PQC-RA

Post-Quantum Cryptography Risk Assessment

An Advanced Cryptographic Assurance and Planning Solution

Assess Current Cryptographic Landscape → **Quantify Quantum Risk Exposure** → **Design Strategic Migration Path to PQC**

acubed.it
Designing Secure Applications

Understanding PQC-RA

Learn how PQC-Risk Assessment tool identifies quantum encryption risks and aids planning in your migration to post-quantum cryptography

Steps in PQC-RA

- Identify Cryptographic Algorithms
- Assign Quantum Risk Score
- Create Prioritisation List
- Compare Against Standards
- Data Migration Roadplan

Assess → Prioritise → Transition

Cryptographic data is extracted, normalised and securely stored for analysis, setting the foundation for accurate risk scoring

Our engine identifies vulnerable or legacy algorithms that may be compromised by quantum computing

Each asset is assigned a Quantum Risk Score – from 0-4 based on encryption type, key length, business impact and future threat projections

You will receive a prioritisation list aligning your organisation with NIST, ISO and NCSC regulatory Standards

A detailed migration roadmap with prioritised steps guides your transition to post-quantum cryptography

A visual Dashboard shows readiness helping stakeholders understand what needs attention now

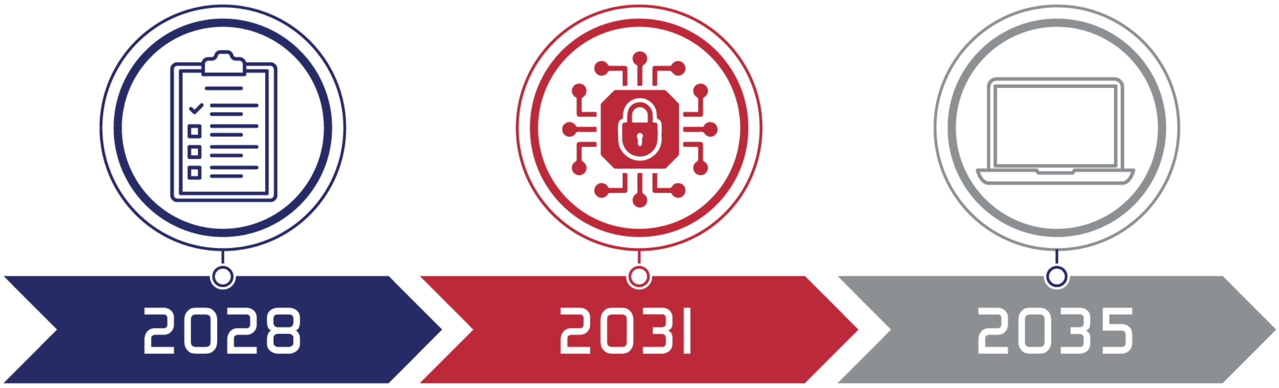
PQC Transition: Deprecation Schedule (NIST)

Organisations should begin phasing out these algorithms and transitioning to PQC:

Algorithm(s)	Status	Recommended Action
SHA-1, SHA-224, SHA3-224, SHA-512/224	Deprecated through 2030 Disallowed after 2030	Use SHA-256 or stronger (e.g., SHA-384, SHA-3).
RSA, ECDSA, EdDSA, DH, ECDH	Deprecated after 2030	Begin migrating to post-quantum cryptographic algorithms.
Algorithms < 128-bit security (incl. 112-bit)	Deprecated after 2030	Upgrade to algorithms with ≥128-bit security strength.

NCSC Timeline

National Cyber Security Centre



2028

Identify cryptographic services needing upgrades and build a migration plan

2031

Execute high-priority upgrades and refine plans as PQC evolves

2035

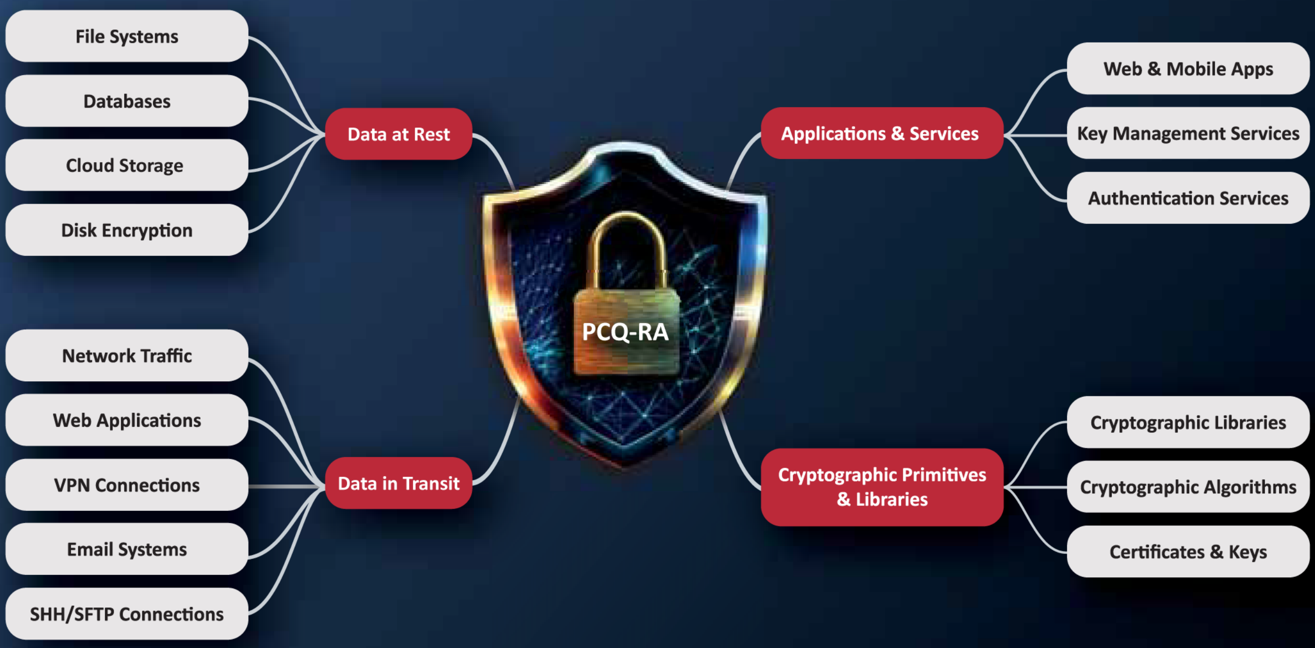
Complete migration to PQC for all systems, services and products

All traditional cryptographic algorithms that lack quantum resistance must be fully replaced with **NIST-approved PQC algorithms**.

Transition now to cutting-edge solutions such as ML-KEM, ML-DSA, and SLH-DSA.

acubed.it
Designing Secure Applications

Map your current cryptographic landscape



Contact Us Now!

Discover how Acubed IT’s PQC-RA can guide you to a quantum-safe future.

✉ PQCRA@acubed.it

🌐 www.acubed.it

in www.linkedin.com/company/acubed-it

Citation ISO Certification — Information security management — ISO 27001: 2022 — REGISTERED
Certificate No 448902024

Citation ISO Certification — Quality management — ISO 9001: 2015 — REGISTERED
Certificate No 471812024

CYBER ESSENTIALS CERTIFIED PLUS

QUALITY PRINCIPLES CERTIFIED

IASME CYBER ASSURANCE

JOSCAR REGISTERED

Crown Commercial Service Supplier

A company registered in the UK, company registration No.12285965