



Post-Quantum Cryptography Migration Architecture Training Course

2 – 6 May 2027
Nairobi

Post-Quantum Cryptography Migration Architecture Training Course

Ref: 402_132742 **Date:** 2 – 6 May 2027 **Location:** Nairobi **Fees:** 4500 Euro

Overview

Post-Quantum Cryptography Migration Architecture Training Course is a five-day advanced course for architecture, security, PKI, risk, application, infrastructure, and transformation professionals who leave with a Quantum-Safe Transition Architecture Pack. The course connects threat exposure, cryptographic discovery, crypto-agility, target architecture, standards, suppliers, testing, governance, and phased delivery. Participants turn scattered cryptographic dependencies into a controlled migration design. Agile Leaders Training Center delivers this course on post-quantum cryptography migration architecture.

Who Should Attend

- Enterprise architecture functions responsible for target states and technology roadmaps
- Security architecture functions responsible for cryptographic patterns and risk controls
- PKI and identity functions responsible for keys, certificates, and trust services
- Application and infrastructure functions responsible for protocols, platforms, and dependencies
- Technology-risk and data-governance functions responsible for exposure and risk acceptance
- Procurement and transformation functions responsible for supplier readiness and delivery governance

The course assumes participants already work with enterprise security architecture and cryptographic services, and it leaves out quantum-computing theory, introductory cybersecurity, and algorithm coding.

Departments and Industries

The course supports post-quantum cryptography migration across regulated, digital, and infrastructure-dependent organizations.

- Cybersecurity, enterprise architecture, identity, and infrastructure departments
- Banking, insurance, payments, and financial-technology organizations
- Telecommunications, cloud, software, and managed-service providers
- Healthcare, energy, transport, and industrial organizations
- Procurement, technology risk, data governance, and transformation offices

Learning Objectives

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



- Analyze quantum exposure across data, systems, and cryptographic dependencies
- Build a governed cryptographic inventory and prioritization model
- Apply crypto-agility principles to target-state architecture
- Evaluate PQC standards, PKI, protocol, supplier, and interoperability impacts
- Compare migration patterns and phased transition options
- Assemble a tested quantum-safe roadmap and assurance pack

Course Agenda

Day 1: Quantum Exposure and Scope

- Quantum Threat and Data-Longevity Exposure Map
- Harvest-Now-Decrypt-Later Risk Scenario
- Business Service and Critical Data Classification Matrix
- Cryptographic Transition Scope and Boundary Canvas
- Quantum-Safe Governance and Accountability Framework

Day 2: Discovery and Prioritization

- Cryptographic Asset Discovery Method
- Algorithm, Key, Certificate, and Protocol Inventory Register
- Application, Infrastructure, and Third-Party Dependency Map
- Vulnerability, Criticality, and Migration Priority Scorecard
- Inventory Evidence and Ownership Control Log

Day 3: Target Architecture and Standards

- Crypto-Agility Capability and Maturity Model
- FIPS 203 ML-KEM Transition Decision Matrix
- FIPS 204 ML-DSA and FIPS 205 SLH-DSA Use-Case Grid
- PKI, Certificate, and Trust-Service Target Architecture
- Hybrid and Staged Cryptographic Transition Pattern

Day 4: Migration Delivery and Assurance

- Application and Infrastructure Migration Wave Plan
- Supplier Readiness and Contract Requirement Checklist
- Interoperability, Performance, and Failure Test Strategy
- Exception, Risk Acceptance, and Compensating-Control Register
- Transition Metrics, Assurance, and Executive Reporting Dashboard



Day 5: Quantum-Safe Architecture Practice

- Suggested Exercise: Cryptographic Inventory Prioritization
- Suggested Exercise: PKI and Application Target-State Design
- Suggested Exercise: Supplier and Interoperability Decision
- Suggested Exercise: Migration Wave and Risk Briefing
- Capstone Exercise: Quantum-Safe Transition Architecture Pack

Practical Exercises

The course uses suggested activities to convert cryptographic evidence into governed migration decisions.

- Suggested activity: prioritize cryptographic dependencies for a payment platform and long-lived healthcare records.
- Suggested activity: design a staged PKI and certificate transition for cloud and on-premises services.
- Suggested activity: assess supplier roadmaps and interoperability constraints across telecommunications and industrial systems.
- Suggested activity: present a migration roadmap with waves, tests, exceptions, risks, and assurance measures.

FAQs

Who suits post-quantum cryptography migration architecture training, and what does it assume?

Post-quantum cryptography migration architecture training suits architecture, security, PKI, risk, application, infrastructure, procurement, and transformation professionals who already work with enterprise security and cryptographic services.

How does post-quantum cryptography migration differ from quantum-computing training?

Post-quantum cryptography migration focuses on enterprise cryptographic exposure, architecture, standards, dependencies, testing, suppliers, and delivery governance, while quantum-computing training explains computational concepts and technologies.

Why does post-quantum cryptography migration require a cryptographic inventory?

A cryptographic inventory identifies algorithms, keys, certificates, protocols, libraries, systems, owners, data exposure, and dependencies so transition priorities and testing scope can be traced.

What does crypto-agility contribute to a quantum-safe transition?

Crypto-agility provides governed mechanisms to replace or reconfigure algorithms, keys, certificates, protocols, and implementations without redesigning every dependent service for each future change.



What belongs in a quantum-safe transition architecture pack?

A quantum-safe transition architecture pack contains exposure analysis, inventory, priorities, target patterns, standards decisions, PKI impacts, supplier requirements, migration waves, test strategy, exceptions, risks, assurance, and reporting measures.

Conclusion

Participants leave with a Quantum-Safe Transition Architecture Pack containing an exposure map, cryptographic inventory, priority model, target architecture, standards decisions, supplier controls, test strategy, roadmap, and assurance measures. The pack changes isolated remediation into a traceable enterprise transition. It supports controlled decisions across applications, infrastructure, PKI, procurement, and risk governance.