Cyber Risk and Board Oversight 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

Cyber Risk and Board Oversight Training Course is designed to equip board members, executives, and senior management with comprehensive knowledge and practical skills to navigate the ever-evolving landscape of cyber threats. As organizations increasingly rely on digital infrastructures, understanding the implications of cybersecurity on corporate governance and strategic decision-making has never been more critical. This course emphasizes proactive risk management, regulatory compliance, and strategic oversight to safeguard organizational assets, reputation, and operational continuity. Participants will learn how to align cyber risk frameworks with organizational objectives, fostering a culture of resilience and informed decision-making.

In today's hyper-connected business environment, cyber threats are becoming more sophisticated and pervasive, demanding vigilant oversight from board members. This training course blends theoretical foundations with practical case studies to ensure participants can identify vulnerabilities, implement effective controls, and respond to incidents with precision. Through interactive sessions, participants will enhance their ability to evaluate risk, prioritize investments in cybersecurity, and integrate oversight responsibilities into board-level governance. By completing this course, board members will gain actionable insights to strengthen organizational resilience, enhance stakeholder confidence, and drive sustainable growth in the digital era.

Programme Curriculum

Cyber Risk and Board Oversight Training Course

Introduction

Cyber Risk and Board Oversight Training Course is designed to equip board members, executives, and senior management with comprehensive knowledge and practical skills to navigate the ever-evolving landscape of cyber threats. As organizations increasingly rely on digital infrastructures, understanding the implications of

cybersecurity on corporate governance and strategic decision-making has never been more critical. This course emphasizes proactive risk management, regulatory compliance, and strategic oversight to safeguard organizational assets, reputation, and operational continuity. Participants will learn how to align cyber risk frameworks with organizational objectives, fostering a culture of resilience and informed decision-making.

In today's hyper-connected business environment, cyber threats are becoming more sophisticated and pervasive, demanding vigilant oversight from board members. This training course blends theoretical foundations with practical case studies to ensure participants can identify vulnerabilities, implement effective controls, and respond to incidents with precision. Through interactive sessions, participants will enhance their ability to evaluate risk, prioritize investments in cybersecurity, and integrate oversight responsibilities into board-level governance. By completing this course, board members will gain actionable insights to strengthen organizational resilience, enhance stakeholder confidence, and drive sustainable growth in the digital era.

Course Objectives

1. Understand the evolving cyber threat landscape and its impact on organizational governance
2. Identify critical cyber risks relevant to board-level decision-making
3. Integrate cyber risk management into corporate strategy and operational oversight
4. Enhance knowledge of regulatory and compliance frameworks affecting cybersecurity
5. Develop frameworks for effective incident response and crisis management
6. Strengthen board-level oversight of cybersecurity initiatives and investments
7. Improve risk reporting and communication between IT teams and executives
8. Apply metrics and KPIs to monitor cybersecurity performance
9. Evaluate third-party and supply chain cyber risks
10. Promote a culture of cyber awareness across the organization
11. Explore emerging technologies and their cybersecurity implications
12. Assess organizational readiness for cyber incidents and breaches
13. Apply lessons from case studies to real-world organizational scenarios

Organizational Benefits

- Strengthened board-level understanding of cyber risk exposure
- Enhanced decision-making on cybersecurity investments and policies
- Improved regulatory compliance and reduced legal liabilities
- Increased resilience against cyber-attacks and data breaches
- Better integration of IT risk management into business strategy
- Stronger stakeholder confidence through proactive risk management
- Streamlined reporting and communication between board and IT teams
- Development of actionable cybersecurity dashboards and KPIs
- Reduction in financial losses due to cyber incidents
- Creation of a culture of cybersecurity awareness across all levels

Target Audiences

1. Board members and directors
2. Chief Executive Officers (CEOs)

3. Chief Information Security Officers (CISOs)
4. Chief Risk Officers (CROs)
5. IT governance professionals
6. Compliance and audit managers
7. Risk management professionals
8. Senior executives involved in strategic planning

Course Duration: 5 days

Course Modules

Module 1: Introduction to Cyber Risk and Governance

- Overview of cyber risk landscape and trends
- Role of boards in cybersecurity oversight
- Key frameworks and governance standards
- Cybersecurity maturity assessment
- Case study: Board response to ransomware attack
- Best practices for board-level risk discussions

Module 2: Regulatory and Compliance Requirements

- Global and regional regulatory frameworks
- Data privacy and protection laws
- Compliance monitoring and reporting
- Penalties and enforcement mechanisms
- Case study: GDPR breach and board accountability
- Strategies for continuous compliance

Module 3: Cyber Risk Identification and Assessment

- Risk identification methodologies
- Threat intelligence and monitoring
- Vulnerability assessment techniques
- Risk prioritization frameworks
- Case study: Third-party supply chain breach
- Creating actionable risk dashboards

Module 4: Incident Response and Crisis Management

- Cyber incident lifecycle
- Board responsibilities during incidents
- Communication strategies with stakeholders

- Contingency and recovery planning
- Case study: Major financial institution breach
- Lessons learned and corrective measures

Module 5: Cyber Risk Metrics and Reporting

- Key risk indicators (KRIs) for boards
- KPI development for cybersecurity
- Effective reporting formats
- Board dashboards and analytics
- Case study: Metrics-driven risk decision-making
- Continuous monitoring strategies

Module 6: Third-Party and Supply Chain Risk Management

- Assessing vendor cybersecurity posture
- Contractual and legal considerations
- Monitoring and auditing third parties
- Case study: Supply chain compromise
- Tools for ongoing risk evaluation
- Integrating supply chain risk into board oversight

Module 7: Emerging Cyber Threats and Technology Implications

- Cloud computing and cybersecurity challenges
- Artificial intelligence and machine learning threats
- IoT security considerations
- Case study: IoT device breach and board action
- Evaluating technology investment risks
- Strategic planning for future threats

Module 8: Creating a Cyber-Aware Organizational Culture

- Promoting awareness across all levels
- Training programs for employees
- Incentivizing cyber-safe behavior
- Monitoring behavioral compliance
- Case study: Cultural transformation in cybersecurity
- Aligning culture with risk governance

Training Methodology

- Interactive lectures and discussions
- Real-world case studies and scenario analysis
- Group exercises and workshops
- Hands-on risk assessment simulations
- Board-level decision-making exercises
- Expert-led Q&A sessions and feedback

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