



TOPICS:

Innovation

SOURCE:

Swiss Financial Market Supervisory Authority

FINMA: Guidance on Quantum Computing

- This guidance **highlights the cybersecurity risks that quantum computing** poses to Swiss financial institutions and sets out supervisory expectations for preparing the transition to post-quantum cryptography (PQC). Based on a survey of 60 regulated institutions, FINMA found that while most organisations recognise the risks of quantum computing, particularly the threat to existing encryption methods, the majority have not yet developed concrete migration plans.
- FINMA recommends that **institutions establish a board-approved PQC strategy supported by a detailed roadmap**, with a roadmap expected by mid-2027. It also advises conducting comprehensive risk assessments and maintaining an inventory of cryptographic assets across all systems, applications and outsourced services to identify vulnerable algorithms and prioritise migration.
- The guidance emphasises **protecting critical data** against “harvest now, decrypt later” attacks, where encrypted information could be stolen today and decrypted once

quantum computers become capable. FINMA also recommends adopting crypto-agility so systems can quickly replace cryptographic algorithms as standards evolve, and ensuring that external service providers support the transition to quantum-safe encryption.

- Although cryptographically relevant quantum computers do not yet exist, FINMA stresses that **migration will be complex and time-consuming**. Institutions are therefore expected to begin planning early to strengthen operational resilience and ensure continued compliance with regulatory requirements.

