SENETAS

A 5-step guide to quantum security

Quantum computing poses a growing threat to traditional encryption. Through “harvest now, decrypt later” attacks, encrypted information captured today could become readable in the future.



STEP 1

Conduct a cryptographic inventory

Create an inventory of cryptographic dependencies, including encryption, authentication and digital signatures, identifying the systems involved and their owners.

ACTION
Create an inventory of what is encrypted, how it is protected and who owns it.



STEP 2

Perform a risk assessment

Prioritise encryption first. Unlike authentication, it is exposed to ‘harvest now, decrypt later’ attacks.

ACTION
Rank systems by data sensitivity, protection lifetime and operational impact.



STEP 3

Decide how to mitigate the risk

Determine whether each system can be upgraded in place, needs to be replaced, or presents a sufficiently low risk to be temporarily accepted.

ACTION
Assign an upgrade, replace or accept pathway to each priority system.



STEP 4

Evaluate and implement quantum safe solutions

Look for certified, crypto-agile solutions that implement NIST post-quantum standards, support appropriate migration and interoperability options, including hybrid cryptography where required. Crypto-agility matters for authentication too: once a capable quantum computer exists, authentication must switch to quantum-resistant algorithms immediately.

ACTION
Include quantum safe capabilities in vendor assessments and future procurement requirements.



STEP 5

Build a phased migration timeline

- By 2030: complete migration of high-priority systems, working towards applicable national or regulatory deadlines.
- Next 90 days: assess encryption risks and priorities.
- Next 12 months: pilot and validate post-quantum cryptography and defining the target architecture.
- Phased rollout: focus on critical infrastructure, governance and migration deadlines.

ACTION
Document a dated roadmap with owners and milestones, aligned to the post-quantum deadlines set by your government or regulator.

Begin preparing for the post-quantum transition today.

Speak to a Senetas consultant about developing your post-quantum security roadmap.

Informed by guidance from NIST (NISTIR 8547), the UK NCSC, the EU and ASD.