Cybersecurity Governance Fundamentals Training Course

Professional Development Training Course Outline

Category	Corporate Governance	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The rapid evolution of digital technologies has transformed the corporate landscape, bringing unprecedented opportunities along with significant cybersecurity risks. Organizations are increasingly dependent on digital assets, making the need for robust cybersecurity governance critical. Cybersecurity Governance Fundamentals Training Course equips participants with essential knowledge and practical skills to design, implement, and manage effective cybersecurity frameworks aligned with organizational objectives. The course focuses on industry best practices, regulatory compliance, risk management, and strategic alignment of cybersecurity policies to protect sensitive data, ensure business continuity, and enhance stakeholder confidence.

This course provides a comprehensive understanding of the principles of cybersecurity governance, including risk assessment, policy development, incident management, and compliance frameworks. Participants will explore emerging cybersecurity threats, learn to implement strategic security controls, and understand the role of governance in reducing vulnerabilities. Through interactive case studies, practical exercises, and real-world scenarios, learners will gain actionable insights into integrating cybersecurity into organizational culture, improving decision-making processes, and enhancing overall security posture.

Programme Curriculum

Cybersecurity Governance Fundamentals Training Course

Introduction

The rapid evolution of digital technologies has transformed the corporate landscape, bringing unprecedented opportunities along with significant cybersecurity risks. Organizations are increasingly dependent on digital assets, making the need for robust cybersecurity governance critical. Cybersecurity Governance Fundamentals Training Course equips participants with essential knowledge and practical skills to design, implement, and

manage effective cybersecurity frameworks aligned with organizational objectives. The course focuses on industry best practices, regulatory compliance, risk management, and strategic alignment of cybersecurity policies to protect sensitive data, ensure business continuity, and enhance stakeholder confidence.

This course provides a comprehensive understanding of the principles of cybersecurity governance, including risk assessment, policy development, incident management, and compliance frameworks. Participants will explore emerging cybersecurity threats, learn to implement strategic security controls, and understand the role of governance in reducing vulnerabilities. Through interactive case studies, practical exercises, and real-world scenarios, learners will gain actionable insights into integrating cybersecurity into organizational culture, improving decision-making processes, and enhancing overall security posture.

Course Objectives

By the end of this course, participants will be able to:

1. Understand core principles of cybersecurity governance and frameworks.
2. Analyze organizational cybersecurity risks and develop mitigation strategies.
3. Implement regulatory compliance measures including ISO 27001, NIST, and GDPR.
4. Design cybersecurity policies aligned with business objectives.
5. Develop incident response and crisis management plans.
6. Identify and manage emerging cybersecurity threats.
7. Integrate risk management into strategic decision-making.
8. Establish accountability and roles for cybersecurity governance.
9. Enhance organizational resilience through continuous monitoring.
10. Apply ethical principles in cybersecurity management.
11. Foster cybersecurity awareness and training programs.
12. Evaluate third-party and supply chain cybersecurity risks.
13. Utilize technology tools to monitor, audit, and report security performance.

Organizational Benefits

- Strengthened cybersecurity posture across all business units
- Reduced risk of data breaches and financial loss
- Compliance with national and international regulations
- Improved stakeholder confidence and trust
- Enhanced decision-making for risk management
- Efficient allocation of cybersecurity resources
- Increased employee awareness and accountability
- Streamlined incident response and recovery processes
- Better alignment of IT and business strategies
- Access to industry best practices and case studies

Target Audiences

- Chief Information Security Officers (CISO)
- IT Managers and Security Officers
- Risk and Compliance Professionals

- Cybersecurity Analysts and Consultants
- Governance, Risk, and Compliance (GRC) Specialists
- Internal Audit Teams
- IT Project Managers
- Business Leaders responsible for digital assets

Course Duration: 5 days

Course Modules

Module 1: Introduction to Cybersecurity Governance

- Principles and frameworks of cybersecurity governance
- Governance vs. management roles
- Organizational cybersecurity culture
- Key performance indicators for governance
- Case Study: Implementing governance in a mid-sized organization
- Practical Exercise

Module 2: Risk Assessment and Management

- Identifying internal and external cybersecurity risks
- Risk assessment methodologies
- Prioritizing risks based on impact and likelihood
- Integrating risk into business strategy
- Case Study: Risk assessment in a financial institution
- Practical Exercise

Module 3: Regulatory Compliance and Standards

- ISO 27001, NIST, GDPR, and other regulations
- Compliance reporting and audits
- Policy development for regulatory adherence
- Penalties and risk mitigation strategies
- Case Study: GDPR compliance implementation
- Practical Exercise

Module 4: Policy Development and Implementation

- Security policies and procedures
- Aligning policies with business objectives
- Policy communication and enforcement
- Policy monitoring and updates

- Case Study: Developing cybersecurity policy for a multinational
- Practical Exercise

Module 5: Incident Response and Crisis Management

- Incident response planning
- Crisis communication strategies
- Investigation and reporting procedures
- Post-incident review and improvements
- Case Study: Responding to a ransomware attack
- Practical Exercise

Module 6: Emerging Cybersecurity Threats

- Overview of current cyber threats
- Malware, phishing, and advanced persistent threats (APT)
- Threat intelligence and monitoring tools
- Scenario analysis and mitigation strategies
- Case Study: Threat landscape assessment in healthcare
- Practical Exercise

Module 7: Third-Party and Supply Chain Security

- Managing third-party risks
- Vendor assessments and audits
- Contractual and legal considerations
- Continuous monitoring of supply chain security
- Case Study: Supply chain breach management
- Practical Exercise

Module 8: Strategic Integration and Reporting

- Integrating cybersecurity into strategic planning
- Key reporting metrics and dashboards
- Communicating risk to executives and board
- Continuous improvement strategies
- Case Study: Cybersecurity reporting for board oversight
- Practical Exercise

Training Methodology

- Interactive lectures and presentations
- Real-world case studies and scenario analysis
- Group discussions and brainstorming sessions
- Hands-on exercises and practical applications
- Role-playing for incident response simulations
- Assessment and feedback sessions

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

Start Date	End Date	Location	Price
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