

Training Course on Digital Trust and Identity Management for CEOs

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

Training Course on Digital Trust and Identity Management for CEOs outlines a critical training program for Chief Executive Officers (CEOs) focusing on **Digital Trust** and **Identity Management**. In an increasingly interconnected and data-driven world, establishing and maintaining **digital trust** is no longer a mere technicality but a strategic imperative. This course empowers CEOs to navigate the complex landscape of **cybersecurity risks**, **data privacy regulations**, and **digital identity verification**, ensuring their organizations not only survive but thrive in the digital economy. We delve into cutting-edge strategies for **secure digital transformation**, **identity governance**, and building **customer confidence** in a **zero-trust** environment, directly impacting brand reputation, operational efficiency, and long-term business sustainability.

The program addresses the pressing need for **executive leadership** to grasp the strategic implications of robust **digital identity frameworks** and **trust architectures**. From mitigating **cyber threats** and ensuring **regulatory compliance** (e.g., GDPR, CCPA) to leveraging **decentralized identity (DID)** and **AI-driven security**, this course provides actionable insights for senior leaders. Participants will gain a holistic understanding of how **identity-centric security** underpins all digital interactions, fostering an organizational culture of **trust by design** and enhancing **digital resilience** against evolving cyber risks.

Programme Curriculum

Training Course on Digital Trust and Identity Management for CEOs

Introduction

Training Course on Digital Trust and Identity Management for CEOs outlines a critical training program for Chief Executive Officers (CEOs) focusing on **Digital Trust** and **Identity**

Management. In an increasingly interconnected and data-driven world, establishing and maintaining **digital trust** is no longer a mere technicality but a strategic imperative. This course empowers CEOs to navigate the complex landscape of **cybersecurity risks**, **data privacy regulations**, and **digital identity verification**, ensuring their organizations not only survive but thrive in the digital economy. We delve into cutting-edge strategies for **secure digital transformation**, **identity governance**, and building **customer confidence** in a **zero-trust** environment, directly impacting brand reputation, operational efficiency, and long-term business sustainability.

The program addresses the pressing need for **executive leadership** to grasp the strategic implications of robust **digital identity frameworks** and **trust architectures**. From mitigating **cyber threats** and ensuring **regulatory compliance** (e.g., GDPR, CCPA) to leveraging **decentralized identity (DID)** and **AI-driven security**, this course provides actionable insights for senior leaders. Participants will gain a holistic understanding of how **identity-centric security** underpins all digital interactions, fostering an organizational culture of **trust by design** and enhancing **digital resilience** against evolving cyber risks.

Course Duration

10 days

Course Objectives

1. Equip CEOs with the strategic vision to champion **digital trust initiatives** across the enterprise.
2. Understand and implement robust **identity and access management (IAM)** and **privileged access management (PAM)** frameworks.
3. Develop proactive strategies to address advanced **persistent threats (APTs)**, **ransomware**, and **data breaches**.
4. Navigate complex global **data protection regulations** (GDPR, CCPA, eIDAS) and ensure ethical **data handling**.
5. Lead the transition towards a **zero-trust security model** for enhanced organizational security.
6. Evaluate the potential of **blockchain-based identity** and **self-sovereign identity** for future business models.
7. Optimize **customer experience** and **loyalty** through secure and seamless digital interactions.
8. Integrate **ethical AI principles** and **responsible innovation** into digital trust strategies.
9. Build trusted digital supply chains to mitigate risks and ensure operational continuity.
10. Secure cloud environments and implement effective **federated identity management**.
11. Establish advanced **threat intelligence** capabilities and robust **incident response plans**.
12. Effectively communicate **cyber risk posture** and **digital trust metrics** to the board and stakeholders.
13. Anticipate and adapt to emerging **digital identity trends** and **security technologies** (e.g., Post-Quantum Cryptography).

Organizational Benefits

- Build deep **customer trust** through transparent and secure data handling.
- Minimize the likelihood and impact of **cyberattacks**, **identity theft**, and **financial fraud**.
- Ensure adherence to stringent **data privacy laws**, avoiding hefty fines and legal repercussions.
- Streamline **identity verification processes**, reduce friction, and automate access controls.

- Foster a secure foundation for adopting new technologies like **AI**, **IoT**, and **cloud computing**.
- Differentiate the organization in the marketplace as a trusted and secure digital entity.
- Demonstrate robust **governance, risk, and compliance (GRC)** practices, attracting and retaining investors.

Target Audience

- Chief Executive Officers (CEOs)
- Chief Operating Officers (COOs)
- Chief Information Officers (CIOs)
- Chief Information Security Officers (CISOs)
- Board Members
- Senior Executive Leaders responsible for digital strategy
- Heads of Digital Transformation
- Heads of Risk Management

Course Outline

Module 1: The Strategic Imperative of Digital Trust for CEOs

- Defining Digital Trust in the Modern Enterprise
- The C-Suite's Role in Building and Maintaining Trust
- Impact of Digital Trust on Brand Value, Reputation, and Market Cap
- Beyond Compliance: Trust as a Competitive Differentiator
- **Case Study:** Equifax Data Breach – Lessons in Eroding Trust

Module 2: Foundations of Digital Identity

- Understanding Digital Identity vs. Physical Identity
- Components of a Robust Digital Identity Ecosystem
- Authentication, Authorization, and Accounting (AAA) Principles
- Challenges in Centralized Identity Systems
- **Case Study:** Target's Data Breach and Identity Compromise

Module 3: Identity and Access Management (IAM) for Executives

- Key Pillars of IAM: User Provisioning, Authentication, Authorization
- Single Sign-On (SSO) and Multi-Factor Authentication (MFA) Strategies
- Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC)
- Governing User Lifecycles from Onboarding to Offboarding
- **Case Study:** Colonial Pipeline Ransomware Attack – Understanding IAM Gaps

Module 4: Privileged Access Management (PAM) for Critical Assets

- Identifying and Securing Privileged Accounts
- Just-in-Time Access and Session Monitoring
- Vaulting and Rotation of Credentials
- Reducing the Attack Surface from Inside Threats
- **Case Study:** SolarWinds Supply Chain Attack – The Impact of Compromised Privileged Access

Module 5: The Zero Trust Security Model

- Principles of "Never Trust, Always Verify"
- Implementing Micro-segmentation and Least Privilege
- Continuous Verification and Adaptive Security
- Transitioning from Perimeter-Based Security to Zero Trust
- **Case Study:** Google's BeyondCorp Model for Zero Trust

Module 6: Data Privacy Regulations and Digital Identity

- Deep Dive into GDPR, CCPA, and Other Global Privacy Laws
- The Right to be Forgotten and Data Portability
- Data Minimization and Privacy by Design Principles
- Consent Management and Transparency in Data Handling
- **Case Study:** Meta (Facebook) and Cambridge Analytica Scandal – Privacy Mismanagement

Module 7: Customer Identity & Access Management (CIAM)

- Enhancing Customer Experience with Seamless Authentication
- Secure Customer Onboarding and Lifecycle Management
- Progressive Profiling and Consent Orchestration
- Balancing Security, Usability, and Privacy in CIAM
- **Case Study:** Marriott International Data Breach and Customer Trust

Module 8: Decentralized Identity (DID) and Blockchain

- Introduction to Self-Sovereign Identity (SSI)
- Blockchain's Role in Secure and Verifiable Credentials
- Advantages of Decentralized Identifiers and Verifiable Data
- Potential for Interoperable Global Digital Identity
- **Case Study:** Estonians' e-Residency Program and Digital Identity

Module 9: AI and Machine Learning in Digital Trust

- Leveraging AI for Anomaly Detection and Threat Prediction
- AI-Powered Fraud Detection and Identity Verification
- Ethical Considerations and Bias in AI Algorithms for Identity
- Balancing Automation and Human Oversight in Security
- **Case Study:** Deepfake Technology and Identity Fraud Risks

Module 10: Digital Risk Management and Incident Response

- Identifying and Assessing Digital Trust Risks
- Developing and Testing Comprehensive Incident Response Plans
- Business Continuity and Disaster Recovery Planning
- Communication Strategies During a Security Incident
- **Case Study:** Maersk's NotPetya Attack – Lessons in Resilience

Module 11: Building Trust in the Digital Supply Chain

- Assessing Third-Party Risk and Vendor Security
- Secure Software Development Lifecycle (SSDLIC)
- Identity Management Across Extended Ecosystems
- Ensuring Integrity of Data and Operations with Partners
- **Case Study:** Kaseya VSA Supply Chain Ransomware Attack

Module 12: Governing Digital Trust: Boardroom Imperatives

- Establishing Digital Trust as a Board-Level Priority
- Key Performance Indicators (KPIs) for Digital Trust
- Reporting Cyber Risk and Identity Posture to Stakeholders
- Legal and Fiduciary Responsibilities of the Board
- **Case Study:** Uber's Cover-up of a Data Breach and Board Accountability

Module 13: Future of Digital Identity & Emerging Technologies

- Quantum-Resistant Cryptography and its Implications
- Biometrics and Behavioral Biometrics in Authentication
- Digital Twins and Metaverse Identity
- Regulatory Foresight for Emerging Identity Paradigms
- **Case Study:** The Evolution of Passwords to Passwordless Authentication

Module 14: Developing a Digital Trust Strategy & Roadmap

- Assessing Current State and Defining Target State
- Creating a Phased Implementation Plan
- Resource Allocation and Budgeting for Digital Trust Initiatives
- Building a Culture of Security and Trust Across the Organization
- **Case Study:** Large Financial Institution's Multi-Year Digital Trust Transformation

Module 15: Leading the Trust Transformation

- Change Management for Digital Trust Adoption
- Effective Communication and Stakeholder Engagement
- Fostering a Security-First Mindset at All Levels
- Measuring Success and Continuous Improvement in Digital Trust
- **Case Study:** A Global Tech Company's Journey to Embed Digital Trust in its DNA

Training Methodology

This executive training course will employ a highly interactive and engaging methodology tailored for senior leaders, emphasizing practical application and strategic decision-making.

- **Interactive Workshops:** Facilitated discussions, group exercises, and collaborative problem-solving.
- **Real-World Case Studies:** In-depth analysis of high-profile incidents and successful implementations to extract actionable insights.
- **Peer-to-Peer Learning:** Opportunities for CEOs to share experiences, best practices, and challenges with their counterparts.
- **Expert-Led Sessions:** Presentations and Q&A with industry thought leaders, cybersecurity veterans, and regulatory experts.
- **Strategic Framework Development:** Guided sessions to help participants develop a tailored digital trust and identity management roadmap for their own organizations.
- **Scenario Planning & Simulation:** Practical exercises to simulate crisis situations and test incident response strategies.
- **Flipped Classroom Elements:** Pre-reading materials and short videos to maximize in-person engagement on complex topics.

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
21 Sep 2026	02 Oct 2026	Online	\$2,000
21 Sep 2026	02 Oct 2026	Physical	\$3,000
21 Sep 2026	02 Oct 2026	Physical	\$0
21 Sep 2026	02 Oct 2026	Physical	\$0
21 Sep 2026	02 Oct 2026	Physical	\$0
21 Sep 2026	02 Oct 2026	Physical	\$0

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Physical	\$0
21 Sep 2026	02 Oct 2026	Physical	\$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com