Quantum Computing Preparedness

AusCERT Quantum Computing Working Group Executive Briefing

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.

The Immediate Threat: "Harvest Now, Decrypt Later"

Active Interception

Adversaries are actively intercepting and archiving encrypted data traffic today.

Data Stockpiling

Data is stockpiled until Cryptographically Relevant Quantum Computers (CRQCs) mature.

Immediate Compromise

Data with a lifespan > 5-10 years (health, IP) is considered already compromised.

Retroactive Liability

Creates a paradigm of permanent, retroactive liability for legacy data.

The 2026 Regulatory Mandate

ASD ISM

Mandates a formally documented, refined Post-Quantum Cryptography (PQC) transition plan by the end of 2026.

SOCI Act

Data storage is now classified as critical infrastructure; directors face personal liability for supply chain cryptographic hazards.

APRA CPS 230

Fully enforceable July 1, 2026, holding entities legally accountable for operational resilience and provider vulnerabilities.

NIST PQC Standards

FIPS 203, 204, and 205 finalised in August 2024, establishing the non-negotiable global baseline.

Our Strategic Response - The Technical Bridge

Visibility

Commission a Cryptographic Bill of Materials (CBOM) to map vulnerable algorithms across the enterprise.

Agility

Implement Hybrid TLS (combining classical and NIST-approved PQC algorithms) within 6-18 months.

Defense-in-Depth

Protect data-in-transit from immediate harvesting while seamlessly preserving backward compatibility.

Sector-Specific Action (For Insurance/Financial Entities)

Post-Quantum Data Vaulting

Segregate long-tail archival records and life insurance policies into highly restricted, AES-256 protected environments.

Quantum Actuary Pilot Programs

Run quantum-simulated "shadow models" to accurately price complex, cascading catastrophe events.

Real-Time Fraud Detection

Leverage quantum algorithms for rapid pattern recognition, potentially reducing calculation times.

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

Strategic Implications & 2026 Action Plan

Board Oversight

Integrate quantum computing explicitly into the board's oversight of enterprise and cyber risk.

Halt Crypto Debt

Mandate verifiable PQC transition roadmaps from all Tier-1 software vendors.

ASD Compliance

Finalize a formally documented PQC transition plan by the end of 2026.

Immediate 90-Day Plan

- Fund a comprehensive, automated CBOM audit.
- Dispatch PQC readiness questionnaires to the top 20 critical vendors.
- Ring-fence a multi-year IT budget specifically for cryptographic modernisation.

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.