Cybersecurity Compliance and Framework 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

The rapidly escalating global threat landscape and the proliferation of stringent regulatory mandates like GDPR, HIPAA, and CCPA have made Cyber Risk Management a C-suite priority, not just an IT function. Organizations across all sectors face unprecedented pressure to demonstrate due diligence and maintain a strong Security Posture to avoid devastating Data Breaches, massive fines, and irreparable reputational damage. This demanding environment requires a new generation of professionals skilled in translating complex security standards into actionable, verifiable business processes. This is where the crucial nexus of Information Security and Governance, Risk, and Compliance (GRC) lies.

Cybersecurity Compliance and Framework Training Course moves beyond mere theoretical understanding, offering a practical, hands-on approach to mastering critical industry frameworks. The curriculum is focused on empowering participants to architect and enforce an effective Information Security Management System (ISMS) using globally recognized standards like NIST CSF 2.0 and ISO 27001. By focusing on real-world Incident Response planning, effective Vulnerability Management, and robust Third-Party Risk Management (TPRM), this training directly addresses the contemporary need for proactive, compliance-driven security leadership. Graduates will be prepared to champion a culture of security awareness and compliance, ensuring their organizations maintain operational resilience and adhere to the highest standards of Data Privacy and protection.

Programme Curriculum

Cybersecurity Compliance and Framework Training Course

Introduction

The rapidly escalating global threat landscape and the proliferation of stringent regulatory mandates like GDPR, HIPAA, and CCPA have made Cyber Risk Management a C-suite priority, not just an IT function. Organizations

across all sectors face unprecedented pressure to demonstrate due diligence and maintain a strong Security Posture to avoid devastating Data Breaches, massive fines, and irreparable reputational damage. This demanding environment requires a new generation of professionals skilled in translating complex security standards into actionable, verifiable business processes. This is where the crucial nexus of Information Security and Governance, Risk, and Compliance (GRC) lies.

Cybersecurity Compliance and Framework Training Course moves beyond mere theoretical understanding, offering a practical, hands-on approach to mastering critical industry frameworks. The curriculum is focused on empowering participants to architect and enforce an effective Information Security Management System (ISMS) using globally recognized standards like NIST CSF 2.0 and ISO 27001. By focusing on real-world Incident Response planning, effective Vulnerability Management, and robust Third-Party Risk Management (TPRM), this training directly addresses the contemporary need for proactive, compliance-driven security leadership. Graduates will be prepared to champion a culture of security awareness and compliance, ensuring their organizations maintain operational resilience and adhere to the highest standards of Data Privacy and protection.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Implement the NIST Cybersecurity Framework (CSF) 2.0 core functions to enhance organizational Cybersecurity Posture.
2. Design and Audit an Information Security Management System (ISMS) aligned with the requirements of ISO/IEC 27001:2022.
3. Assess and Mitigate Common Cloud Security and Multi-Cloud compliance risks, focusing on shared responsibility models.
4. Translate the mandates of major data privacy regulations, including GDPR and CCPA, into enforceable Data Protection policies.
5. Develop robust Incident Response and Disaster Recovery (DR) plans to ensure business continuity following a security breach.
6. Apply the Zero Trust Architecture (ZTA) principle to modernize Identity and Access Management (IAM) and network segmentation.
7. Conduct a comprehensive Risk Assessment and Gap Analysis against regulatory benchmarks.
8. Evaluate vendor risk and establish a defensible Third-Party Risk Management (TPRM) program for the modern Supply Chain.
9. Utilize continuous monitoring and SIEM (Security Information and Event Management) tools to maintain ongoing compliance and threat detection.
10. Analyze and report on an organization's security status for an SOC 2 audit to assure clients and stakeholders.
11. Establish an effective Vulnerability Management program that integrates compliance requirements with technical patching cycles.
12. Integrate Governance, Risk, and Compliance (GRC) technology platforms to automate policy enforcement and audit trails.
13. Communicate complex security risks and compliance requirements effectively to both technical teams and C-suite leadership.

Target Audience

1. IT & Security Professionals.
2. GRC (Governance, Risk, and Compliance) Specialists.
3. IT Auditors & Consultants.
4. Data Protection Officers.
5. IT/Security Managers.
6. C-Suite & Senior Leadership
7. Legal & Contract Professionals.
8. Business Continuity & Disaster Recovery Planners.

Course Modules

Module 1: Foundations of Cybersecurity GRC and Risk

- Defining Governance, Risk, and Compliance and its strategic role in the business.
- The three pillars of Information Security
- Understanding the legal, regulatory, and contractual drivers for compliance
- Introduction to the risk management lifecycle.
- Case Study: Analyzing a major financial institution's PCI DSS non-compliance penalty and the resulting fallout.

Module 2: Implementing the NIST Cybersecurity Framework (CSF 2.0)

- Deep dive into the five Core Functions.
- Mapping NIST CSF tiers to organizational maturity.
- Applying the NIST Risk Management Framework step-by-step for federal and critical infrastructure use.
- Using the Informative References section to cross-map with other standards
- Case Study: Utilizing NIST guidelines to recover from a Ransomware attack on a municipal utility.

Module 3: ISO 27001 and the ISMS

- The structure and requirements of ISO/IEC 27001:2022 and the development of an ISMS.
- The mandatory Annex A controls and the use of the Statement of Applicability
- The importance of Top Management commitment and the context of the organization.
- Conducting an internal audit program to maintain the ISO 27001 certification cycle.
- Case Study: A company achieving ISO 27001 certification, opening up new international market access and client trust.

Module 4: Global Data Privacy and Compliance

- Detailed review of the General Data Protection Regulation principles and lawful processing bases.
- Compliance with US State-level privacy laws, specifically the CCPA/CPRA and consumer rights.
- Implementing Privacy by Design and conducting Data Protection Impact Assessments
- Managing cross-border data transfers and compliance with specific regional data residency laws.
- Case Study: A tech firm facing a significant GDPR fine due to a lack of proper user consent mechanisms.

Module 5: Third-Party Risk and Supply Chain Security

- Identifying and classifying vendors based on access to Sensitive Data and criticality.
- Developing due diligence questionnaires and security requirements for vendor contracts.

- The role of frameworks like SOC 2 Type II reports in assuring vendor security controls.
- Continuous monitoring and lifecycle management of vendor relationships.
- Case Study: The analysis of a major Supply Chain Attack and the failure of upstream vendor risk assessment.

Module 6: Cloud and Modern Architecture Compliance

- The Shared Responsibility Model across IaaS, PaaS, and SaaS environments
- Applying security compliance controls in a dynamic cloud setting
- Implementation of Zero Trust Architecture principles for modern, borderless networks.
- Understanding and meeting regulatory requirements for data stored in multi-cloud environments.
- Case Study: A company that failed a compliance audit because it misunderstood its security obligations under the AWS Shared Responsibility Model.

Module 7: Detection, Incident Response, and Business Continuity

- Establishing a proactive Threat Detection and security monitoring program.
- Developing an effective and tested Incident Response Plan with clear roles and communication paths.
- Forensics readiness and maintaining chain of custody for legal and regulatory purposes.
- Integrating Disaster Recovery and Business Continuity Planning with the security strategy.
- Case Study: Reviewing the response of a major retailer to a Data Breach focusing on the speed of detection and public communication.

Module 8: Audit, Reporting, and GRC Automation

- Preparing for external audits and managing audit evidence.
- Key metrics and reporting for executive leadership and the Board on Cyber Risk.
- Introduction to GRC automation tools to streamline control mapping and compliance evidence collection.
- Strategies for building a sustainable, top-down security culture and awareness program.
- Case Study: Examining a successful SOC 2 Type II audit report and the subsequent business growth and trust gained.

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.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
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