Cybersecurity Planning and Policy 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

Cybersecurity Risk Management is no longer solely an IT concern; it is a critical Business Resilience imperative. In a landscape dominated by sophisticated Cyber Threats and stringent Regulatory Compliance, organizations must move beyond reactive defense to proactive, Strategic Planning and robust Policy Development. Cybersecurity Planning and Policy Training Course is engineered to equip current and future leaders with the essential knowledge and methodologies to forge a comprehensive Information Security strategy. By focusing on aligning security policies with overarching Organizational Objectives and fostering a strong Security Culture, participants will learn to build a Cyber Risk posture that is both effective and financially justifiable.

The dynamic nature of the digital environment including the rise of Cloud Computing, IoT Security, and AI-driven attacks demands a fresh approach to governance. This intensive training provides a deep dive into creating, implementing, and governing Enterprise Security Architecture and policies that mitigate risk, ensure Data Protection, and maintain business continuity. Graduates will be prepared to function as strategic partners, guiding their organizations through the complexities of Digital Transformation while establishing a clear, defensible, and compliant framework for managing their most critical digital assets.

Programme Curriculum

Cybersecurity Planning and Policy Training Course

Introduction

Cybersecurity Risk Management is no longer solely an IT concern; it is a critical Business Resilience imperative. In a landscape dominated by sophisticated Cyber Threats and stringent Regulatory Compliance, organizations must move beyond reactive defense to proactive, Strategic Planning and robust Policy Development. Cybersecurity Planning and Policy Training Course is engineered to equip current and future leaders with the essential knowledge and methodologies to forge a comprehensive Information Security

strategy. By focusing on aligning security policies with overarching Organizational Objectives and fostering a strong Security Culture, participants will learn to build a Cyber Risk posture that is both effective and financially justifiable.

The dynamic nature of the digital environment including the rise of Cloud Computing, IoT Security, and AI-driven attacks demands a fresh approach to governance. This intensive training provides a deep dive into creating, implementing, and governing Enterprise Security Architecture and policies that mitigate risk, ensure Data Protection, and maintain business continuity. Graduates will be prepared to function as strategic partners, guiding their organizations through the complexities of Digital Transformation while establishing a clear, defensible, and compliant framework for managing their most critical digital assets.

Course Duration

5 days

Course Objectives

1. Master methodologies for identifying, quantifying, and prioritizing Enterprise-Wide Cyber Risks and vulnerabilities.
2. Analyze and apply major global and industry-specific regulations to inform policy creation.
3. Design and implement security governance structures using frameworks like NIST Cybersecurity Framework and COBIT.
4. Develop a multi-year, strategic Information Security Roadmap aligned with core Business Objectives and digital transformation goals.
5. Craft clear, enforceable, and comprehensive Cybersecurity Policies.
6. Formulate and test a robust Security Incident Response Plan to ensure rapid and effective crisis management and Business Continuity.
7. Implement policies and controls for Data Lifecycle Management, Encryption, and protecting Personally Identifiable Information (PII).
8. Establish a program to assess and manage Supply Chain Security and the risks posed by vendors and outsourced services.
9. Create a program to build a proactive, organization-wide Security-First Culture to serve as the "human firewall."
10. Develop governance and security policies tailored specifically for Hybrid and Multi-Cloud environments.
11. Define key performance indicators (KPIs) and metrics to communicate the organization's Governance, Risk, and Compliance (GRC) posture to executive leadership.
12. Justify and allocate budget and human resources effectively for core security programs and high-priority initiatives.
13. Establish a continuous process for auditing, reviewing, and updating policies to adapt to Emerging Threats and technological changes.

Target Audience

1. Cybersecurity Managers/Directors.
2. Chief Information Security Officers (CISOs) and Aspiring CISOs role.
3. IT/Compliance/Audit Professionals.
4. Risk Managers.
5. Senior Business Leaders/Executives.
6. Policy Developers and Legal Counsel.
7. System Owners and Business Unit Managers.

8. Security Consultants.

Course Modules

Module 1: Foundations of Cybersecurity Strategy and Governance

- Mapping Cybersecurity to Organizational Objectives and business functions.
- Understanding the Governance, Risk, and Compliance triad.
- Case Study: Analyzing a major company's post-breach report to determine failures in governance and executive oversight.
- Introduction to core frameworks.
- Defining the roles and responsibilities of the CISO, Board, and employees in maintaining Security Posture.

Module 2: Advanced Cyber Risk Management and Assessment

- Conducting Quantitative and Qualitative Risk assessments.
- Developing a risk appetite and risk tolerance statement for executive approval.
- Case Study: Modeling the financial impact of a targeted ransomware attack and developing a corresponding mitigation plan.
- Methods for identifying and documenting critical assets and the impact of their compromise.
- Integrating cyber risk into the broader Enterprise Risk Management program.

Module 3: Policy Development and Lifecycle Management

- Principles of effective policy writing.
- Developing a hierarchical policy library.
- Case Study: Redrafting an ambiguous Bring Your Own Device policy to ensure compliance with data protection laws.
- The process for policy approval, communication, and mandatory employee acknowledgment.
- Strategies for maintaining policy relevance through regular review and version control.

Module 4: Regulatory Compliance and Legal Landscape

- Deep dive into mandatory global regulations and industry-specific acts
- Developing a Privacy Impact Assessment and a Data Protection Officer framework.
- Case Study: Simulating a regulatory audit by the ICO and demonstrating policy-driven compliance artifacts.
- Understanding international data residency requirements and cross-border data transfer policies.
- The legal implications of policy violations and non-compliance penalties.

Module 5: Policy for Data Protection and Information Lifecycle

- Developing a robust Data Classification Policy.
- Implementing policies for secure data storage, transit, processing, and destruction
- Case Study: Creating an acceptable use policy for Generative AI tools to prevent intellectual property leakage and ensure data sanitization.
- Policy requirements for strong Encryption and Key Management throughout the data lifecycle.
- Governance of access controls, including Role-Based Access Control and the principle of Least Privilege.

Module 6: Incident Response and Business Continuity Planning

- Building a structured Incident Response Team and defining their roles using the six phases of IRP.
- Developing a Communication Plan for internal stakeholders, law enforcement, and media during a breach.
- Case Study: Leading a live Tabletop Exercise simulating a nation-state sponsored attack, testing policy adherence and decision-making under pressure.
- Integrating IRP with Disaster Recovery and Business Continuity Planning to ensure resilience.
- Policy requirements for digital Forensics, evidence collection, and legally sound reporting.

Module 7: Cloud and Third-Party Risk Policies

- Developing a Cloud Adoption Framework and policies for IaaS, PaaS, and SaaS environments.
- Policy for Cloud Security Posture Management and Configuration Baselines.
- Case Study: Evaluating the security clauses and policy alignment of a major cloud service provider and a third-party application vendor.
- Strategies for continuous monitoring and auditing of vendor and Supply Chain Security.
- Creating a policy for secure application development and vulnerability management.

Module 8: Leadership, Metrics, and Policy Communication

- Translating technical security policy into executive-level risk and investment language.
- Developing a board-level Cybersecurity Dashboard using metrics like Mean Time to Detect and policy compliance rates.
- Case Study: Presenting a proposed security budget increase to a simulated Board of Directors, justifying the investment based on risk reduction.
- Techniques for overcoming organizational resistance and fostering a positive Security Culture
- Planning for continuous professional development and keeping the security team current on Emerging Threats.

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