Training Course on Board Oversight of Digital Transformation and Cybersecurity

Professional Development Training Course Outline

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

Course Introduction

In today's rapidly evolving business landscape, **Digital Transformation** is no longer optional; it's a **strategic imperative**. Organizations globally are leveraging emerging technologies like **Artificial Intelligence (AI)**, **Cloud Computing**, and **Big Data** to innovate business models, enhance operational efficiency, and drive competitive advantage. However, this transformative journey inherently introduces complex **Cybersecurity Risks** and necessitates robust **Digital Governance**. Effective board oversight is paramount to navigate these dual challenges, ensuring that digital investments translate into sustainable growth while safeguarding critical assets and maintaining stakeholder trust. Boards must evolve their understanding beyond traditional IT oversight to embrace a proactive, strategic role in managing digital opportunities and mitigating cyber threats.

Training Course on Board Oversight of Digital Transformation and Cybersecurity is meticulously designed to equip board members and senior executives with the essential **knowledge and frameworks** required for effective **Board Oversight** in the age of **Digital Transformation** and escalating **Cybersecurity Threats**. We will delve into the intricate interplay between technological innovation and **Corporate Governance**, emphasizing the board's fiduciary duties in ensuring **Digital Resilience**, **Data Privacy**, and adherence to evolving **Regulatory Compliance**. Through practical insights and real-world case studies, participants will develop the **strategic acumen** to steer their organizations through complex digital initiatives, foster a **cyber-aware culture**, and build **sustainable competitive advantage** in the digital economy.

Programme Curriculum

Training Course on Board Oversight of Digital Transformation and Cybersecurity

Introduction

In today's rapidly evolving business landscape, **Digital Transformation** is no longer optional; it's a **strategic imperative**. Organizations globally are leveraging emerging technologies like **Artificial Intelligence (AI)**, **Cloud Computing**, and **Big Data** to innovate business models, enhance operational efficiency, and drive competitive advantage. However, this transformative journey inherently introduces complex **Cybersecurity Risks** and necessitates robust **Digital Governance**. Effective board oversight is paramount to navigate these dual challenges, ensuring that digital investments translate into sustainable growth while safeguarding critical assets and maintaining stakeholder trust. Boards must evolve their understanding beyond traditional IT oversight to embrace a proactive, strategic role in managing digital opportunities and mitigating cyber threats.

Training Course on Board Oversight of Digital Transformation and Cybersecurity is meticulously designed to equip board members and senior executives with the essential **knowledge and frameworks** required for effective **Board Oversight** in the age of **Digital Transformation** and escalating **Cybersecurity Threats**. We will delve into the intricate interplay between technological innovation and **Corporate Governance**, emphasizing the board's fiduciary duties in ensuring **Digital Resilience**, **Data Privacy**, and adherence to evolving **Regulatory Compliance**. Through practical insights and real-world case studies, participants will develop the **strategic acumen** to steer their organizations through complex digital initiatives, foster a **cyber-aware culture**, and build **sustainable competitive advantage** in the digital economy.

Course Duration

10 days

Course Objectives

1. Empower boards to align **digital transformation strategy** with overall business objectives and **organizational resilience**.
2. Enhance board understanding of **cybersecurity risk management frameworks**, including **NIST**, **ISO 27001**, and **CIS Controls**.
3. Provide insights into governing risks and opportunities associated with **Artificial Intelligence (AI) Governance**, **Generative AI**, **Cloud Security**, and **IoT Security**.
4. Strengthen board capacity to oversee **data privacy**, **data ethics**, **GDPR compliance**, and **data protection regulations**.
5. Develop **digital fluency** and **cybersecurity awareness** among board members to facilitate informed decision-making.
6. Equip boards to effectively oversee **cyber incident response planning**, **breach management**, and **business continuity**.
7. Understand board responsibilities in overseeing **supply chain cyber risk** and **vendor cybersecurity assessment**.
8. Guide boards in making strategic **cybersecurity investment** decisions and optimizing **security spend**.
9. Ensure board understanding of evolving **cybersecurity regulations**, **disclosure requirements**, and **legal liabilities**.
10. Foster a board-led **cybersecurity culture** and promote **security-by-design** principles across the organization.
11. Enable boards to define and interpret relevant **cybersecurity metrics**, **KPIs**, and **boardroom reporting** for effective oversight.
12. Integrate **Environmental, Social, and Governance (ESG) principles** with digital transformation and cybersecurity strategies.
13. Prepare boards for effective **crisis communication** and reputation management in the event of a significant cyber incident.

Organizational Benefits

- Proactive identification and mitigation of cyber threats, ensuring business continuity and operational stability.
- Confident adoption of new technologies, driving innovation and market leadership.
- Comprehensive understanding and governance of digital and cyber risks across the enterprise.
- Demonstrates accountability, transparency, and a commitment to protecting stakeholder interests.
- Adherence to evolving data privacy and cybersecurity regulations, minimizing legal and financial penalties.
- Signals a well-governed organization prepared for future digital challenges.
- Intelligent investment in digital and cybersecurity initiatives with measurable ROI.
- Safeguarding brand image and customer trust in an increasingly interconnected world.
- Enables secure experimentation and deployment of transformative technologies.
- Embedding security as a shared responsibility across all levels of the organization.

Target Audience

1. Board of Directors (Executive & Non-Executive)
2. C-Suite Executives (CEO, CIO, CTO, CISO, CRO)
3. Company Secretaries
4. Audit and Risk Committee Members
5. Senior Legal and Compliance Professionals
6. Heads of Governance and Corporate Affairs
7. Aspiring Board Members
8. Senior Business Leaders Driving Digital Initiatives

Course Outline

Module 1: The Evolving Digital Landscape and Board Imperatives

- Understanding the velocity and breadth of **Digital Transformation (DX)**.
- Key **digital trends** impacting governance: AI, IoT, Cloud, Blockchain.
- The board's expanded fiduciary duties in the digital age.
- Shifting from reactive to **proactive digital governance**.
- Case Study: **Kodak's missed digital opportunity** - lessons in strategic foresight.

Module 2: Foundations of Cybersecurity Governance for Boards

- Core **cybersecurity concepts** and terminology for non-technical directors.
- Understanding the **threat landscape**: ransomware, APTs, insider threats.
- The difference between **cybersecurity management** and **board oversight**.
- Establishing **cyber risk appetite** and tolerance.
- Case Study: **Target Data Breach** - board accountability and oversight failures.

Module 3: Integrating Digital and Cyber Strategy

- Aligning DX initiatives with **cybersecurity strategy**.
- Developing a **digital vision** that incorporates security by design.
- The role of the board in defining **digital ethics** and responsible innovation.
- Resource allocation for secure digital transformation.
- Case Study: **Equifax Data Breach** - the cost of neglecting integrated security in large-scale data projects.

Module 4: Risk Management Frameworks and Board Reporting

- Overview of leading **cybersecurity frameworks** (NIST CSF, ISO 27001, COBIT).
- Effective **cyber risk assessment** and categorization.
- Designing **board-level cyber reporting** and dashboards.
- Translating technical risk into business language for the board.
- Case Study: **Colonial Pipeline Attack** - the importance of understanding OT/IT convergence risks.

Module 5: Governing Emerging Technologies: AI & Cloud

- **AI governance principles** and ethical considerations.
- Oversight of **Cloud adoption** risks and shared responsibility models.
- Managing the complexities of **Generative AI** and large language models (LLMs).
- Data sovereignty and international data transfer implications.
- Case Study: **ChatGPT's data privacy concerns** - navigating AI's ethical minefield.

Module 6: Data Governance, Privacy, and Compliance

- Board's role in establishing robust **data governance frameworks**.
- Navigating **global data privacy regulations** (GDPR, CCPA, PIPL).
- **Data classification**, retention, and destruction policies.
- Protecting sensitive **Personally Identifiable Information (PII)**.
- Case Study: **Cambridge Analytica/Facebook** - board responsibilities in data misuse and privacy breaches.

Module 7: Cybersecurity Incident Response & Business Continuity

- Board's role in **crisis management** and incident preparedness.
- Testing and validating the **Incident Response Plan (IRP)**.
- Communication protocols during and after a cyber incident.
- Ensuring **business continuity** and disaster recovery.
- Case Study: **Maersk NotPetya Attack** - demonstrating the need for comprehensive resilience.

Module 8: Third-Party & Supply Chain Risk Oversight

- Identifying and assessing **supply chain vulnerabilities**.
- **Vendor due diligence** and contractual security requirements.
- Continuous monitoring of third-party cybersecurity posture.
- Managing **Nth-party risks** in complex ecosystems.
- Case Study: **SolarWinds Supply Chain Attack** - profound impact of compromised vendors.

Module 9: Legal, Regulatory, and Disclosure Obligations

- Understanding **board legal liabilities** in cybersecurity.
- SEC, DORA, NIS2, and other relevant **cybersecurity regulations**.
- Effective **cyber risk disclosure** to investors and stakeholders.
- The evolving landscape of **cyber insurance**.
- Case Study: **Uber Data Breach & Cover-up** - legal ramifications and leadership accountability.

Module 10: Building a Cyber-Resilient Culture

- The board's role in fostering an organization-wide **cybersecurity culture**.
- Promoting **employee cyber awareness** and training.
- Incentivizing secure behaviors and discouraging risky practices.
- Developing a "speak up" culture for security concerns.
- Case Study: **Internal Threats at Tesla** - the human element in cybersecurity.

Module 11: Board Composition, Expertise, and Succession Planning

- Assessing current **board cybersecurity expertise**.
- Strategies for enhancing **digital literacy** within the boardroom.
- Considering the appointment of a **cyber expert director**.
- Succession planning for key technology and security roles.
- Case Study: **Equipping Boards with Cyber Expertise** - examples of companies adding cyber-savvy directors.

Module 12: Measuring and Monitoring Cybersecurity Performance

- Key **performance indicators (KPIs)** for cybersecurity.
- Effective metrics for measuring **cyber resilience**.
- Utilizing **cyber threat intelligence** for proactive defense.
- Regular reviews and audits of cybersecurity posture.
- Case Study: **IBM's Cost of a Data Breach Report** - understanding the financial impact of security failures.

Module 13: Crisis Communication and Reputation Management

- Developing a **crisis communication plan** for cyber incidents.
- Managing stakeholder expectations during a breach.
- Protecting organizational **reputation** and brand trust.
- Post-incident analysis and lessons learned.
- Case Study: **Sony Pictures Hack** - a masterclass in crisis communication (or lack thereof).

Module 14: Future Trends and Strategic Foresight

- Anticipating **future cyber threats** (e.g., Quantum computing impact).
- The convergence of **physical and cyber security**.
- Exploring **Web3** and the **Metaverse** from a governance perspective.
- The role of the board in **sustainable digital innovation**.
- Case Study: **Emerging threats to critical infrastructure** - preparing for future challenges.

Module 15: Practical Board Exercises & Action Planning

- **Tabletop exercises** simulating cyber incidents for board response.
- Developing a **board action plan** for digital and cyber oversight.
- Peer discussion and best practice sharing.
- Tools and resources for ongoing board development.
- Case Study: **Simulated Ransomware Attack** - real-time decision-making exercise for the board.

Training Methodology

This training course employs a highly interactive and practical methodology designed for senior leaders and board members. It combines:

- **Expert-Led Presentations:** Engaging sessions delivered by industry thought leaders and seasoned governance professionals.
- **Interactive Discussions:** Fostering peer-to-peer learning and knowledge exchange among participants.
- **Real-World Case Studies:** In-depth analysis of high-profile digital transformation initiatives and cybersecurity incidents.
- **Boardroom Simulations & Tabletop Exercises:** Practical application of concepts in a simulated crisis environment.
- **Group Exercises & Workshops:** Collaborative problem-solving and development of actionable strategies.
- **Q&A Sessions:** Opportunities for direct engagement with instructors and expert insights.
- **Pre-reading Materials:** Providing foundational knowledge to maximize in-class engagement.
- **Post-course Resources:** Curated materials for continued learning and 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
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 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