QUANTUM SECURITY & PQC

Post-Quantum Foundation

FOUNDATIONAL COURSE

Understand the quantum threat, NIST algorithms and PQC migration. Build the foundation for informed decisions and the next step toward PQCS training.

DURATION

Half day

A focused introduction

LEVEL

Foundational

First course on the PQC track

PREREQUISITES

None

No prior quantum knowledge

Your entry point to post-quantum cryptography.

WHAT YOU WILL LEARN

- Explain quantum risks to RSA, ECC and Diffie-Hellman, including HNDL and TNFL.
- Describe the NIST algorithm suite and distinguish finalized standards from work still in standardization.
- Outline migration phases, regulatory drivers and the business case for starting now.
- Apply Mosca's inequality to migration timing while quantum-computer timelines remain uncertain.

WHO SHOULD ATTEND

Security professionals, IT managers, compliance officers, risk analysts, software developers, enterprise architects and business leaders.

STARTING KNOWLEDGE

No prior quantum computing or advanced cryptography knowledge is required.

First course on the Post-Quantum track

Your certificate of completion is required before PQCS Training. Foundation is not a certification or an exam-preparation course.

What you will study

Four modules for evidence-based conversations about post-quantum migration.

01 The Quantum Threat to Cryptography

What quantum computers can and cannot do. How Shor's algorithm threatens RSA and elliptic-curve cryptography, and why AES and hash functions are less affected. Distinguish quantum advantage demonstrations from cryptographically relevant capability. Explore harvest-now-decrypt-later (HNDL) risks to encrypted data and trust-now-forge-later (TNFL) risks to signatures, software updates, legal documents and financial transactions. Understand why both create urgency before a cryptanalytically relevant quantum computer (CRQC) exists.

02 NIST Post-Quantum Standards

ML-KEM for key encapsulation, ML-DSA for general-purpose signatures and SLH-DSA as a hash-based alternative are finalized standards. FN-DSA (formerly FALCON) remains in standardization as FIPS 206. HQC, selected by NIST in March 2025, is a code-based KEM in standardization. Explore intended uses, performance and deployment considerations, algorithmic diversity, and how to read the standards for planning conversations.

03 PQC Migration Overview

Follow the PQC Migration Framework from discovery and inventory through implementation, verification and operational handover. Understand why migrations take years: discovery, testing, vendor dependencies and coordination across interconnected systems. Learn where organizations start, how hybrid cryptography supports transition, and why migration becomes a permanent operational capability.

04 Regulatory and Market Drivers

Explore CNSA 2.0 and the January 2027 US acquisition gate; EU quantum-readiness initiatives, NIS2 and the EU Cybersecurity Act; financial-services drivers, the PCI DSS roadmap, GSMA guidance and NSM-10. Examine commercial pressure from insurance and client contracts, and distinguish compliance-driven from risk-driven migration. Exact obligations depend on jurisdiction, sector and system scope.

Recommended reading and practitioner perspective

Quantum Ready: the complete guide to PQC migration – a PDF copy is included.
PQC Migration Framework – the open-source methodology referenced throughout the course.
Built on the Applied Quantum PQC Migration Framework, published under Creative Commons at pqcframework.org and written by the practitioners who teach here. Instructors are running migration programs inside organizations today.

Plan your participation

Course formats and fees

Online on-demand	**US$349**
Live online	**US$529**
In person	**US$699**
Private team training	**Custom quote**

Private team training is quoted per engagement through training@quantumacademy.com. All prices are in US dollars.

What is included

- Course handbook and a PDF of the full material with written instructor notes, yours to keep.
- PDF copy of Quantum Ready, included at no extra cost.
- 180 days of online on-demand access, including with live online and in-person enrollment. Where that course is not yet published, the 180 days start on the day it is.

Foundation to PQCS bundles

On-demand bundle	**US$2,649**
In-person bundle	**US$3,999**

Each bundle includes Foundation, PQCS training in the selected format, and the PQCS exam. Foundation itself has no exam or professional credential.

Certificate of completion

Upon completion, you will receive a Quantum Academy certificate of completion. This is not a professional certification. It does not include an exam or a credential.

This course does not prepare you for hands-on implementation, migration planning, or any Quantum Academy certification exam.

YOUR NEXT STEP

Your certificate of completion is required before Post-Quantum Certified Specialist (PQCS) Training. An active PQCS certification then opens the Manager, Architect and Validator tracks.

Explore dates and enrollment

View Post-Quantum Foundation at QuantumAcademy.com

support@quantumacademy.com | +1 (312) 803-4969

155 N Wacker Dr, Suite 4250, Chicago, IL 60606

ABOUT THIS PROGRAM

Quantum Academy credentials are private professional credentials issued by Quantum Academy, a trade name of Post-Quantum Institute. They are not government-issued licenses, accredited degrees, or academic credit, and earning one does not guarantee employment, promotion, regulatory approval, or any other specific outcome.

Quantum Academy programs are educational and informational only, and are not legal, compliance, or engineering advice.