FullProxy

Preparing for the Quantum Future

A Practical Checklist for PQC Readiness

Define & Discover
Identify cryptographic dependencies, assess risks, and map out migration goals.

2028

Prioritise & Pilot
Start high-impact migrations, pilot PQC solutions, and refine strategy.

2031

Complete Migration
Ensure all systems and suppliers are quantum-safe.

2035

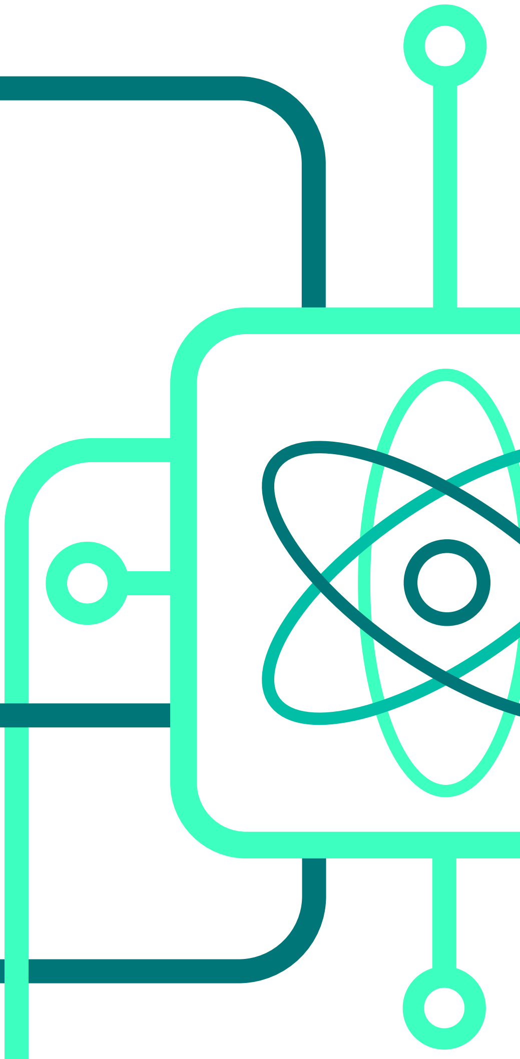
Actionable steps to help you protect your business

The UK's National Cyber Security Centre (NCSC) has issued a phased PQC roadmap to guide you and your organisation through the migration process. 2028 is the first big PQC milestone in the NCSC roadmap. It might seem distant, but that's less than three years away, and there's a lot to do. Our quantum readiness checklist will help you get PQC ready.

Building your Foundation

Why the groundwork matters

Before you can transition to post-quantum cryptography, you need to fully understand your current cryptographic estate and the capabilities of your existing hardware. Without this baseline, it's impossible to prioritise or plan your migration effectively.



1

Audit your certificates and crypto score

Do you know where all your digital certificates are, when they expire, or what algorithms they use? If not, there may be blind spots and potential vulnerabilities you can't see. Begin by cataloguing your certificates and getting full visibility of your estate, noting expiry dates, key lengths, and signing algorithms. This gives you a baseline "crypto score" to measure against PQC standards.

2

Assess your hardware and networks

Quantum-ready encryption will demand more processing power. Some current firewalls, load balancers, and VPN devices may not cope with the increased computational load, potentially slowing business-critical services to unacceptable levels. Conduct an audit to determine whether your infrastructure can scale, or whether it needs upgrading.

3

Understand your encryption methods

Catalogue your keys and determine which are asymmetric (e.g., RSA, Diffie-Hellman) versus symmetric (e.g., AES). Asymmetric keys are most at risk from quantum attacks, and algorithms like RSA will become obsolete. Meanwhile, SSL offloading and key exchanges will need to move to PQC-ready ciphers to remain secure.

Did you know?

- Almost all certificates issued today are not PQC ready. Identifying these now puts you ahead of the curve.
- Widely used encryption methods like RSA and Diffie-Hellman will be made obsolete when quantum computers arrive.
- While NIST-approved PQC algorithms such as CRYSTALS-Kyber (for key exchange) and CRYSTALS-Dilithium (for digital signatures) point the way forward, managing certificate lifecycles will be just as critical to staying secure.

Read more

Defining your PQC standards

Why your standards matter

Once you’ve mapped your cryptographic environment, you need to define what “good” looks like for your organisation. Standards ensure consistency across your estate and create a benchmark for supplier engagement.

4

Prioritise critical systems

Your first priority should be high-risk, high-impact assets: public-facing websites, customer portals, B2B VPNs managing your supply chain, and workforce access controls (especially for remote work).

5

Map dependencies

Every system connects to a web of networks, applications, and third-party services. Audit which technologies these critical systems rely on and identify any gaps or weaknesses in PQC readiness.

6

Evaluate suppliers

Your chain is only as strong as its weakest link. Research your vendors’ PQC plans and timelines. Some may already be developing PQC-capable products, while others may lag behind. Understanding this helps you plan your own technology refresh cycle.

7

Plan for technology refresh and adoption

Create a realistic, phased timeline for refreshing hardware, software, and certificates over the coming years. Where possible, adopt PQC functionality now - even if standards are still evolving. If your current infrastructure isn’t ready, consider deploying a PQC-ready proxy (such as an F5) to bridge the gap.

FullProxy

Taking Action

The NCSC's advice is clear; quantum processing is coming within the next few years, and the time to act is now. Waiting until quantum computers arrive will put your data, systems, and compliance at risk.

Here's a summary checklist:

✓ Conduct a full cryptographic inventory

✓ Establish certificate management practices that enable crypto-agility

✓ Pilot PQC-ready solutions

✓ Engage with your suppliers

✓ Continuously monitor certificate lifecycles, algorithm updates and complicate requirements

The quantum threat doesn't have a fixed date, but preparation shouldn't wait. By auditing your certificates, defining your standards, and planning your migrations today, you'll ensure you're secure and resilient to face the quantum era.

appviewx

AppViewX enables certificate lifecycle management and automation, ensuring a seamless transition to PQC-compliant certificates at scale

FORTINET
EXPERT PARTNER

Fortinet provides network security platforms aligned with NIST PQC standards and robust, scalable key management.

f5 unity+ GOLD

We deliver secure application delivery with crypto-agility and TLS readiness for post-quantum ciphers through F5.

Start your PQC readiness journey today

Get in touch for more info and resources, or to book a PQC readiness review with one of our experts.

www.fullproxy.com/PQC

hello@fullproxy.com

+44 141 291 5500