
Post-Quantum Cryptography Migration Training Course: Inventory, Agility and Roadmap

4 – 8 January 2027
Rome





Post-Quantum Cryptography Migration Training Course: Inventory, Agility and Roadmap

Ref: 651_32608 **Date:** 4 – 8 January 2027 **Location:** Rome **Fees:** 5500 GBP

Programme Summary

Post-quantum cryptography migration is the subject of this one-week training course for security, architecture and technology risk leaders at managerial level, ending in a migration roadmap pack for one organisation. Public-key protections that secure payments, identities and archived records may fail once capable quantum computers arrive, yet most organisations cannot say where those protections sit. The programme moves from the quantum threat to inventory, algorithm choice, crypto-agility and sequencing, applied to an organisation the participant selects. Mars Training Centre UK delivers this programme on post-quantum cryptography migration to mixed-organisation cohorts.

The Business Case

Data stolen today can be decrypted later, so information with a long life is exposed before any quantum computer exists. Replacing cryptography touches applications, devices, suppliers and contracts, and it cannot be finished at the last moment. Banks, health bodies and telecommunications operators that fix an inventory, a set of algorithm rules and a sequence now can spread the work over years and answer boards and auditors with evidence.

- Long-Life Data Exposure: Falls as systems are ranked by how long their data must stay confidential.
- Migration Cost Overruns: Fall as dependencies and supplier timelines are mapped before work is funded.
- Rework Risk: Falls as crypto-agility lets algorithms be replaced without redesigning each system.

Principles and Evidence Base

- NIST IR 8547 Transition to Post-Quantum Cryptography Standards: Frames the migration planning and sequencing built in Sessions 2 and 4.
- FIPS 203, FIPS 204 and FIPS 205: Supply the post-quantum algorithm standards compared in Session 3.
- Cryptographic Inventory Practice: Guides the discovery and scoring of algorithms, keys and certificates in Session 2.
- Crypto-Agility Principles: Shape the replaceable design patterns developed in Session 3.



Intended Participants

- Security leaders who own cryptographic policy and the risk of long-life data exposure.
- Enterprise and security architects who design the systems that depend on public-key cryptography.
- Technology risk managers who report migration progress to boards and auditors.
- Infrastructure and platform heads who run the certificates, keys and devices to be changed.
- Procurement and vendor managers who hold supplier commitments for upgraded products.

Typical functions include banks, health bodies, telecommunications operators and government digital agencies.

Learning Outcomes

1. Participants will be able to evaluate which data and systems face long-term exposure to future quantum attack.
2. Participants will be able to construct a cryptographic inventory that records algorithms, keys, certificates and owners.
3. Participants will be able to prioritise systems for migration using an exposure scoring matrix.
4. Participants will be able to compare replacement algorithms and hybrid patterns against performance and interoperability needs.
5. Participants will be able to design crypto-agility principles that allow later algorithm changes.
6. Participants will be able to justify a sequenced migration roadmap and its residual risks to a board.

Programme Structure

Day 1: Post-Quantum Cryptography Migration Foundations

Which of today's cryptographic protections could a quantum computer break, and by when does that matter?

- Quantum Threat Timeline Brief
- Public-Key Dependency Map
- Harvest-Now Exposure Test
- Data Lifetime Classification Sheet
- Migration Principles Register

Day 2: Cryptographic Inventory and Exposure Diagnosis

Where are algorithms, keys and certificates used, and which systems are most exposed?

- Cryptographic Inventory Template
- Certificate and Key Discovery Plan
- Vendor and Supply Chain Dependency Table
- Exposure Scoring Matrix
- Priority System Shortlist



Day 3: Algorithm Choice and Crypto-Agility Design

Which replacement algorithms and designs allow the next change without another rebuild?

- Standardised Algorithm Selection Table
- Hybrid Deployment Pattern
- Crypto-Agility Design Principles
- Performance and Interoperability Test Plan
- Key Management Change Outline

Day 4: Roadmap, Governance and Risk Decisions

How is the migration sequenced, funded and governed across many owners?

- Migration Wave Plan
- Dependency and Sequencing Chart
- Governance Role Map
- Residual Risk Register
- Board Briefing Outline

Day 5: Migration Roadmap Pack for One Organisation

Do the inventory, algorithm choices and sequencing support one migration decision?

- Applying the Session 2 Exposure Scoring Matrix
- Testing the Session 3 Standardised Algorithm Selection Table
- Reviewing the Session 4 Residual Risk Register
- Checking the Session 4 Migration Wave Plan
- Completing the Migration Roadmap Pack

Methodology

The programme uses a data workshop method built on a shared case of a payments and records environment with legacy applications, a certificate estate and several suppliers. Participants build each artefact on the case with prepared data, then adapt it to an organisation they know, receiving written facilitator feedback in every session.

- Suggested activity: Scoring twenty systems for exposure and agreeing a priority shortlist.
- Suggested activity: Comparing two algorithm options on performance and interoperability evidence.
- Suggested activity: Presenting a migration sequence to a mock technology risk committee.



Capstone Output

Each participant completes a migration roadmap pack for one organisation. It holds an inventory template, an exposure scoring matrix, an algorithm selection table, a migration wave plan and a residual risk register. The pack is used at work to open the inventory exercise, brief the board and set supplier requirements for upgraded products.

Frequently Asked Questions

Is post-quantum cryptography migration training suitable for leaders who are not cryptographers?

Yes. Post-quantum cryptography migration is taught through cases and templates, assuming responsibility for security, architecture or technology risk but no mathematical background in cryptography.

Which standards does post-quantum cryptography migration training rest on?

Post-quantum cryptography migration training rests on NIST IR 8547, FIPS 203, FIPS 204 and FIPS 205, together with cryptographic inventory practice and crypto-agility principles.

How is the roadmap pack from post-quantum cryptography migration training used at work?

You use the migration roadmap pack to start the inventory exercise, brief the board and set requirements for suppliers of upgraded products.

How does post-quantum cryptography migration differ from general cybersecurity training?

Post-quantum cryptography migration centres on replacing public-key protections in a planned sequence, while general cybersecurity training covers threats, controls and incident response across all systems.