

The quantum-cyber risk is not a future problem. It is a present-day decision. Sensitive data collected today can be harvested now and decrypted later, once quantum capabilities mature. Organizations that identify their exposure and begin acting now hold a readiness advantage while others remain exposed. This series prepares government, enterprise, and technical teams to do exactly that, in plain language, without requiring anyone to become a quantum physicist.

Three courses. One readiness model.

Course 1 builds the vocabulary. Course 2 makes the risk urgent and personal. Course 3 turns it into engineering and governance you can act on. The series is sequenced to move a learner from awareness to execution. Professional Certificates are included with Courses 2 and 3.

WHY THIS MATTERS NOW

- **Harvest now, decrypt later.** Long-life data (customer records, intellectual property, regulated and government-related information) is exposed by decisions made today.
- **Standards and deadlines are set.** NIST has finalized the post-quantum standards (FIPS 203, 204, 205), with federal migration targeted through 2030 to 2035. The clock is running.
- **Early action is a differentiator.** Organizations that inventory vulnerable systems, prioritize sensitive data, and plan migration now will be positioned ahead of those forced into a rushed response later.
- **Practical, not academic.** The goal is not to turn people into quantum scientists. It is to help leaders and technical professionals understand what is changing, why it matters, and what to prepare for.

THE SECUREFI READINESS MODEL

Every course is built on the SecureFi Readiness Model, designed for professionals who must act under uncertainty rather than memorize facts. Each concept is paired with a decision, a moment of reflection, and an AI-supported prompt the learner can run against their own environment. Learners do not just read about quantum-aware risk; they apply each concept to their own organization and take real findings back to work the same day.

COURSE 1

Introduction to Quantum for Government & National Security

Foundational awareness. Offered free.

A plain-language foundation in quantum computing for leaders and professionals, with no physics background required. It explains what quantum computing is and is not, why governments and industry are investing now, and where the technology affects cybersecurity, national security, critical infrastructure, and long-term planning. Learners finish able to separate realistic developments from hype and to participate confidently in planning conversations.

Best for:

- Government and enterprise leaders, program managers, policy and acquisition staff
- Technical professionals who want strategic context before Courses 2 and 3

Level	Foundational
Format	Self-paced, SecureFi Readiness Model
Certificate	Certificate of Completion included
Price	Free

COURSE 2

Quantum-Aware Cyber Risk: Harvest Now, Decrypt Later

Advanced. Professional Certificate.

A structured, application-level view of harvest-now-decrypt-later exposure. Learners work through a five-step assessment to find long-life data, map cryptographic dependencies across identity, APIs, storage, backups, and vendors, score migration urgency, and sequence remediation toward the FIPS 203/204/205 standards. The course produces a reusable exposure profile and findings register the learner keeps.

Best for:

- CISOs, security and risk leaders, cyber professionals, enterprise and solution architects
- Executives who must understand long-life data exposure and brief on migration planning

Included Professional Working Guide. 61 AI-assisted assessment prompts, a reusable application profile, a five-step workflow, and a findings register, so learners can run an authorized assessment in their own approved AI environment.

Level	Advanced
Format	Self-paced, SecureFi Readiness Model
Assessment	40-question professional assessment, 80% to pass
Certificate	SecureFi Institute Professional Certificate
Price	\$299 per learner, volume pricing available

COURSE 3

Cyber-Ready: Trusted Systems Engineering

Most advanced. Professional Certificate.

The most advanced course in the series. It expands from encryption to the full question of system trust across 12 domains, in an environment shaped by AI acceleration, post-quantum transition, and adversaries already mapping the trust chain. Eighteen modules, each anchored to a real adversary case (SolarWinds, NotPetya, MOVEit, Equifax, Volt Typhoon, and others), build toward a Trust Chain assessment and a 90-day roadmap with named owners.

Best for:

- Technical staff, security and platform engineers, and architects responsible for system trust
- Security leads navigating AI adoption, supply-chain exposure, and cryptographic transition

Included AI Working Guide. 75 domain-specific prompts across the 12 trust domains, plus a capstone that produces six board-ready deliverables including a domain scorecard and 90-day roadmap.

Level	Most advanced
Format	Self-paced, SecureFi Readiness Model
Assessment	Professional assessment, 80% to pass
Certificate	SecureFi Institute Professional Certificate
Price	\$499 per learner, volume pricing available

PRICING AND ENROLLMENT

Course 1 is free. Courses 2 and 3 are \$299 and \$499 per learner. The Complete Series (Courses 2 + 3) earns two Professional Certificates and saves about \$100 per learner versus buying separately. Volume pricing is available for teams, and government and public-sector pricing is quoted by channel and volume.

Enroll now at LearningAcademyLD.com - A SecureFi Institute program. *Learn more at SecureFiInstitute.com*