Fintech Security and Blockchain Risk Mitigation Training Course



16 - 20 Nov 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #CYB6586_88898

Course Introduction / Overview:

The rapid convergence of finance and technology has created a dynamic ecosystem ripe with innovation but also fraught with complex security challenges. This course provides a comprehensive exploration of the critical security and risk management principles essential for navigating the Fintech and blockchain landscapes. As financial services become increasingly digitized and decentralized, the need for robust security protocols and astute risk mitigation strategies has never been more critical. This program, offered by BIG BEN Training Center, is meticulously designed to move beyond theoretical concepts, offering practical, actionable insights. We will delve into the architectural intricacies of blockchain technology, drawing on foundational principles discussed by experts like Andreas M. Antonopoulos in works that illuminate distributed consensus and cryptographic security. Participants will learn to identify, assess, and counteract the unique threats facing digital assets, smart contracts, and decentralized applications. The curriculum covers everything from common attack vectors to the nuances of regulatory compliance, ensuring a holistic understanding of how to build and maintain a secure financial technology infrastructure in an era of constant evolution and emerging threats.

Target Audience / This training course is suitable for:

- Financial Technology (Fintech) Professionals.
- Blockchain Developers and Engineers.
- Cybersecurity Analysts and Consultants.
- Risk Management Professionals.
- Compliance Officers and Managers.
- IT Auditors and Security Assessors.
- Financial Regulators and Policymakers.
- Venture Capitalists and Investors in Fintech.
- Product Managers in the financial sector.
- Information Security Officers.

Target Sectors and Industries:

- Banking and Financial Services.
- Investment and Asset Management.
- Insurance (Insurtech).
- Cryptocurrency Exchanges and Wallet Providers.
- Technology and Software Development.
- Consulting and Professional Services.
- Governmental and Regulatory Bodies.
- Venture Capital and Private Equity.
- E-commerce and Payment Processing.

Target Organizations Departments:

- Information Technology (IT) and Security.
- Risk Management and Assessment.
- Compliance and Legal.
- Internal Audit.
- Product Development and Innovation.
- Finance and Treasury.
- Operations Management.
- Research and Development (R&D).

Course Offerings:

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

- Analyze the unique security threat landscape of Fintech and blockchain technologies.
- Identify common vulnerabilities in smart contracts and decentralized applications (dApps).
- Develop and implement comprehensive risk management frameworks for digital assets.
- Conduct thorough security audits and penetration tests on blockchain-based systems.
- Design robust incident response plans tailored to cryptocurrency and Fintech breaches.
- Navigate the complex regulatory environment, including AML, KYC, and data privacy laws.
- Evaluate the security of different consensus mechanisms and cryptographic protocols.
- Apply threat modeling techniques to proactively identify and mitigate potential risks.
- Understand the security implications of emerging trends like DeFi and NFTs.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and highly practical. We believe that mastering complex topics like Fintech security and blockchain risk requires more than passive listening. Therefore, this course is built around a blended learning approach that combines expert-led instruction with hands-on application. Participants will engage in detailed case study analyses of real-world security breaches, dissecting the attack vectors and the subsequent mitigation strategies. Interactive workshops and group discussions will encourage collaborative problem-solving, allowing attendees to explore diverse perspectives on regulatory and security challenges. The curriculum includes practical lab sessions where participants will use industry-standard tools to simulate security audits and vulnerability assessments in a controlled environment. Continuous feedback from the instructor ensures that each participant can grasp the core concepts and apply them effectively. This dynamic and engaging approach guarantees that attendees leave not just with knowledge, but with the confidence and skills to secure complex financial technology systems.

Course Agenda (Course Units):

Unit One: Foundations of Fintech and Blockchain Security

- Introduction to the Fintech Ecosystem.
- Fundamentals of Blockchain Technology and Cryptography.
- Core Principles of Information Security in Finance.
- The Modern Threat Landscape for Digital Finance.
- Understanding Public, Private, and Consortium Blockchains.
- Key Differences Between Traditional and Decentralized Security Models.
- Introduction to Digital Assets and Cryptocurrency Security.

Unit Two: Common Vulnerabilities and Attack Vectors

- Smart Contract Security and Common Exploits (e.g., Reentrancy).
- Analyzing Consensus Mechanism Attacks (e.g., 51% Attacks).
- Social Engineering, Phishing, and Scams in the Crypto Space.
- Security of Digital Wallets (Hot, Cold, and Custodial).
- Threats to Decentralized Applications (dApps) and Oracles.
- Network-Level Vulnerabilities and Sybil Attacks.
- Privacy and Anonymity Risks on Public Ledgers.

Unit three: Risk Management and Mitigation Frameworks

- Developing a Fintech and Blockchain Risk Assessment Methodology.
- Threat Modeling for Decentralized Systems.
- Best Practices for Secure Software Development Lifecycle (SSDLC).
- Conducting Smart Contract Audits and Code Reviews.
- Implementing Robust Key Management and Custody Solutions.
- Building an Effective Incident Response and Recovery Plan.
- Business Continuity and Disaster Recovery for Digital Assets.

Unit Four: Regulatory Compliance and Legal Aspects

- Anti-Money Laundering (AML) and Know Your Customer (KYC) in Crypto.
- Navigating Data Privacy Regulations (e.g., GDPR, CCPA).
- The Global Regulatory Landscape for Digital Assets.
- Legal Enforceability and Implications of Smart Contracts.
- Understanding the Role of Regulatory Sandboxes.
- Compliance as a Service (CaaS) in Fintech.
- Reporting Obligations and Working with Law Enforcement.

Unit Five: Advanced Security and Future Trends

- Introduction to Zero-Knowledge Proofs for Privacy.
- Security Considerations for Decentralized Finance (DeFi) Protocols.
- Non-Fungible Token (NFT) Security and Market Risks.
- The Emerging Threat of Quantum Computing to Cryptography.
- Advanced Persistent Threats (APTs) Targeting the Finance Sector.
- Forensic Analysis of Blockchain Transactions.
- Capstone Project: Designing a Security Architecture for a Fintech Solution.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As decentralized finance (DeFi) aims to eliminate intermediaries, how can we design security and regulatory frameworks that protect users without re-introducing the centralization it seeks to avoid?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by offering a holistic and forward-looking perspective that bridges the critical gap between technical cybersecurity, strategic risk management, and regulatory compliance. While many programs focus narrowly on one of these domains, our curriculum is uniquely structured to integrate all three, reflecting the multifaceted reality of securing the modern financial ecosystem. We move beyond purely theoretical discussions by grounding every module in practical, real-world applications and detailed case studies of significant security events. This emphasis on applied knowledge ensures that participants learn not just what the threats are, but how to practically architect defenses, conduct meaningful audits, and develop resilient incident response plans. Furthermore, the course is designed with an eye toward the future, dedicating significant time to emerging trends like DeFi security, NFT risks, and the long-term threat of quantum computing. This forward-thinking approach, facilitated by expert instructors at BIG BEN Training Center, equips professionals not only to solve today's challenges but also to anticipate and strategically prepare for the evolving threats of tomorrow.