Navigating the Quantum Horizon

Moving from R&D to Operational Resilience

The Quantum Horizon: Moving from R&D to Operational Resilience

Welcome: Today’s Priority

- Moving quantum readiness from a future concept to today's board-level priority.

Immediate & Regulatory Focus

- The "Harvest Now, Decrypt Later" threat.
- Tightening Australian regulatory landscape (SOCI Act, APRA, Privacy Act).

Hidden Supply Chain Threats

- Uncovering supply chain vulnerabilities vulnerabilities and why current trust models are breaking.

Actionable Takeaways

- AusCERT CLN toolkit for FY26/FY27 budgets.
- Risk triage and actionable strategy.

THE TIMELINE HAS COLLAPSED

Quantum Verifiable Advantage is a Reality in 2026

Google “Willow”

105 qubits with exponential error reduction.

Performance Reality

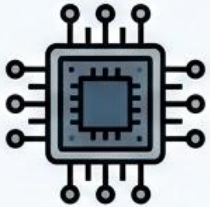
5 minutes vs. 10 septillion years of classical computing.

IBM Heron R2

156-qubit processor demonstrating 50x speedups.

The Australian Paradox & Supply Chain Opacity

Global Leader vs. Corporate Laggard: Only 8.5% of Australian firms quantum-safe.



Domestic Infrastructure: PsiQuantum's $940M Brisbane facility targeting 1 million qubits.

The Blind Spot: Cryptographic supply chain opacity.

The Rule: If our SaaS vendor isn't quantum-ready,

we aren't quantum-ready.

What is Actually Vulnerable?

Highly Vulnerable (Must Replace): Asymmetric cryptography (RSA, ECC, Diffie-Hellman) securing web traffic and PKI.
The Signature Threat: Digital certificates, firmware signing, and software updates ar at risk of being forged ("Trust Now, Forge Later").
Quantum Resilient (Safe): Symmetric encryption like AES26. Grover's algorithm only halves its strength, leaving a highly secure 128-bit effective defense.

Vulnerable: Asymmetric crypto (web traffic, PKI), digital certificates, and firmware signing. Risk of "Trust Now, Forge Later".

Safe: Symmetric encryption. Grover's algorithm only halves effective strength to a highly secure 128-bit.

The Situation Right Now: Broken Trust & HNDL

Critical Security Risks in the Quantum Age

- **"Harvest Now, Decrypt Later" (HNDL):** Adversaries are already intercepting and decoding TLS traffic.
- **"Trust Now, Forge Later":** Every standard we rely on today to verify identity will be broken.
- **The Firmware Threat:** Digital certificates validating firmware and software will be successfully forged by quantum adversaries.

Assessing the Impact: Temporal Data & Hidden Risks

- **The Temporal Nature of Data:** Does a breach today matter if decrypted in 1 to 2 years?
- **Retroactive Liability:** Previous breaches will become active future liabilities.
- **SaaS and Supply Chain Risk:** Inherit cryptographic vulnerabilities of your providers.
- **Mandatory Action:** Must be added to your Enterprise Risk Register immediately.

The Regulatory Stick - Inaction is a Breach

- **SOCI Act (2026 Reforms):** Expanded to data storage, targeting supply chain & vendor risks.
- **Privacy Act (2024/2026):** Statutory torts for privacy invasion; new ADM transparency rules.
- **APRA (CPS 230 & 234):** Strict operational resilience and third-party risk management by July 2026.
- **ASD Mandate:** Transition plan for Post-Quantum Cryptography required by the end of 2026.

SOCI Act (2026 Reforms)

Expanded to data storage, targeting supply chain & vendor risks.

Privacy Act (2024/2026)

Statutory torts for privacy invasion; new ADM transparency rules.

APRA (CPS 230 & 234)

Strict operational resilience and third-party risk management by July 2026.

ASD Mandate

Transition plan for Post-Quantum Cryptography required by the end of 2026.

Budgeting for Remediation

Remediation Scope

Addressing the entire **IT and OT ecosystem**.

Hardware Security Modules (HSMs)

Upgrading infrastructure to support new NIST FIPS 203/204 algorithms.

Firmware Replacements

Phasing out legacy hardware that cannot support quantum-safe patching.

Vendor Replacement

Funding the transition away from non-compliant "Red Risk" SaaS providers.

The Tools to Get You There: QC WG Artefacts

Tool 1: AusCERT Executive Briefing

Quantum Computing Preparedness v1.0. A presentation pack for executives including:

- SWOT analysis & regulatory overview
- QC risk modeling framework summary

Tool 2: Vendor PQC Questionnaire

Auditing and scoring your third-party SaaS providers.

- Inventorying vendor crypto capabilities
- Assessing post-quantum readiness

Tool 3: Cryptographic Bill of Materials (CBOM)

Audit template and scoring matrix

Inventorying and assessing internal crypto assets

AusCERT QC WG Executive Briefing Pack

The "Q-Day" Horizon Has Shifted

Active Operational Risk
Timeline has shifted to **2026**, moving from the previous theoretical 2030 target.

Quantum Supremacy
Google's Willow chip demonstrated an **813,000x** performance advantage over classical supercomputers.

Australian Leadership
Australia is a tier-one global leader with a **$940M investment** in PsiQuantum's Brisbane facility.

Preparedness Gap
Only **5%** of orgs have a defined strategy, while **60%** of tech pros anticipate increased threats.

SWOT Analysis

INTERNAL FACTORS	**STRENGTHS +** • Proactive leadership & board awareness • Academic partnerships (UNSW, ANU) • Agile IT architecture (Hybrid TLS) • Robust ERM framework integration • Centralised data governance
	WEAKNESSES – • Lack of CBOM (supply chain opacity) • No dedicated PQC migration budget • Risk knowledge siloed in IT • Reliance on legacy RSA/ECDSA systems • Limited internal crypto expertise
EXTERNAL FACTORS	**OPPORTUNITIES +** • First-mover advantage & NIST compliance • QaaS for advanced computing access • Quantum catastrophe risk modeling • $472M domestic quantum grant access • Modernize legacy IT via PQC transition
	THREATS – • HNDL attacks & retroactive liability • SOCI Act director liability penalties • Third-party supply chain failures • Sudden math breakthroughs (obsolescence) • Critical global skills shortage

Enterprise Quantum Risk Modeling Frameworks

Strategic alignment of PQC migration with enterprise risk management and audit requirements.

FRAMEWORK	SPONSOR	CORE METHODOLOGY & SCOPE	GRC INTEGRATION & AU USE CASE
QRAMM	CyberSecurity NonProfit	Evaluates crypto inventory, governance, and readiness.	Automated Excel scoring; ideal for SOCI Act compliance roadmaps.
ISACA Risk IT	ISACA	Embeds quantum risk into existing ERM; focus on risk appetite.	Aligns with Board governance; best for APRA CPS 230 workflows.
PQC Risk Model	FS-ISAC	Sector-specific; crypto agility and complex PKI environments.	Essential for APRA-regulated banks and major insurers.
WEF Toolkit	World Economic Forum	Executive principles; leadership education and phased execution.	Drives C-suite narrative; secures funding from non-tech boards.
NIST CSWP-48	NIST NCCoE	Maps migration to NIST CSF 2.0 and SP 800-53 controls.	Crucial for critical infrastructure and government auditability.

Regulatory Considerations

Regulatory Body / Standard	2026 Status & Focus Area	Direct Impact on Quantum Readiness
NIST PQC Standards	FIPS 203, 204, 205 Finalized; FIPS 206 Drafted.	Establishes the non-negotiable mathematical baseline (ML-KEM, ML-DSA) for all global encryption migration.
ASD ISM	March 2026 Update.	Mandates a refined PQC transition plan by the end of 2026; complete abandonment of classical asymmetric cryptography by 2030.
SOCI Act	May 2026 CIRMP Enhancements.	Data storage classified as critical infrastructure. Directors face personal liability for unmanaged cryptographic supply chain hazards.
APRA CPS 230	Fully enforceable July 1, 2026 (for non-SFIs).	Insurers and banks are legally accountable for the cryptographic vulnerabilities of their third-party material service providers.
ASIC	2026 Key Issues Outlook.	Boards must demonstrate technical literacy and explicitly disclose material risks related to emerging technologies, including quantum threats.

PCQ Questioniaire and Scoring

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 Cryplographic 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 / Ralling 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 data to support Hybrid TLS (classsist + PQC algorithms) to prntect our data-in-hansit arainet immerfiate HkiDl	[ ] Currently Supported / 2026 **(2 pts)** [ ] Planned for >2026 **(1 pt)**

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 mechanium 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 tacks structural execution. *Action:* Require quartetty 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 tall 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 Remedlation (Max 4 points)

Cryptographic Bill of Materials (CBOM) audit template

Asset or System	Asset Type (Internal, SesS, (COTs, Hardware)	Data Sensitivity Lifespan (Score A)	Asymmetric Algorithm in Use (Score B)	Symmetric Algorithm in Use (Score C)	Crypto-Agility & Vendor Roadmap (Score D)	Cryptographic Functien / Service (Score E)	Total Risk Score (Auto-Som A-E)
Example: Core Policy Admin	Internal App	> 10 Years	RSA-2048	AES-156	Hardcoded / No Roadmap	Data at Rest & TLS	14 (Critical)
Example: Cloud HR Portal	SaaS	5 - 10 Years	RCA-256	AES-256	Roadmap > 2027	Authentication & TLS	12 (High)
Example: Network Router	Hardware	1 - 5 Years	RSA-4096	AES-256	Readmap 2027+	Firmware Sgriing	13 (Critical)
Example: Secure Vault	Internal App	> 10 Years	None (Symmetric Only)	AES-256	Fully Aglly / PQC Ready	Data at Rest	6 (Moderate)

Parameter Scoring Logic

Category	Response Option	Points	Risk Contest & Justification
A: Data Sensitivity Lifespan	> 10 Years	4	Prime target for "Harvest Now, Decrypt Later" (HNDL) attecss, data outlives current encryption strength.
A: Data Sensitivity Lifespan	5 - 10 Years	3	High exposure; lifespan exceeds optimistic quantum computing migration timelines.
A: Data Sensitivity Lifespan	1 - 5 Years	2	Moderate exposure.
A: Data Sensitivity Lifespan	< 1 Year	1	Low HNDL risk (e.g., short-lived session takons, temperary telemetry).
B: Asymmetric Crypto	RSA, ECC, Diffie-Hellman, USA	4	Highly univerable to Shor's Algorithm: fundamental break of trust and confidentiality.
B: Asymmetric Crypto	Hybrid TLS (Classical + POC)	2	Recommended transitional detense-in-depth approach to mitigate immediate horvesting.
B: Asymmetric Crypto	None, or NIST FIPS 203/204/205	0	Quantum-resilient.
C: Symmetric Crypto	Legacy (SDES, SHA-1)	4	Highly univerable and deprecated algorithms.
C: Symmetric Crypto	AES-128	2	Weakened by Grever's Algorithm but refains accestable short-term security.
C: Symmetric Crypto	AES-256	0	Quantum-resilient benchmark for long-term security; recommended by ASD.
D: Crypto- Agllity & Readmap	Hardcoded / No Vendor Roadmap	4	Severe supply chain risk; requires immediate hardware replacement or code results.
C: Crypto- Agllity & Readmap	Vendor Roadmap 2027+	3	Delayed compliance risk approaching the ASD 2030 legacy deprecation deadline.
D: Crypto- Agllity & Readmap	Vendor Roadmap = 2027	1	Aglle and on track for the ASD 2028 migration commencement.
D: Crypto- Agllity & Readmap	Fully Agile / POC Upgraded	0	Seamless awas capabilities or already compliant.
E: Cryptegraphic Functien	Firmware/Software Signing & Roots of Trust	4	Highest risk of "Trust Now, Forge Later" sttacks; allows adversaties to inject malicious code via forged certificates.
E: Cryptegraphic Functien	Data in Transit (TLS, VPN, IPsec)	4	Highest risk of Immediate "Harvest Now, Decrypt Later" data interception.
E: Cryptegrsphic Function	Dats at Rest (Databases, Storage)	2	Lower immediate hervesting risk, assuming physical network perimeters remain unbreached.
E: Cryptegraphic Function	Ephemeral / Session Auth	1	Temporary value, minimal long-term quantum descyption threat.

Overall Triage & Action Matrix

This table sums the points from Table 2A (Maximum of 20 points) to fullill the ASDS requirement to prioritiss individual systems for transition based on their risk profile.

Total Score	Risk Level	ASD Triage Priority	Required Executive & Remediation Action
16 - 20	CRITICAL	Priority 1	Immediate Action Required. Highly vulnerable to HNDC or signature forging, isclate long-tail data, hait non-compliant sendor renewais, and budget for emergency hardware firmware upgrades in the FY26 cycle.
11 - 15	HIGH	Priority 2	Action required before 202S. Represents significant supply chain risk. Begin scheduling migrations to AES-356 and mandate third-party SaaS senders to accelarate their PQC timelines to meet NIST standards.
6 - 10	MODERATE	Priority 3	Acceptable short-term risk. Plan routine lifecycle upgrades. Monitor vendor progression to ensure they meet the final ASD legacy asymmetric deprecation deadline of 2030.
0 - 5	LOW	Priority 4	Monitor. Quartium-resilient or low temporal data value. Maintain continuous monitoring and validate cryptographic implementations periodically to ensure engoing compliance.

The Industry Action Plan (2026 and Beyond)

NOW (0-3 Months)

NOW (0-3 Months)

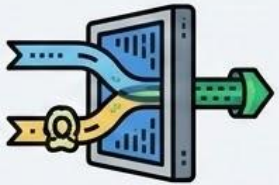
Execute your Cryptographic Bill of Materials (CBOM) and issue Vendor PQC Questionnaires.

Q4 2026

Q4 2026

Finalize your ASD-aligned PQC Transition Plan and secure dedicated FY27 budgets.

2027-2028



2027-2028

Commence active transition by deploying Hybrid TLS (Classical + PQC) across critical external gateways.

2030

2030

Achieve complete eradication of legacy asymmetric cryptography to meet the final ASD deadline.

Questions?


Decryption of RSA2048/ECC 266
QUANTUM COMPUTER
TRADITIONAL
COMPLETE
COMPLETE
COMPLETE