Cyber Law, Policy, and Compliance (NIST/ISO/GDPR) Training Course

Professional Development Training Course Outline

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

Course Introduction

Cyber law, policy, and compliance are critical components of modern digital governance, providing legal, technical, and procedural frameworks to secure information assets and ensure regulatory adherence. Organizations face increasing cyber threats, data breaches, and regulatory scrutiny, making it imperative for IT professionals, compliance officers, and managers to understand the legal frameworks, standards, and policies governing cybersecurity Cyber Law, Policy, and Compliance (NIST/ISO/GDPR) Training Course emphasizes the integration of global frameworks such as NIST, ISO 27001, and GDPR, enabling participants to identify regulatory obligations, assess risks, and implement effective compliance programs.

Participants will gain in-depth knowledge of cybercrime laws, privacy requirements, data protection standards, and incident response obligations. Through practical exercises, case studies, and policy analysis, learners will understand how to design, implement, and monitor compliance programs, mitigate cyber risks, and align organizational policies with international best practices. By the end of the course, participants will be equipped to lead cybersecurity governance initiatives, strengthen regulatory adherence, and foster a culture of digital risk awareness across their organizations.

Programme Curriculum

Cyber Law, Policy, and Compliance (NIST/ISO/GDPR) Training Course

Introduction

Cyber law, policy, and compliance are critical components of modern digital governance, providing legal, technical, and procedural frameworks to secure information assets and ensure regulatory adherence. Organizations face increasing cyber threats, data breaches, and regulatory scrutiny, making it imperative for IT professionals, compliance officers, and managers to understand the legal frameworks, standards, and policies governing cybersecurity Cyber Law, Policy, and Compliance (NIST/ISO/GDPR) Training Course emphasizes

the integration of global frameworks such as NIST, ISO 27001, and GDPR, enabling participants to identify regulatory obligations, assess risks, and implement effective compliance programs.

Participants will gain in-depth knowledge of cybercrime laws, privacy requirements, data protection standards, and incident response obligations. Through practical exercises, case studies, and policy analysis, learners will understand how to design, implement, and monitor compliance programs, mitigate cyber risks, and align organizational policies with international best practices. By the end of the course, participants will be equipped to lead cybersecurity governance initiatives, strengthen regulatory adherence, and foster a culture of digital risk awareness across their organizations.

Course Objectives

1. Understand international and national cyber laws affecting organizations.
2. Analyze GDPR compliance requirements for data protection and privacy.
3. Apply ISO 27001 standards to information security management systems.
4. Implement NIST cybersecurity framework for risk management and resilience.
5. Assess organizational cyber risk exposure and mitigation strategies.
6. Develop internal policies, procedures, and governance frameworks for compliance.
7. Conduct audits and assessments to ensure legal and regulatory adherence.
8. Design incident response and breach notification plans.
9. Integrate cybersecurity awareness and training programs for staff.
10. Evaluate third-party compliance and vendor risk management.
11. Monitor emerging cyber threats and evolving legal requirements.
12. Ensure ethical handling of data and privacy across digital platforms.
13. Develop strategic recommendations for cyber governance and policy improvement.

Organizational Benefits

- Strengthened legal and regulatory compliance
- Improved data protection and privacy management
- Reduced risk of cybercrime and data breaches
- Enhanced corporate governance and accountability
- Better incident response and business continuity
- Improved staff awareness and cybersecurity culture
- Strengthened vendor and third-party compliance
- Enhanced reputation and stakeholder trust
- Efficient risk assessment and mitigation practices
- Alignment with international standards and best practices

Target Audiences

- IT security professionals
- Compliance officers and risk managers
- Legal and regulatory advisors
- Data protection and privacy officers
- Governance and internal audit teams
- IT managers and operations staff
- Cybersecurity consultants
- Senior management and board members

Course Duration: 10 days

Course Modules

Module 1: Introduction to Cyber Law and Governance

- Overview of cyber laws and regulations globally
- Historical evolution of cyber governance
- Key definitions: cybercrime, data protection, privacy
- Roles of regulatory authorities and enforcement agencies
- Emerging trends in cyber legal frameworks
- Case Study: Cyber legal compliance failure in a multinational firm

Module 2: Understanding GDPR

- Key principles and scope of GDPR
- Rights of data subjects and obligations of controllers
- Data processing and consent requirements
- Cross-border data transfer regulations
- Penalties and enforcement mechanisms
- Case Study: GDPR breach and fine in a European organization

Module 3: ISO 27001 Overview

- Information security management systems (ISMS) concepts
- ISO 27001 standards and compliance requirements
- Risk assessment and treatment methodologies
- Policy development and documentation practices
- Certification process and auditing essentials
- Case Study: ISO 27001 certification journey of a financial institution

Module 4: NIST Cybersecurity Framework

- Core functions: Identify, Protect, Detect, Respond, Recover
- Implementation tiers and profiles
- Risk management and control selection
- Integration with existing security programs
- Continuous monitoring and improvement
- Case Study: NIST framework adoption in a government agency

Module 5: Cybercrime and Legal Implications

- Types of cybercrime: hacking, phishing, ransomware
- Criminal liability and prosecution procedures
- Legal remedies and sanctions
- International conventions and treaties
- Cybercrime reporting mechanisms
- Case Study: Legal action following a ransomware attack

Module 6: Privacy and Data Protection Policies

- Developing organizational privacy policies
- Data retention, classification, and usage rules
- Personal data handling and ethical considerations

- Employee awareness and responsibilities
- Monitoring and enforcement mechanisms
- Case Study: Policy implementation challenges in a bank

Module 7: Compliance Management Systems

- Establishing compliance frameworks
- Audit and assessment planning
- Documentation and reporting requirements
- Compliance performance metrics
- Continuous improvement and updates
- Case Study: Successful compliance management system adoption

Module 8: Risk Assessment & Management

- Identifying organizational cyber risks
- Conducting vulnerability assessments
- Risk mitigation and treatment strategies
- Quantitative and qualitative risk analysis
- Reporting risk findings to management
- Case Study: Cyber risk mitigation in a microfinance institution

Module 9: Incident Response & Breach Notification

- Developing incident response plans
- Roles and responsibilities during breaches
- Communication and reporting obligations
- Post-incident analysis and remediation
- Integrating lessons learned into policies
- Case Study: Data breach response in a tech firm

Module 10: Cybersecurity Awareness & Training

- Employee training programs for cyber risk mitigation
- Developing awareness campaigns
- Phishing simulations and tabletop exercises
- Evaluation of training effectiveness
- Continuous skill development
- Case Study: Staff awareness program reducing cyber incidents

Module 11: Third-Party & Vendor Compliance

- Evaluating vendor cyber risk
- Contractual obligations and monitoring
- Auditing third-party compliance
- Managing cloud service provider risks
- Integrating third-party oversight into governance
- Case Study: Vendor-induced breach and lessons learned

Module 12: Emerging Technologies and Legal Challenges

- AI, IoT, blockchain, and cloud implications

- Legal and regulatory considerations
- Risk assessment for new technology adoption
- Privacy impact assessments
- Policy updates for emerging threats
- Case Study: Legal compliance issues in IoT deployment

Module 13: Internal Audits and Continuous Compliance

- Planning internal cyber audits
- Audit methodologies and techniques
- Corrective actions and follow-ups
- Reporting audit findings to stakeholders
- Continuous improvement programs
- Case Study: Audit revealing systemic compliance gaps

Module 14: Cyber Governance & Organizational Culture

- Leadership role in cyber compliance
- Integrating cybersecurity into corporate governance
- Establishing accountability and reporting lines
- Promoting a culture of compliance and risk awareness
- Metrics for monitoring governance effectiveness
- Case Study: Governance improvement following a cyber audit

Module 15: Strategic Recommendations & Policy Implementation

- Developing actionable cyber policy recommendations
- Aligning policies with organizational goals
- Scaling compliance programs across the enterprise
- Measuring impact and effectiveness
- Long-term monitoring and review strategies
- Case Study: Strategic implementation of cyber policies in a multinational organization

Training Methodology

- Instructor-led presentations and discussions on cyber laws and standards
- Hands-on exercises with GDPR, ISO 27001, and NIST frameworks
- Case study analysis and group discussions
- Compliance audit simulations and policy drafting exercises
- Risk assessment and incident response tabletop exercises
- Action plan development for organizational implementation

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
02 Nov 2026	13 Nov 2026	Online	$2,000
02 Nov 2026	13 Nov 2026	Physical	$3,000
02 Nov 2026	13 Nov 2026	Physical	$6,000
02 Nov 2026	13 Nov 2026	Physical	$6,000
02 Nov 2026	13 Nov 2026	Physical	$12,000
02 Nov 2026	13 Nov 2026	Physical	$9,000
02 Nov 2026	13 Nov 2026	Physical	$12,000
02 Nov 2026	13 Nov 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