Vendor Post-Quantum Cryptography (PQC) Assessment Questionnaire

Instructions for the Procurement and Third-Party Risk Management Teams: This assessment can be dispatched to all vendors processing sensitive organisational data or supplying critical software, hardware, or cloud infrastructure. Respondents must select the answer that best fits their current state.

Target Return Date:	

Section 1: Strategic Governance & Visibility

Specific Inquiry	**Required Vendor Response Format (Select One)**
1. Strategic Governance: Has your organisation established a formal, board-approved Quantum Readiness Strategy, and who is the designated executive accountable?	[ ] Yes (Provide Name/Title) **(2 pts)** [ ] In Progress (Provide ETA) **(1 pt)** [ ] No **(0 pts)**
2. Inventory (CBOM): Can you provide a comprehensive Cryptographic Bill of Materials mapping vulnerable asymmetric algorithms (e.g., RSA, ECC) within your provided services?	[ ] Yes, full CBOM available **(2 pts)** [ ] Partial inventory initiated **(1 pt)** [ ] No inventory initiated **(0 pts)**
3. Financial Commitment: Has a dedicated, multi-year budget been ring-fenced to ensure complete migration to PQC standards prior to the ASD 2030 mandate?	[ ] Yes **(2 pts)** [ ] Partial / Currently planning **(1 pt)** [ ] No **(0 pts)**

Section 2: Technical Readiness & Architecture

Specific Inquiry	**Required Vendor Response Format (Select One)**
4. NIST FIPS Migration: What is your specific implementation timeline for natively supporting the finalised NIST PQC standards (FIPS 203, 204, 205) in production?	[ ] Supported / Rolling out in 2026 **(2 pts)** [ ] Roadmap planned for 2027-2028 **(1 pt)** [ ] >2028 / No current plans **(0 pts)**
5. Data-in-Transit: What is your roadmap date to support Hybrid TLS (classical + PQC algorithms) to protect our data-in-transit against immediate HNDL interception?	[ ] Currently Supported / 2026 **(2 pts)** [ ] Planned for >2026 **(1 pt)** [ ] No hybrid plans; direct switch later **(0 pts)**
6. Data Vaulting: For stored sensitive data (PII, financial, health), what is your architectural roadmap to migrate from classical encryption-at-rest to quantum-safe storage?	[ ] Detailed PQC roadmap defined **(2 pts)** [ ] Basic AES-256 segmentation only **(1 pt)** [ ] No vaulting roadmap defined **(0 pts)**

Specific Inquiry	Required Vendor Response Format (Select One)
7. Hardware Roots of Trust: Are the Hardware Security Modules (HSMs) underpinning your cryptographic keys capable of being updated to PQC standards via firmware?	[ ] Firmware upgradable (Crypto-agile) **(2 pts)** [ ] Partial / Unknown **(1 pt)** [ ] Requires physical hardware overhaul **(0 pts)**
8. Incident Response / Crypto-Agility: If a PQC algorithm is compromised, do you possess automated crypto-agility capabilities to rapidly swap algorithms without disruption?	[ ] Yes, fully automated **(2 pts)** [ ] Partially agile (requires manual patch) **(1 pt)** [ ] No capability currently exists **(0 pts)**

Section 3: Supply Chain Risk & Legacy Remediation

Specific Inquiry	Required Vendor Response Format (Select One)
9. Supply Chain Risk: Have you formally assessed your primary upstream cloud and infrastructure providers (e.g., AWS, Azure) for PQC readiness and FIPS 203/204 roadmaps?	[ ] Yes, all upstream aligned **(2 pts)** [ ] Assessment in progress; gaps exist **(1 pt)** [ ] No assessment conducted **(0 pts)**
10. Legacy Remediation: Do you rely on any deprecated or highly vulnerable legacy cryptography (e.g., SHA-1, 3DES, RSA <2048) anywhere in the service delivery chain provided to us?	[ ] No legacy cryptography utilised **(2 pts)** [ ] Yes (Mandatory 2026 remediation set) **(1 pt)** [ ] Yes (No remediation date set) **(0 pts)**

Internal Section-by-Section Scoring Calculator & Action Matrix

Instructions for Evaluator: Tally the points for each section individually to generate a Red, Amber, Green (RAG) status profile. This scoring mechanism aligns vendor maturity with the expectations of the Post-Quantum Cryptography Maturity Model (PQCMM) framework and highlights specific domains requiring immediate remediation under APRA CPS 230.

Section 1: Strategic Governance & Visibility (Max 6 points)

GREEN (5 - 6 points)	The vendor demonstrates mature governance and full visibility into their cryptographic footprint. Proceed with standard monitoring.
AMBER (3 - 4 points)	The vendor recognises the threat but lacks structural execution. *Action:* Require quarterly updates from their executive team on their CBOM progress.
RED (0 - 2 points)	Fundamental governance failure. *Action:* Flag as a critical APRA CPS 230 compliance risk. The vendor lacks the basic awareness required to protect long-tail data.

Section 2: Technical Readiness & Architecture (Max 10 points)

GREEN (8 - 10 points)	The vendor possesses high crypto-agility and an aggressive NIST transition timeline.
AMBER (4 - 7 points)	The vendor relies on manual patching or has delayed timelines (2027+). *Action:* Ensure that the "Liability for Data Breach" contract clauses explicitly cover retrospective data decryption resulting from HNDL attacks due to their delayed transition.
RED (0 - 3 points)	High HNDL Liability. *Action:* The vendor’s architecture is rigid and deeply vulnerable. Halt new contract expansions and mandate the development of a rapid exit strategy.

Section 3: Supply Chain Risk & Legacy Remediation (Max 4 points)

GREEN (4 points)	Clean software supply chain with quantum-ready upstream dependencies.
AMBER (2 - 3 points)	Legacy crypto is present but being actively remediated. *Action:* Institute milestone tracking for the removal of legacy algorithms (e.g., SHA-1, RSA <2048) within the current fiscal year.
RED (0 - 1 points)	Unacceptable third-party risk. *Action:* If the vendor utilises legacy cryptography without a firm remediation date, or has no visibility into their own cloud providers, they represent an active SOCI Act vulnerability. Escalate immediately to the Executive Risk Committee.