital landscape, data breaches and cyber incidents are not just technological threats—they are serious legal liabilities. With global regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) setting the tone for stringent compliance standards, organizations must be equipped with legal knowledge and regulatory strategies to manage and respond to incidents effectively. Training Course on Legal and Regulatory Aspects of Incident Response is designed to help professionals align incident response plans with regulatory

requirements, ensuring both proactive risk mitigation and rapid legal compliance when breaches occur.

This specialized training delves into the legal and regulatory frameworks governing data protection and cybersecurity, focusing on how organizations must respond under pressure. From breach notification obligations to consumer rights, cross-border data transfer laws, and litigation risks, you'll learn how to navigate high-stakes incidents within the scope of laws such as GDPR, CCPA, HIPAA, and global data protection acts. Equip yourself with actionable strategies, real-world case studies, and compliance playbooks essential for every data privacy officer, legal counsel, CISO, and IT security leader.

Course Objectives

1. Understand the GDPR and CCPA breach notification requirements.
2. Identify legal responsibilities in incident response under global regulations.
3. Assess privacy compliance risks in cybersecurity incidents.
4. Execute data subject rights during and after a security breach.
5. Mitigate legal exposure in cross-border data incidents.
6. Map incident response plans to legal compliance frameworks.
7. Address third-party vendor breach liabilities legally.
8. Develop a regulatory communication strategy post-incident.
9. Prepare for privacy audits and compliance checks.
10. Understand data retention and destruction laws post-incident.
11. Utilize forensic evidence legally in regulatory investigations.
12. Analyze high-profile GDPR/CCPA legal case studies for best practices.
13. Build a legally compliant incident response policy tailored to your jurisdiction.

Target Audience

1. Chief Information Security Officers (CISOs)
2. Data Protection Officers (DPOs)
3. Legal Counsel & Compliance Officers
4. IT Security Managers
5. Privacy Consultants
6. Risk Management Professionals
7. Cybersecurity Auditors
8. Regulatory Affairs Managers

Course Duration: 10 days

Course Modules

Module 1: Overview of Data Protection Laws (GDPR, CCPA, etc.)

- Introduction to global data privacy laws
- Key legal terms and definitions
- Regulatory bodies and enforcement
- Differences and similarities between GDPR & CCPA
- Mapping legal requirements to incident response
- **Case Study:** Facebook-Cambridge Analytica data misuse

Module 2: Breach Notification Laws and Timelines

- GDPR's 72-hour notification rule
- CCPA consumer breach notification requirements
- Notification format and content guidelines
- Penalties for delayed or incorrect notifications

- Legal exceptions to breach reporting
- **Case Study:** Marriott International data breach

Module 3: Rights of Data Subjects During Incidents

- Right to access and erasure
- Data portability and correction
- Communication with affected users
- Handling user complaints and requests
- Coordinating with legal and IT teams
- **Case Study:** TikTok’s data rights compliance issue

Module 4: Legal Risk Assessment in Incident Response

- Identifying legal exposure points
- Tools for privacy risk analysis
- Mapping legal risk to technical risk
- Contractual and third-party considerations
- Legal risk prioritization strategies
- **Case Study:** Equifax breach legal fallout

Module 5: International Data Transfers and Legal Implications

- GDPR cross-border data rules
- Standard contractual clauses and alternatives
- Data localization laws
- Transfer impact assessments
- Regulatory authority cooperation
- **Case Study:** Schrems II case and its impact

Module 6: Third-Party Breach Liabilities

- Contractual clauses and responsibilities
- Vendor due diligence and legal coverage
- Shared responsibility matrix
- Breach reporting obligations across partners
- Insurance and liability management
- **Case Study:** Target’s vendor breach through HVAC system

Module 7: Legal Aspects of Digital Forensics

- Role of digital forensics in legal investigations
- Legal admissibility of evidence
- Chain of custody protocols
- Collaboration between legal and forensic teams
- Data integrity preservation
- **Case Study:** Capital One and legal forensic audits

Module 8: Creating a Legally Compliant IR Policy

- IR policy legal components
- Aligning IR with data protection laws
- Internal governance structure
- Documenting legal compliance procedures
- Communication protocols with regulators
- **Case Study:** Uber’s concealed breach and policy overhaul

Module 9: Communication with Regulators and Law Enforcement

- Legal obligations in regulator communication
- Structuring breach notifications
- Working with law enforcement during incidents
- Attorney-client privilege in IR communications
- Preparing compliance reports
- **Case Study:** Yahoo's regulatory reporting delay

Module 10: Preparing for Privacy Audits

- Audit triggers and scope
- Documentation requirements
- Internal audit readiness checklist
- Legal exposure areas in audits
- Closing audit findings
- **Case Study:** Google's GDPR audit in France

Module 11: Managing Litigation Risks

- Common litigation following breaches
- Legal defense strategies
- Class action management
- Role of legal counsel during incidents
- Avoiding punitive damages
- **Case Study:** T-Mobile breach litigation

Module 12: Incident Response Tabletop Exercises with Legal Focus

- Legal roles in tabletop drills
- Drafting legal-focused IR scenarios
- Capturing compliance documentation
- Role-playing regulatory communication
- Post-exercise legal analysis
- **Case Study:** Healthcare industry tabletop simulation

Module 13: Data Retention and Destruction Laws

- GDPR/CCPA data lifecycle requirements
- Legal hold versus deletion conflicts
- Secure data destruction standards
- Documentation for audit trails
- Updating IR policy for data lifecycle
- **Case Study:** Amazon Alexa data retention controversy

Module 14: Handling Insider Threats Legally

- Legal considerations of employee monitoring
- Employment law versus privacy rights
- Insider threat incident workflow
- Legal response planning for HR + Legal teams
- Disciplinary/legal actions and documentation
- **Case Study:** Tesla internal data leak

Module 15: Future Trends in Cybersecurity Law

- Emerging privacy laws (U.S. states, India, etc.)

- AI and privacy law intersections
- Legal aspects of zero trust frameworks
- Evolving role of DPO and legal counsel
- Compliance automation technologies
- **Case Study:** ChatGPT and AI privacy challenges

Training Methodology

- Interactive instructor-led sessions with live Q&A
- Real-world case study analysis and role-playing
- Downloadable templates and legal compliance checklists
- Quizzes and legal knowledge assessments
- Group discussions and privacy simulations
- Access to GDPR/CCPA legal resource library

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

Start Date	End Date	Location	Price
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