

QUANTUM COMPUTING SECURITY

# Quantum Computing Security Professional

QCSP TRAINING

Protect quantum computing infrastructure across control systems, firmware, cloud platforms and the supply chain.

ON DEMAND

~40 hours

Self-paced

LIVE TRAINING

24 hours

Across four days

LEVEL

Advanced

Certification preparation

## Secure the quantum computing system.

WHAT YOU WILL LEARN

- ✓ Map the attack surface and threat-model quantum computing infrastructure.
- ✓ Assess control systems, firmware and calibration-data security.
- ✓ Evaluate cloud access, isolation, APIs and quantum-HPC interfaces.
- ✓ Assess physical protection and specialized supply-chain dependencies.

WHO SHOULD ATTEND

Cybersecurity professionals, security architects, SOC analysts, penetration testers, cloud security engineers, and defense or government security specialists.

PREREQUISITES

None. A security background is recommended. CQTP and Post-Quantum Track credentials are not required.

### Preparation for the QCSP certification

Completing training does not confer the credential. You must pass the separate exam.

# What you will study

Seven modules connecting core concepts with applied professional decisions.

## 01 The Attack Surface of a Quantum Computer

Map threat actors, sensitive circuit designs and computation results. Identify attack vectors across the classical infrastructure supporting a quantum computer.

## 02 Classical Control System Security

Assess pulse generators, signal routing, readout and control electronics. Design network segmentation, monitoring and anomaly detection for the control plane.

## 03 Firmware and Signal Chain Security

Evaluate firmware updates, calibration integrity and component provenance. Assess how manipulation can affect computation quality and identify verification approaches.

## 04 Cloud Quantum Platform Security

Review authentication, APIs, job isolation, multi-tenancy and data handling. Assess audit logging, resource abuse and denial-of-service risks.

## 05 Quantum-HPC Integration Security

Secure job submission, compilation and classical pre- and post-processing. Protect sensitive circuit designs, communications and result integrity.

## 06 Physical and Facility Security

Assess access controls and environmental monitoring for quantum facilities. Address insider threats and the protection requirements of different deployment models.

## 07 Supply Chain and Vendor Security

Evaluate specialized suppliers, component concentration and vendor security. Assess dependencies in cryogenics, control electronics and materials, including geopolitical constraints.

### Applied learning

The course draws on Quantum Systems Integration by Marin Ivezic and faculty experience with quantum engineering. Its focus is protecting quantum computers and their supporting infrastructure.

# Plan your participation

## Training formats and fees

|                       |              |
|-----------------------|--------------|
| Online on-demand      | US\$2,499    |
| Live online           | US\$2,999    |
| In person             | US\$3,499    |
| Private team training | Custom quote |

Live online and in-person delivery: four days, six hours of instruction per day. On-demand delivery: approximately 40 hours at your own pace.

Includes a certificate of completion. This is not a professional certification.

## Included with training

- Course handbook with the full material and written instructor notes.
- PDF copy of Quantum Systems Integration by Marin Ivezić, included at no extra cost.
- 180 days of online on-demand access. Where that course is not yet published, the 180 days start on the day it is.

## Training and exam options

|                  |           |
|------------------|-----------|
| On-demand + exam | US\$2,999 |
| In-person + exam | US\$3,999 |
| Exam only        | US\$699   |

Training-only fees exclude the exam. Select a bundle to include the certification assessment.

## The QCSP exam

120 questions: 110 scored + 10 unscored pilot items.

180 minutes; closed book; proctored.

Multiple-choice and scenario questions.

Passing score: 700 on a 100-900 scale.

Plan 30-50 hours of independent study in addition to the course.

## After certification

Explore The Quantum Threat: Technical Deep Dive for cryptanalytic risk. PQCA addresses migration design and requires an active PQCS credential.

Three-year validity. US\$149 annual maintenance covers all active Quantum Academy credentials. See the [credential page](#) for renewal and exam terms.

## Explore dates and enrollment

View the QCSP program at [QuantumAcademy.com](https://QuantumAcademy.com)



On-demand enrollment opens soon. Check the course page for live dates and availability.

[support@quantumacademy.com](mailto:support@quantumacademy.com) | +1 (312) 803-4969 | [training@quantumacademy.com](mailto:training@quantumacademy.com) (teams)

Prices: September 2026; applicable taxes are shown at checkout. Quantum Academy credentials are private professional credentials of Post-Quantum Institute, not government-issued licenses, accredited degrees or academic credit. No employment, promotion, regulatory approval or specific outcome is guaranteed. Programs are educational and informational only, not legal, compliance or engineering advice.