itworksmsp.ca
1 (800) 566-4188

Post-Quantum Cryptography Readiness Checklist

A 20-point audit for Canadian businesses preparing for the NIST 2030 deprecation timeline

Why this matters

NIST finalized three post-quantum encryption standards in August 2024. Current algorithms (RSA, ECDSA, ECDH) are deprecated by 2030 and disallowed by 2035. NIST estimates a 42–54 month migration timeline. Use this checklist to find out where your business stands today.

01 Cryptographic Inventory

- [ ] Identified all software and systems that use encryption (VPN, email, cloud storage, file servers, remote access).
- [ ] Documented encryption algorithms currently in use (RSA, AES, ECDSA, TLS 1.2/1.3, etc.).
- [ ] Mapped where encrypted data is stored and how long it is retained.
- [ ] Identified all systems handling digital signatures, certificates, or authentication tokens.

02 Data Classification & Risk Assessment

- [ ] Identified data that must remain confidential for 5+ years (client files, contracts, health records, financial data, IP).
- [ ] Rated each data category by sensitivity level: High / Medium / Low.
- [ ] Flagged data shared with government agencies, regulated industries, or US-based partners.
- [ ] Confirmed that data retention and destruction policies are documented and current.

03 Vendor & Third-Party Assessment

- [ ] Asked key software and cloud vendors: "What is your post-quantum cryptography migration roadmap?"
- [ ] Confirmed whether vendors plan to support NIST standards: FIPS 203 (ML-KEM), 204 (ML-DSA), 205 (SLH-DSA).
- [ ] Reviewed cloud storage, backup, and email provider security and update commitments.
- [ ] Identified any vendors serving US federal government customers (subject to stricter CNSA 2.0 timelines).

04 Governance & Incident Response

- [ ] Assigned internal ownership of the PQC migration initiative (IT lead, operations owner, or MSP partner).
- [ ] Reviewed cyber insurance policy and confirmed it addresses future cryptographic exposure scenarios.
- [ ] Updated incident response plan to include cryptographic compromise and encrypted data exposure scenarios.
- [ ] Briefed privacy officer or legal counsel on quantum risk and the 2030–2035 compliance timeline.

05 Migration Planning

- [ ] Set a target start date for PQC migration planning (recommended: no later than 2027 given 42–54 month timelines).
- [ ] Identified highest-priority systems for early migration (those protecting the most sensitive, longest-lived data).
- [ ] Evaluated whether current IT infrastructure can support post-quantum algorithm updates.
- [ ] Added PQC readiness as a criterion in all future vendor and software evaluations.

SCORE YOUR POSTURE

17–20 checked	**Strong posture**	Begin formal migration planning.
10–16 checked	**Gaps exist**	Prioritize a readiness assessment in the next 90 days.
9 or fewer	**High exposure**	Contact IT Works MSP for a Cybersecurity Posture Review.

Not sure where to start?

Book a Cybersecurity Posture Review. We cover the fundamentals — backups, MFA, email security, endpoint protection — plus a forward-looking PQC readiness assessment.

itworksmsp.ca/contact

or call 1 (800) 566-4188

This checklist is informational and does not constitute legal or regulatory advice. Cryptographic posture should be verified by a qualified professional.