SOUTHERN QUANTUM

CRYPTOGRAPHIC AGILITY

southernquantum.au

Gold Coast | Sydney

EBOOK

Quantum risk

A guide for Australian boards

Stephen Chey

Founder, Southern Quantum

stephen@southernquantum.au

First edition, November 2026

SOUTHERN QUANTUM PTY LTD

ABN 78 701 793 026

CONTENTS

Foreword ... 3
Board summary ... 4
01 Why quantum risk is a board matter ... 5
02 The quantum threat model ... 8
03 Directors' duties and the regulatory framework ... 12
04 Know what you hold ... 17
05 The transformation program ... 20
06 The supply chain ... 28
07 Cryptographic sovereignty ... 32
08 The questions boards should ask ... 37
Milestones timeline ... 43
Glossary ... 45
Sources ... 47
About Southern Quantum and the author ... 50

ABOUT THIS GUIDE

This guide explains quantum risk as a governance matter for Australian boards. It is written for directors of APRA-regulated entities, critical infrastructure operators, listed companies, universities and any organisation holding data that must stay confidential for many years. It brings together Stephen Chey's published articles on this subject.

It reflects the PSPF Release 2026, the Information Security Manual (September 2026) and APRA's 2026–27 Corporate Plan, as at 7 November 2026.

Foreword

Every Australian board now oversees a risk that leaves no trace when it occurs and does not appear in ordinary board reporting. Much of the encryption that protects payments, health records, research, legal advice and the systems that run power and water is public-key cryptography. It was designed on the assumption that some mathematical problems are too hard to solve. A sufficiently capable quantum computer will solve them. When that happens, data stolen years earlier can be read, and signatures that looked trustworthy can be forged.

I wrote this guide for the directors who are accountable for that risk. It is not a technical manual, and it is not legal, financial or professional advice (see the disclaimer at the back of the guide). It explains what the threat is, what Australian law and regulators already expect of boards, what a credible response contains, and how a director can tell whether management's answers are adequate.

It brings together articles I have published on this subject, in one accessible format. I have edited the material to remove repetition, corrected it where needed and brought it up to date to November 2026.

Post-quantum cryptography is an emerging field. Standards, regulation and practice are still changing, and some of what this guide describes will change after publication. I welcome feedback, corrections and suggestions for future editions at stephen@southernquantum.au.

How to use this guide

The chapters follow the order in which a board usually needs to think about the risk:

- **Chapters 1 and 2** explain why quantum risk is a board matter and what the threat actually is.
- **Chapter 3** sets out, in one place, the legal and regulatory obligations that already apply.
- **Chapters 4 to 6** describe what a credible response contains: knowing what the organisation holds, running the transformation program, and managing the supply chain.
- **Chapter 7** covers a question most frameworks leave out: who owns and controls the cryptography.
- **Chapter 8** gives the eight questions a board should put to management, with guidance on what to do when an answer is inadequate.

A director with 10 minutes should read the board summary on the next page. A director preparing for a board or committee meeting should read Chapter 8. Each chapter ends with a short set of prompts that link back to the questions in Chapter 8.

The glossary at the back explains the technical terms. Numbers in square brackets refer to the sources listed at the end of the guide.

Board summary

THE RISK IN ONE PARAGRAPH

Experts consider a quantum computer able to break today's public-key encryption "quite possible" within 10 years and "likely" within 15.[1] Data stolen today can be read once such a computer exists, and that harm cannot be undone. That makes it a board matter now, not when the computer arrives. The Australian Signals Directorate (ASD) and the Australian Institute of Company Directors (AICD) have already named quantum computing as a board responsibility.[2]

The three quantum threats

Threat	What happens	Exploitable now?
1. Confidentiality	Data is collected now and decrypted later ("harvest now, decrypt later").	Collection, yes. Decryption needs a quantum computer.
2. Integrity	Signatures on contracts, records and software are forged.	The exposure exists now. Forgery needs a quantum computer.
3. Access	Hidden access is planted during periods of change.	Yes. No quantum computer is needed.

Table 1. The three quantum threats (Chapter 2)

ASD's recommended milestones[3]

- **End of 2026:** a refined transition plan. This is now weeks away.
- **End of 2028:** transition started for critical systems and long-lived sensitive data.
- **End of 2030:** transition complete. RSA, Diffie-Hellman and elliptic curve algorithms lose ISM approval.[4]

These dates are closer than they look. Cryptography is built into almost every application, system and device, much of it inside vendors' products, and specialist skills are scarce.

The eight questions for management

1 Do we hold data or systems that would be seriously damaging if exposed, and do we know where they are?

2 Who owns this risk, and is it managed or only recorded?

3 Are we still creating new exposure through what we buy and what we build?

4 Are we governing forged signatures and planted access, not only harvested data?

5 Is there a credible roadmap and cost estimate?

6 Can we trust what we are told?

7 What do we already owe under law and contract?

8 If this goes wrong, what protects us personally?

01 Why quantum risk is a board matter

This chapter explains why quantum risk belongs on the board agenda now, even though the computer that creates it does not yet exist. It sets out how the law judges directors on known risks, why cryptographic risk differs from cyber and AI risk, and what earlier technology migrations teach about delay.

Directors are judged on how they govern a known risk

Every Australian company director should know the James Hardie case. In February 2001, the board of James Hardie Industries approved an announcement to the Australian Securities Exchange (ASX). It stated that a new compensation foundation was "fully funded" and had "sufficient funds to meet all legitimate compensation claims". The foundation was later found to be more than $1 billion short. In 2012, the High Court found that the directors who approved it had breached their duty of care under the Corporations Act. [5]

The harm from asbestos had built up over decades, long before anyone in that boardroom understood the size of the liability. The directors were not held responsible for that harm. They were held responsible for what they did, or failed to do, once the risk was known and foreseeable.

Australian directors are in a similar position with quantum risk. The risk is known. Australia's technical authority and the peak body for directors have described it as a board matter.[2] What remains open is how each board governs it.

For directors and senior executives of entities regulated by the Australian Prudential Regulation Authority (APRA), the obligation is also personal. Under the Financial Accountability Regime (FAR), named Accountable Persons are individually accountable for prudential obligations, including information security under CPS 234.[6] The question for them is not whether the obligation exists, but whether they can show they have met it.

The attack has already started

A quantum computer capable of breaking today's public-key encryption does not yet exist. The collection phase of the attack does not need one. Nation-states and well-resourced criminal groups are collecting encrypted data now, to decrypt once quantum computers mature. This is known as "harvest now, decrypt later". Chapter 2 explains the threat in detail.

If an organisation holds data that must stay confidential for 10 years or more, it is the kind of data these actors collect. No public source confirms collection against a named Australian organisation, Because harvesting leaves no trace, none may ever do so. Boards cannot confirm that the exposure is absent. That uncertainty, not proof of compromise, is what they must govern.

Who needs to move first

Not every organisation faces the same timeline. Technical guidance from the Dutch intelligence service AIVD and the research institutes CWI and TNO separates two groups. Some organisations must move now. Others can wait for standards and products to mature.[7] The deciding factors are whether an organisation holds data that must stay confidential for a long time, or runs critical or long-lived infrastructure.

On that test, the following organisations cannot wait:

- entities regulated by APRA, including banks, insurers and superannuation funds
- operators of critical infrastructure under the Security of Critical Infrastructure Act 2018 (SOCI Act)
- universities and research institutions holding sensitive or defence-linked research
- any organisation holding long-lived health, legal, identity or government records.

Australia does not set the technology, but it holds the accountability

Much of the public discussion of post-quantum cryptography (PQC) comes from the United States. The new algorithms were standardised by the US National Institute of Standards and Technology (NIST).[8] Cloud platforms, software vendors and hardware makers set their roadmaps offshore.

Australian boards do not need to invent post-quantum cryptography. They do need to govern how their organisations adopt it, within Australian conditions. These conditions include:

- critical infrastructure exposure
- the expectations of APRA and the Australian Securities and Investments Commission (ASIC)
- Privacy Act consequences
- the concentration of suppliers
- the long-lived health, insurance, superannuation, legal and government records held in this country.

The technology is set offshore. The accountability stays here.

Cryptographic risk differs from cyber and AI risk

Directors who have invested in cyber security and AI governance may assume the quantum threat is covered. It is not. It differs from both, as the table below shows. Three differences matter most.

	Cyber security risk	AI risk	Cryptographic risk
When the harm occurs	Now, and usually detectable	In future decisions	Already under way, and may never be visible
Can the harm be reversed?	Mostly, by restoring and patching	Often, by correcting the model	No. Decrypted data stays exposed.
What must be known first	Assets and threats	Where AI is used	Where every algorithm, key and certificate is used
What sets priority	Current threat and impact	The impact of each use	How long data must stay confidential, and how long migration will take
How it is managed	Strengthen and monitor existing systems	Govern design, use and deployment	Replace the algorithms in every system that uses them, over several years
Who must act	Mostly the organisation	The organisation and its AI suppliers	The organisation, its vendors and its counterparties
The board's question	Are we protected and ready to respond?	Are we using this technology responsibly?	Have we already been compromised in ways we cannot see, and are we moving fast enough to limit the damage?

Table 2. How cryptographic risk differs from cyber and AI risk

The harm is retroactive and permanent. When a ransomware attack occurs, an organisation isolates systems, restores from backup and recovers. Once a quantum-capable adversary decrypts harvested data, confidentiality cannot be restored. No patch, response plan or insurance payout reverses it. The exposure covers everything the organisation has ever sent or stored under quantum-vulnerable encryption, not only current systems.

Some flaws can be patched. The quantum flaw cannot. Cryptography is often weakened by poor implementation, such as weak settings or expired certificates. These flaws can be fixed, and should be. The quantum flaw is in the mathematics of public-key algorithms such as RSA and elliptic curve cryptography. No implementation protects them, so they must be replaced. A transition program should fix both.

The attack may leave no trace. Harvesting encrypted traffic takes nothing that appears to be missing. There may be no alert and no anomaly in an access log. Most organisations using quantum-vulnerable encryption have no way of knowing what has already been collected.

Threat briefings, penetration tests and AI model approvals are still needed, but they are not enough. A **cryptographic inventory** and a **migration roadmap** tied to ASD's milestones are also needed (Chapters 4 and 5).

Earlier migrations show the cost of delay

SWIFT and ISO 20022. The SWIFT financial messaging network required its members to move from the legacy MT message format to the ISO 20022 standard. The industry coexistence period ended in November 2025.[9] Institutions that deferred ran emergency programs late in the coexistence period, at higher cost. SWIFT postponed the start of the migration twice, first because banks were not ready and then to align with the European Central Bank. The end date did not move.

Y2K. The US financial sector, under deadlines set by regulators and with board-level accountability required from the start, reached 99.7 per cent readiness across about 22,000 institutions before the year 2000.[10]

In both cases, organisations that treated a known technology risk as a board matter, funded it properly and acted early met their deadlines. Those that waited for the deadline to force action paid more.

The scale of the post-quantum task is large even when it is planned. The US Government has estimated that moving its prioritised federal information systems to post-quantum cryptography will cost about USD 7.1 billion (in 2024 dollars) between 2025 and 2035. The estimate excludes national security systems, and the report describes it as a rough order of magnitude.[11]

The James Hardie directors were informed. They failed to act with enough care on what they knew. For quantum risk, the threat is known and the regulatory guidance is explicit. The question is whether to act while orderly change is still possible.

> QUESTIONS TO TAKE FROM THIS CHAPTER
>
> - Does our organisation hold data or run systems that put us among those who cannot wait? (Question 1)
> - Has the board formally recorded its view of quantum risk, and who owns it? (Question 2)

02 The quantum threat model

Quantum risk is usually described as a threat to encryption. That description is correct but incomplete. This chapter sets out three distinct threats and tests each against a standard method for judging whether a threat is credible. It then lists the seven elements a board should expect in management's threat model.

How soon, and why the date matters less than it seems

A cryptographically relevant quantum computer is one capable of breaking the public-key algorithms in use today. The Global Risk Institute's 2025 survey of 26 international experts found such a machine "quite possible" within 10 years and "likely" within 15.[1] Estimates of the hardware needed keep falling. In 2025, a Google Quantum AI researcher reduced the estimated resources needed to break a 2048-bit RSA key about 20-fold compared with his own 2019 estimate.[12]

Boards do not need to predict the date. A simple test, known as Mosca's inequality, shows why.[7] Add two numbers:

- the number of years the data must stay confidential, and
- the number of years it will take to move the systems protecting it to new algorithms.

If the total is greater than the number of years until a quantum computer exists, the data is already at risk. Take records that must stay confidential for 10 years, held in systems that will take five years to migrate. They are already at risk if a quantum computer arrives within 15 years, which the experts surveyed consider likely.

Means, opportunity and motive

Security analysts judge whether any threat is credible by asking three questions about the adversary. Do they have the **means**? Do they have the **opportunity**? Do they have a **motive**? This is not a quantum-specific framework. Applied to quantum risk, it gives a result that boards rarely hear: for two of the three threats, means is the only missing element. For the third, nothing is missing.

Threat 1: confidentiality (harvest now, decrypt later)

Means. A quantum computer able to break RSA or elliptic curve keys. This does not yet exist. There is one exception. Cryptographic assessments find weaknesses that a well-resourced attacker can already break without a quantum computer, such as outdated 1024-bit Diffie-Hellman settings. These weak settings are often found in the same systems that need post-quantum migration.[13] For those systems, means is already present.

Opportunity. Encrypted data must be intercepted before it can be harvested. State signals intelligence agencies are built to do exactly this, through network interception, compromised infrastructure and access to data in transit. Any organisation whose data crosses networks these agencies already monitor has provided the opportunity, whether or not it has been targeted.

Motive. National intelligence services collect for long-term value: government communications, defence and dual-use research, infrastructure designs, and any data still useful after a 10 to 15-year wait. ASD's Annual Cyber Threat Report 2024–25 describes state-sponsored actors as a serious and growing threat to Australian government, critical infrastructure and business.[14] ASIO has said that if it had a threat level for

espionage and foreign interference, it would be at the highest level.[15] Harvesting encrypted data is espionage.

Operational technology (OT) is a clear case of long-lived data. Control system settings, engineering data and firmware often stay in service for 15 to 25 years, and frequently run cryptography that was not designed with confidentiality in mind.

Threat 2: integrity (forged trust)

Means. The same quantum capability as threat 1, used to derive a private signing key from its public key.

Opportunity. This is the element most boards do not expect. The opportunity already exists by design. Digital signatures and the public keys used to check them are meant to be shared. A code-signing certificate, a signed contract or a patent filing is already as exposed as it needs to be. No interception is needed.

Motive. A forged signature allows things that stolen data cannot. An attacker could pose as a trusted software vendor and push a malicious update through a channel every customer already trusts. The same method could transfer intellectual property through a forged assignment, or alter long-held audit records.[16] The range of actors is wider than for threat 1. It includes financially motivated criminals as well as state actors, because forgery brings direct financial gain.

Records signed today will be forgeable once a quantum computer exists. Moving to post-quantum signatures for new records does nothing for records already signed.

This threat is also furthest behind on remediation. A 2024 review by AIVD, CWI and TNO of completed migrations at Google, Cloudflare and Meta found that post-quantum protection for confidentiality is mature and in wide use across the internet. Post-quantum signatures are not. Current post-quantum signatures are larger and slower to verify, which strains the certificate chains the web depends on.[7]

> CASE: AN AUSTRALIAN UNIVERSITY
>
> A 2026 cryptographic assessment of an Australian university's public-facing systems found some movement towards post-quantum key exchange, but no post-quantum digital signatures.[13] It also found no documented cryptographic standards policy, no algorithm review process, and no named person responsible for certificates, the quantum transition or cryptographic procurement. Some certificates had expired without anyone noticing. The university holds research data that must stay confidential for many years. The technical findings could be fixed within ASD's timeline. The lack of ownership was what had allowed them to build up, and ownership is a board question.

Threat 3: access (backdoors planted now, used later)

Means. No quantum computer is needed. This is what makes the threat exploitable today. The XZ Utils backdoor, found in March 2024, shows what means looks like here. A contributor using the name "Jia Tan" spent about two years building a record of genuine-looking work on an open-source compression library. The library is used in most Linux distributions. The contributor then inserted a backdoor.[17]

Opportunity. Created by the organisation's own change. Opportunity rises during mergers, new system builds, large vendor onboarding and adoption of open-source components: any period when new code or infrastructure is trusted before it has been tested. A post-quantum migration is itself a period of exactly this kind.

Motive. Documented. In February 2024, US agencies CISA, the NSA and the FBI issued a joint advisory with international partners.[18] It confirmed that the China-linked actor Volt Typhoon had placed access inside US critical infrastructure networks to enable disruption in a future crisis. The targets were industrial control systems for energy, water and transport. A compromise of this kind leads to physical disruption, not data loss.

In Australia, planted access is hardest to see in the parts of the energy system the law does not yet reach. The independent review of the SOCI Act was delivered to the Minister for Home Affairs on 31 January 2026. It found that the Act's asset thresholds do not reliably capture inverter manufacturers, aggregators or virtual power plant operators, which it named as major points of attack.[19]

What the model shows

	Means	Opportunity	Motive
1. Confidentiality	Not yet, except where classical weaknesses exist	Present: data crossing monitored networks	Present: espionage
2. Integrity	Not yet	Present by design: signatures are shared	Present: impersonation and fraud
3. Access	Present: no quantum computer needed	Present: created by change	Present and documented: disruption in a crisis

Table 3. Means, opportunity and motive for the three threats

> Opportunity and motive are present for all three threats. Means is missing for two of them, and present for the third. "There is no quantum computer to worry about yet" answers the wrong question.

Post-quantum migration addresses threats 1 and 2, by removing the means once new algorithms are in place. It does nothing for threat 3. That threat needs separate controls: knowing what components are inside the software the organisation deploys, checking where they came from, limiting what any single system is trusted to do by default, and assessing vendors' own security practices.

Seven elements of a threat model

A credible quantum threat model is more than a migration timeline. It is a structured answer, asset by asset, to three questions. Which threats apply? Do the actors able to exploit them have opportunity and motive? Which program is responsible for closing the gap? A threat model has seven elements.

1 **Map of assets and how long they must stay confidential.** What data exists, where it lives and how long it must stay confidential. The foundation for threat 1 (Chapter 4).

2 **Trust-dependency map.** Which processes rely on a signature that must stay valid for years: contracts, patents, intellectual property transfers, audited records and software releases. The foundation for threat 2.

3 **Map of periods of elevated trust.** The points where new systems, vendors or infrastructure are brought in with less scrutiny and more default trust. The foundation for threat 3.

4 **Vendor accountability.** Which vendors control the organisation's migration path for each threat, and whether each has given a dated, credible roadmap rather than a general assurance (Chapter 6).

5 **A means, opportunity and motive assessment for each asset.** Two assets with the same confidentiality requirement can carry very different urgency once opportunity and motive are considered.

6 **A named owner for each threat.** Threat 3 rarely falls within a program called "post-quantum migration". A risk that fits no existing program usually has no owner.

7 **A clear statement of what migration does not cover.** A program that does not name the gap for threat 3 has built a roadmap for two-thirds of the problem.

QUESTIONS TO TAKE FROM THIS CHAPTER

- Which of our data must stay confidential long enough that threat 1 already applies, and has it been prioritised? (Question 1)
- Which contracts, records and software releases depend on signatures that could be forged? (Question 4)
- Who makes sure nothing is being planted in the systems we are building, buying or onboarding now? (Question 4)

03 Directors' duties and the regulatory framework

Quantum risk does not need a new law to become a director's concern. Existing duties already reach it. This chapter brings together, in one map, the obligations that already apply. It starts with the duties every director owes and the guidance that settles foreseeability. It then covers the obligations that apply to most organisations, and those that apply by sector.

The map of obligations

Instrument	Who it applies to	What it means for quantum risk
Corporations Act, ss 180, 181, 189	All directors	Care and diligence on foreseeable risks; reliance on management only where reasonable
Corporations Act, s 912A	Australian Financial Services Licence holders (credit licensees have a similar duty under credit law)	Adequate risk management systems, including for cyber risk
ASD and AICD board priorities; ASD quantum guidance	Guidance for all boards	Makes quantum risk foreseeable for any director who pays attention, and sets the minimum engagement expected
Privacy Act 1988	Australian Government agencies and businesses with turnover above $3 million, plus some smaller businesses such as health service providers	Reasonable steps to protect personal information; large penalties
Cyber Security Act 2024	Organisations with turnover above $3 million (ransomware reporting)	Report ransomware and extortion payments within 72 hours
ASX Principles and continuous disclosure	Listed entities	Board oversight of non-financial risk; disclosure of material risk
APRA CPS 234, CPS 230, CPG 220 and FAR	APRA-regulated entities	Classify information assets; manage third-party risk; independent assurance; named individual accountability
SOCI Act	Owners and operators of critical infrastructure assets in 11 sectors	Incident reporting; for many asset classes, a risk management program and ownership register
PSPF and ISM	Non-corporate Commonwealth entities; suppliers through contracts	PQC transition plan; approved algorithms; procurement rules

Table 4. Australian obligations that reach quantum risk

Duties every director owes

Section 180 of the Corporations Act requires every director to act with the care and diligence a reasonable person would in their position.[20] Section 181 requires good faith and proper purpose. Section 189 allows

directors to rely on advice from management and experts, but only where the reliance is reasonable in the circumstances. A director may accept a presentation that says the risk is managed, without seeing an inventory, a roadmap or vendor assessments. That director will find it hard to show the reliance was reasonable.

Holders of Australian Financial Services Licences must also maintain adequate risk management systems under section 912A. Credit licensees have a similar duty under the National Consumer Credit Protection Act 2009. ASIC has used this provision, not section 180, in its cyber enforcement actions so far.

Two cases set the standard.

- **ASIC v RI Advice Group (2022).** The Federal Court found that RI Advice failed to have adequate systems to manage cyber risk, in breach of section 912A.[21] The court made declarations and ordered a $750,000 contribution to ASIC's costs. No civil penalty was imposed. The case established cyber risk management as part of a licensee's core obligations.
- **ASIC v FIIG Securities (2026).** The Federal Court ordered a $2.5 million civil penalty for sustained under-investment in cyber security controls between March 2019 and June 2023.[22] The case showed that having written policies is not enough if the controls are not operated.

ASIC Chair Joe Longo has said ASIC is looking for "the right case where company directors and boards failed to take reasonable steps or make reasonable investments proportionate to the risks that their business poses".[22] That case has not yet been brought against individual directors.

Guidance has settled the question of foreseeability

A director's duty of care is measured against what a reasonable director would have known. Australia's technical authority and the peak body for directors have jointly published guidance that names the risk and says what boards should do. A director cannot now credibly say the risk was unforeseeable.

The ASD and Australian Institute of Company Directors (AICD) publication *Cyber Security Priorities for Boards of Directors 2025–26* (30 October 2025) names quantum computing as a board responsibility.[2] It says boards should oversee steps to anticipate business requirements and dependencies for vulnerable systems during the transition to post-quantum standards. The publication asks three questions:

1 Have we acknowledged the long-term impact of quantum computing?

2 Have we assessed the potential impact of quantum threats to our systems and data?

3 Have we established a post-quantum cryptography transition plan?

In February 2026, ASD's Australian Cyber Security Centre (ACSC) published a primer on the cyber security risks of quantum computing.[23]

APRA's 2026–27 Corporate Plan, published on 20 August 2026, makes this expectation stronger.[24] It is a formal planning document, not a speech. Under its first strategic objective, APRA states it is increasing its focus on quantum computing risk. It cites ASD's recommended milestones and states that it expects entities to make timely progress on their transition plans, starting with their most critical information assets and operations. For APRA-regulated entities, this is a statement of what APRA will supervise against. More broadly, a formal commitment of this kind from the prudential regulator adds to the guidance that shapes the reasonable director standard. That standard applies to every director, not only those of APRA-regulated entities.

APRA Chair John Lonsdale told the 2026 ABA Banking Conference that non-financial and emerging risks are where risk management across APRA-regulated industries is "generally less mature".[25] Speaking about

geopolitical risk, he said awareness "has not always been matched by practical action". The same pattern applies to quantum risk.

ASD's milestones are recommendations, and they still matter

ASD recommends a refined transition plan by the end of 2026, transition started for critical systems by the end of 2028, and transition complete by the end of 2030.[3] The guidance uses "should". No Australian law attaches a penalty to missing these dates. They are still the clearest published statement of what a reasonable organisation would have done. A board that cannot show it engaged with them is more exposed than one that considered them and recorded a decision to defer.

The first milestone is now weeks away. Building a genuine plan from scratch takes longer than that for most organisations. A board that will not have a credible plan by the end of 2026 faces an interim question: what can it show a regulator or counterparty in the meantime, and what is the credible path to the 2028 milestone?

Privacy, cyber security and class actions

Privacy Act

The Privacy Act 1988 requires organisations to take reasonable steps to protect personal information.[26] Penalties for serious or repeated interference with privacy are the greater of $50 million, three times the benefit obtained, or 30 per cent of adjusted turnover.

These penalties are being used. In 2025, the Federal Court imposed the first civil penalty under the Act: $5.8 million against Australian Clinical Labs for a breach affecting 223,000 people.[27] Civil penalty proceedings against Medibank over its 2022 breach, affecting 9.7 million Australians, are under way.[28]

The Privacy and Other Legislation Amendment Act 2024 created a statutory tort for serious invasions of privacy from 10 June 2025.[29] It gives individuals a direct right to sue and is expected to be tested as a path for class actions after large data breaches.

A quantum-enabled decryption event could expose records covering decades and millions of people at once, at a scale the current enforcement record does not approach. A further question has not been tested: whether harvesting already under way is itself a notifiable data breach: one that must be reported to the regulator and to the people affected. Boards should seek legal advice on this, not rely on a technical view.

Cyber Security Act 2024

Since 30 May 2025, organisations with annual turnover above $3 million must report any ransomware or cyber extortion payment within 72 hours.[30]

Listed companies

The ASX Corporate Governance Council's *Principles and Recommendations* (4th edition) comment on board oversight of risk under Recommendation 7.2. They say a key role of a listed entity's board is to monitor the adequacy of its risk management framework, financial and non-financial.[31] Quantum risk is a non-financial risk with financial consequences, and falls within that role. During consultation, the Council considered listing cyber security as a required board skill and chose not to, partly to avoid implying that boards must be made up of experts. The board does not need to understand quantum cryptography. It needs to govern the risk.

Listed companies also face disclosure risk. The Medibank breach led to a shareholder class action alleging that Medibank failed to disclose weaknesses in its security.[28] A listed company that suffers a quantum-related breach after its board knew of the risk could face the same claim.

APRA-regulated entities

- **CPS 234 Information Security** has applied since 1 July 2019. It requires entities to identify and classify all information assets, including those managed by third parties, by criticality and sensitivity. The board is ultimately responsible.[32] Chapter 4 explains why this requirement is the foundation of any quantum response.
- **CPS 230 Operational Risk Management** has applied since 1 July 2025. It extends third-party risk management to all material service providers and requires entities to notify APRA before entering material offshoring arrangements.[33] A vendor's cryptographic readiness is now an operational risk question, not only an information security one.
- **CPG 220** describes three lines of defence: management owns the risk, an independent risk function challenges it, and internal audit assures the board.[34] A quantum program designed, run and reported on by the same team does not meet that standard.
- **The Financial Accountability Regime** has applied to banks since 15 March 2024, and to insurers and superannuation trustees since 15 March 2025.[6] APRA now requires superannuation trustees to name the Accountable Persons responsible for CPS 234 compliance.

Critical infrastructure

The SOCI Act requires operators of critical infrastructure assets in 11 sectors to keep and review a Critical Infrastructure Risk Management Program, and to report serious cyber incidents.[35] Owners and operators must also report ownership and control information to the Register of Critical Infrastructure Assets.

The independent review of the Act found that quantum cryptography vulnerabilities are among the risks the Act does not yet address. Recommendation 4 asks Home Affairs to examine the Act's coverage of quantum, AI and OT risk.[19] Directors should treat the Act's current scope as the minimum, not the limit. Proposed "Tranche Two" reforms would extend obligations to some suppliers (Chapter 6).

Commonwealth entities and their suppliers

The Protective Security Policy Framework (PSPF) is Australian Government policy. It is not legislation. It binds non-corporate Commonwealth entities, which include most federal departments and agencies.[36] Since 1 July 2026, PSPF Release 2026 has required those entities to:

- buy only new cryptographic products that support approved post-quantum algorithms (Requirement 0212), and
- develop, implement and maintain a post-quantum transition plan (Requirement 0223). The PSPF says the plan should apply ASD's LATICE method.

The PSPF does not bind private companies directly. It reaches them through contracts, deeds and panel arrangements with government. Directors of companies with Commonwealth contracts should ask which contracts carry PSPF obligations and what those obligations require. PSPF requirements also feed into government tenders, so quantum readiness can affect eligibility for future work.

The Information Security Manual (ISM) sets ASD's technical controls. It is mandatory for federal agencies through the PSPF and widely used as a benchmark by state agencies, universities, superannuation funds and critical infrastructure operators.[4] The September 2026 release:

- approves ML-KEM-768 and ML-KEM-1024 for key exchange (ISM-1995), and ML-DSA-65 and ML-DSA-87 for digital signatures (ISM-1991)
- requires new cryptographic equipment, applications and libraries to support ML-KEM-1024, ML-DSA-87, SHA-384, SHA-512 and AES-256 by 2030 (ISM-1917), after which the lower strengths lose approval
- states that RSA, Diffie-Hellman and elliptic curve algorithms will not be approved beyond 2030
- requires a post-quantum transition plan (ISM-2073), but does not itself set a date for it. The end-2026 date is ASD's planning milestone.

The ISM's guidelines for software development also recommend that developers provide customers with a Cryptographic Bill of Materials (CBOM), a list of the cryptography used in a product.[37] Asking a vendor for one is now a normal request.

Does D&O insurance respond?

Directors' and officers' (D&O) insurance covers directors and officers if they are personally sued over decisions made in those roles. Directors should not assume it covers personal liability arising from a cyber or quantum-related governance failure. Policies differ in how they treat cyber claims, and some claims after a data breach may fall under a separate cyber policy instead. The only way to know is to check the wording of the organisation's own policies with the broker. Chapter 8, Question 8, sets out what to ask.

INTERNATIONAL COMPARISONS

Australia's approach to board cyber duties has been built mainly through case law and guidance. Other jurisdictions have legislated more directly.

- The European Union's NIS2 Directive (Article 20) has been in force since October 2024. It makes the management bodies of the entities it covers responsible for approving and overseeing cyber security risk measures. Board members must also undertake cyber security training.[38]
- The UK's Network and Information Systems Regulations 2018 impose security and incident reporting duties on operators of essential services. The Cyber Security and Resilience Bill, introduced in 2025, would extend them.[39]

Australia may follow the same direction.

QUESTIONS TO TAKE FROM THIS CHAPTER

- Can the board answer ASD and the AICD's three questions with evidence? (Questions 1, 2 and 5)
- Which of our contracts carry PSPF obligations, and what is our disclosure position? (Question 7)
- Would our reliance on management's assurance be judged reasonable? (Question 8)

04 Know what you hold

A credible quantum risk response depends on knowing what the organisation holds: what sensitive data it has, where that data is, how it is protected and how long it must stay confidential. APRA's evidence suggests many organisations cannot answer these questions. This chapter explains why this knowledge comes first, how it connects to the cryptographic inventory, and how findings should reach the board.

What APRA found

APRA's CPS 234 has required every APRA-regulated entity to identify and classify its information assets, including those held by third parties, since 1 July 2019.[32] It applies to about 680 banks, insurers, superannuation trustees and private health insurers, which together oversee $9.8 trillion in assets.

Between 2020 and 2024, APRA ran "tripartite" assessments, involving APRA, the entity and an external auditor, of how more than 300 regulated entities were meeting CPS 234. Findings from the first group, covering about a quarter of APRA-regulated entities, were published in July 2023. They identified six gaps across the sector.[40] The most common was incomplete classification of critical and sensitive information assets.

The other five gaps were limited assessment of third parties, inadequate control testing, untested incident response plans, limited internal audit, and inconsistent reporting to APRA. Each depends on the first. If an entity does not know what data it holds, none of its other controls can be set correctly.

> Not weak encryption. Not missing controls. The most common failure in Australia's most regulated sector was not knowing what data it held.

The consequences of CPS 234 failures are financial. In July 2023, APRA increased Medibank's capital requirement by $250 million after its October 2022 data breach, to stay in place until an agreed remediation program was complete.[41] It was the first time APRA imposed a capital charge specifically for a cyber attack.

Why classification is the basis for prioritising migration

CPS 234 requires classification by criticality and sensitivity. ASD's guidance asks organisations to prioritise migration by how sensitive data is and how long it must stay confidential.[3] An organisation that has classified its information assets has already done the first step of a quantum risk assessment. Critical or highly sensitive data that must stay confidential for more than 10 years is the first place to look for quantum exposure.

The ASD milestone of a refined transition plan by the end of 2026 cannot be met without this work. If entities under APRA's supervision struggled to classify their information assets, the task for other organisations is at least as hard.

The cryptographic inventory extends the asset register

Classification tells an organisation what data is sensitive and where it is. A post-quantum transition also needs to know how that data is protected: which algorithms are used, where they are used in code, certificates and protocols, and whether they are vulnerable.

The **Cryptographic Bill of Materials (CBOM)** records this. It is the cryptographic layer added on top of the asset register. The order cannot be changed: discover the assets, classify them, then record the cryptography protecting them. An organisation without a complete asset register cannot build a credible CBOM, and without a CBOM it cannot build a credible migration roadmap.

Two gaps commonly undermine this work.

- **No one owns the link.** The data governance function owns the classification register. The cryptographic program owns the CBOM. The application inventory that connects them often has no owner.
- **Operational technology is left out.** Building management systems, physical access controls and industrial equipment are usually owned by facilities or engineering teams, not the chief information security officer (CISO). The cryptography in these systems will not appear in an IT-only inventory.

Holding less data also reduces exposure. Every dataset held under vulnerable encryption is a liability the organisation has chosen to carry. Retention and archiving policies should be reviewed against real business need. The same discipline applies in mergers and acquisitions: a buyer inherits all of the target's cryptography, including every unfixed exposure. Quantum readiness belongs on the due diligence checklist.

Getting findings to the board

Findings have to pass from the person who finds a certificate or classifies a dataset to the teams that rely on it, and then to the people who set policy and report to the board. Most organisations have no formal way for this to happen. A finding can stay in a security team spreadsheet and never reach the risk register.

The Financial Services Information Sharing and Analysis Center (FS-ISAC) Post-Quantum Cryptography Working Group has proposed a three-tier model for this problem.[42]

- **Key lifecycle operations** cover the assets: keys, certificates, cryptographic libraries and modules, and the rules for creating and retiring them.
- **Consumption operations** cover how those assets are used and monitored day to day.
- **Governance and compliance** cover the policies, architecture standards and third-party rules the other tiers must follow.

The model's main rule is that a change found at one tier must be passed to the other two tiers, not dealt with only where it was found. Examples are a new certificate, a reclassified dataset or a vulnerable algorithm found in a code scan. That is the discipline CPS 234 requires and the tripartite assessments found missing. Chapter 5 shows how the seven commitments of the transformation program fit across the three tiers.

Operational technology

Operational technology is usually the weakest part of the inventory. Control system inventories are often incomplete. Undocumented legacy devices stay in service for decades after the people who installed them have left. Asset registers built for IT tools often stop where OT begins.

For operators required to keep a SOCI Act risk management program, that program starts with the same step as CPS 234: identifying the assets that need protecting.[35] A board that has classified sensitive records but not the control systems running physical operations has done only half the inventory the Act requires.

SECTOR FOCUS: HIGHER EDUCATION

Universities hold sensitive data that must stay confidential for many years: research with commercial or defence value, partner data and student records. Defence-linked research can need protection for decades, which places it within threat 1 (Chapter 2).

- **Regulation.** Universities registered in the Australian university category of the National Register of Higher Education Providers are critical infrastructure assets under the SOCI Act. Only two obligations currently apply: mandatory cyber incident reporting, and telling data storage or processing providers that they hold business-critical data. Universities do not have to keep a Critical Infrastructure Risk Management Program.[43] Commonwealth contracts may also bring PSPF obligations (Chapter 3). The ISM is widely used as a benchmark in the sector.[4]
- **Structure.** Universities are decentralised. Faculties, research centres and partners often run their own systems or cloud services outside central IT. This makes a complete inventory harder to build.
- **What the evidence shows.** At one Australian university, the assessment in Chapter 2 found unnoticed expired certificates and no named owner for certificates, the quantum transition or cryptographic procurement.[13]
- **Where to start.** Councils should ask for: a classification of research data by how long it must stay confidential; a CBOM that includes faculty and research systems; and a named transition owner.

SECTOR FOCUS: SUPERANNUATION

Superannuation funds hold member records for a lifetime: identity details, contact details, employment history, beneficiaries and account balances. Much of this data must stay confidential for decades, longer than the period in which experts consider a quantum computer likely.

- **Regulation.** Trustees are APRA-regulated. CPS 234 requires classification of information assets, CPS 230 requires management of material service providers, and the FAR has applied to trustees since 15 March 2025.[32][33][6] Trustees must name the Accountable Persons for CPS 234.
- **Structure.** Many funds outsource administration, investment management, custody and technology. Much of the cryptography protecting member data is therefore run by service providers, which makes the vendor questions in Chapter 6 central.
- **Supervisory focus.** APRA's 2026–27 Corporate Plan says it is increasing its focus on quantum risk and expects timely progress on transition plans, starting with the most critical assets.[24]
- **Where to start.** Boards should ask whether: the classification register captures how long member data must stay confidential; each material service provider has given a CBOM and a dated roadmap; and an Accountable Person owns the transition.

QUESTIONS TO TAKE FROM THIS CHAPTER

- Can management table the classification register itself, showing how long each dataset must stay confidential? (Question 1)
- Does a CBOM exist, and does it reach operational technology and third parties? (Question 1)
- How do findings at the operational level reach the risk register and the board? (Question 6)

05 The transformation program

A post-quantum transition is not a one-off IT project. It reaches across procurement, legal, risk and the business, and it does not end when new algorithms are installed. This chapter explains why it differs from a conventional transformation and sets out seven commitments a board should obtain from management. Each commitment addresses a risk that ordinary program governance does not reach. Management delivers the commitments. The board's role is to obtain them, test them and minute what it finds.

A different kind of program

Most security initiatives add new controls to existing operations. A cryptographic transformation must work through every governance, procurement, policy and technology process the organisation already runs, because the vulnerable cryptography is built into those processes. Every purchase, system refresh, policy review and risk assessment either extends the exposure or reduces it.

	Conventional transformation	Cryptographic transformation
Pausing	Can be slowed or stopped if the business case weakens	Cannot be paused without cost. Data in systems not yet migrated can still be collected for later decryption.
Success	Visible: new features, uptime, savings	Invisible: done correctly, nothing appears to change
Deadline	Set and renegotiated by the organisation	Set by adversary capability, and cannot be confirmed until it is too late
Endpoint	Fixed: ends when the new system is live	Not fixed. Old algorithms must be retired, and monitoring continues after migration.
Verification	Functional: it works or it does not	Can pass every test while being subtly wrong
Compliance target	Fixed before the program starts	Will keep changing. Algorithms, required strengths, dates and regulation will all continue to evolve. The organisation must be able to change its cryptography again, which is called cryptographic agility.
Outsourcing	Many vendors and contractors can do the work	The skilled workforce does not yet exist in the numbers needed

Table 5. How a cryptographic transformation differs from a conventional one

Two further features set this program apart. First, it needs outside coordination at a scale most organisations have never managed, because standards and supply chains are global. Second, it needs automated, continuous discovery, because vulnerable cryptography is spread across code, certificates, protocols and data flows at a scale no manual process can cover. This matters more as attacks get faster. ASD has found that AI is speeding up the discovery and exploitation of vulnerabilities, and that defenders need to adopt these tools at least as quickly as attackers.[44]

The seven commitments at a glance

Commitment	The risk it addresses
1. Governance and risk management	A program designed, run and reported on by the same team, with no independent check
2. Policy	A policy that covers only future decisions, leaving older encrypted data, the target of harvesting, unaddressed
3. Awareness and training	Training records that show courses were completed, while the organisation cannot act under pressure
4. External collaboration and alignment	A migration planned alone that cannot finish, because counterparties still depend on the cryptography being retired
5. Procurement	Vendor risks that are visible only across the whole vendor base (Chapter 6)
6. Application and infrastructure lifecycle	Systems with no planned refresh have no migration path and stay vulnerable while the roadmap reports progress
7. Observability	Every other commitment produces a snapshot; without continuous monitoring, assurance becomes out of date from the day it is given

Table 6. Seven commitments a board should obtain

The first five commitments build cryptographic change into processes most organisations already run. The last two add a layer of visibility most organisations do not yet have: knowing which algorithms run where, and checking that migration is working.

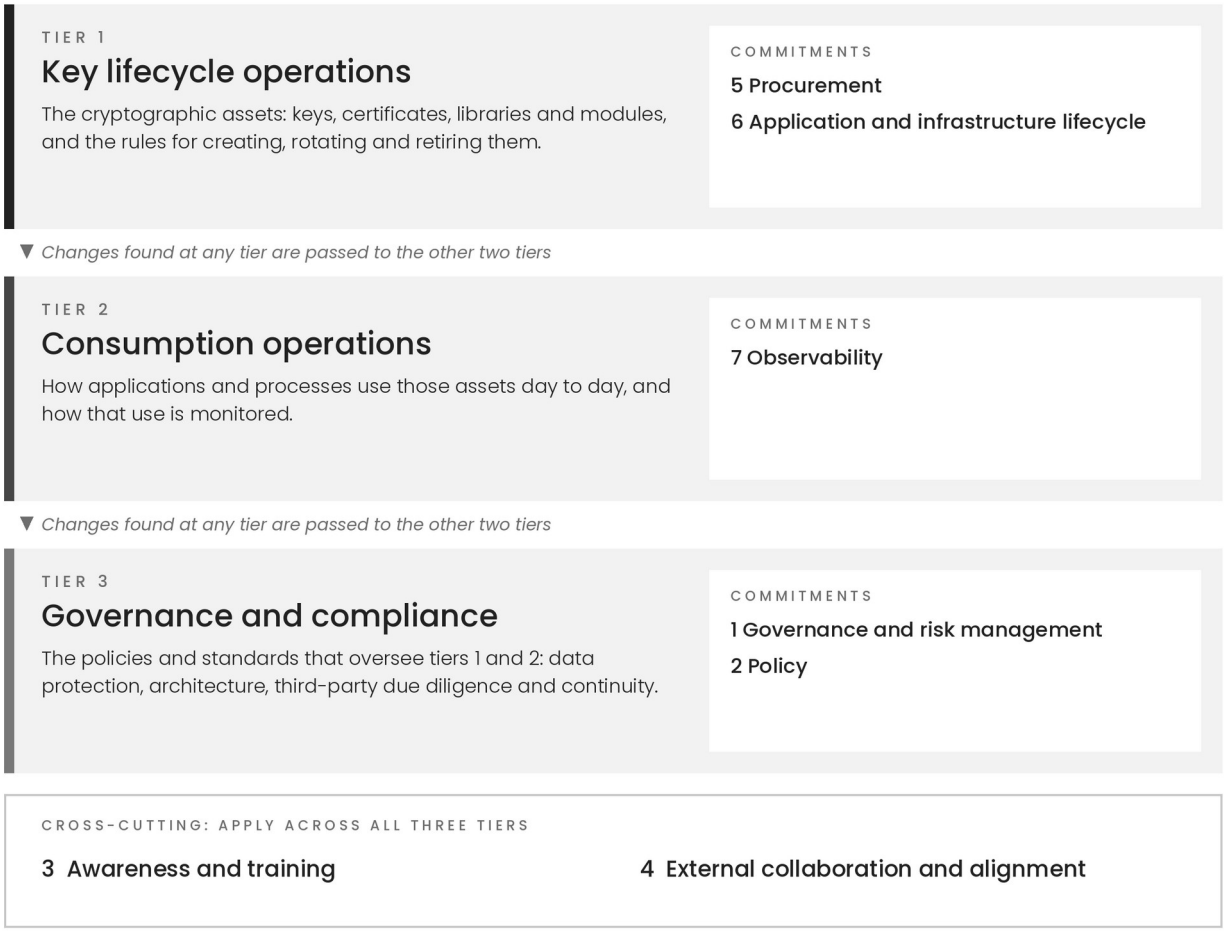


Figure 1. The FS-ISAC three-tier model, with the seven commitments mapped to it. Commitments 3 and 4 apply across all three tiers. Adapted from FS-ISAC PQC Working Group, Current State (Crypto Agility), 2023.[42]

1. Governance and risk management

Quantum risk must be part of the enterprise risk framework, not a separate security project. A program outside the risk register will not survive changes in leadership, budget cycles or competing priorities. Cryptographic risk should be as visible to the board as financial, operational and reputational risk.

The risk this commitment addresses is a program designed, run and reported on by the same team, with no independent check. APRA's CPG 220 expects three independent lines of defence (Chapter 3).[34] A structure that collapses all three into one IT or security team does not meet that expectation. For entities under the FAR, that is a named individual's failure.

Testing the cost estimate. Directors do not need to price the program to govern it. They need four tests for any estimate management presents:

- **Coverage.** Does it cover the whole program, including governance, training, outside collaboration and monitoring, or only technology?
- **Retiring old cryptography.** Does it fund the retirement of old cryptography, or stop when the new algorithms are deployed?
- **The cost of delay.** What does each year of deferral add? In earlier mandated migrations such as ISO 20022, late work cost more than planned work.

- **Scope beyond algorithms.** Changing algorithms is a small part of the total cost. Most of the cost is in changing applications and integrations, coordinating vendors, testing and re-certification, and running old and new cryptography side by side during the transition.

An estimate made before the inventory is complete, which does not show these categories separately, has probably not yet worked them out. A board should treat it as a preliminary range, not a budget.

> QUESTIONS FOR MANAGEMENT
>
> - Is quantum risk on the enterprise risk register, with independent second and third-line assurance?
> - Does the cost estimate pass the four tests above?

2. Policy

SHA-1, an older algorithm that NIST disallowed for digital signatures from the end of 2013, was still in wide use on websites in 2016. Organisations had a policy. It was not enforced where technology decisions were made. Browser makers extended SHA-1 support past their own deadlines to avoid widespread connection failures.[45] A cryptographic policy fails the same way unless it is built into information security policy, data classification and technology standards, and enforced at the point of design and purchase.

The policy's most important choice is where its list of approved algorithms comes from. Organisations should not write and maintain that list themselves. ASD's ISM maintains a list of approved algorithms and protocols. Adopting it by reference means the policy takes up every ASD update automatically.[4]

Every exception should be time-limited, individually justified and visible to the board, not a gap hidden in an otherwise clean compliance report. The US National Security Agency's CNSA 2.0 guidance offers a model: any unapproved algorithm needs a waiver specific to the algorithm, implementation and use, with no blanket exemptions.[46]

The risk this commitment addresses is a policy that governs only future decisions. The data most at risk from harvesting was encrypted before any policy existed. Mosca's inequality (Chapter 2) should be applied to data already stored, so that data already at risk is found and treated as a priority in its own right.

> QUESTIONS FOR MANAGEMENT
>
> - Does our policy adopt ASD's approved algorithm list by reference, with every exception time-limited, justified and visible to the board?
> - Has Mosca's inequality been applied to data we already hold?

3. Awareness and training

The shortage of post-quantum skills is well documented. A 2024 study for Entrust by the Ponemon Institute covered nine countries, including Australia and New Zealand. It found that awareness had risen sharply, but skills and technology had not grown at the same rate.[47]

Training must reach every role that makes cryptographic decisions, including directors, legal, procurement and engineering, with content specific to each. A single general briefing does not meet this need. The gap

between the specialist skills the program needs and those the organisation has should be a board-visible measure, with an owner and a date for closing it.

The risk this commitment addresses is training records that show courses were completed, while the organisation cannot act under pressure. A timed tabletop exercise, in which staff talk through a simulated cryptographic incident, tests whether roles work together. It also exposes gaps in escalation and decision rights that individual training records cannot show.

> QUESTIONS FOR MANAGEMENT
>
> - Has role-specific training been delivered and tested against a named competency framework?
> - Has a tabletop exercise been run, with findings reported to the board as a tested control?
> - Is the skills gap measured, reported to the board and closing on a dated timeline?

4. External collaboration and alignment

This commitment has no direct equivalent in conventional security programs. Standards bodies, including NIST, ISO and ETSI, are finalising post-quantum standards on overlapping timelines. Sector peers are migrating on different schedules. Regulation is changing at the same time. Most organisations do not need to help write the standards. They do need to take part in the bodies that coordinate how their sector adopts them.

- ASD's Cyber Security Partnership Program is open to any Australian organisation and has more than 149,500 partners.[48]
- FS-ISAC's PQC Working Group plays a similar role for financial services at a global level.
- Australia does not yet have equivalent sector-level coordination for post-quantum migration. That gap is itself a risk.

The risk this commitment addresses is a migration that cannot finish. FS-ISAC's September 2025 guidance shows why.[49] Suppose two institutions plan alone and sequence their work differently, one starting with secure web connections and the other with payment messaging. Neither can retire old cryptography from the links they share until both have migrated those links. The risk also applies in reverse. Once counterparties finish their migration, they will turn off support for old cryptography. Any organisation that has not moved will find those connections stop working, on the counterparty's timeline.

Delay does not reduce the work. FS-ISAC notes that it compresses the same tasks into less time, at higher cost.[49]

> QUESTIONS FOR MANAGEMENT
>
> - Are we an active participant, not only a registered member, in the coordination body for our sector?
> - Has our sequencing been tested against peer timelines and the chance that regulation changes before we finish?

5. Procurement

Every technology purchase made without a post-quantum readiness requirement creates exposure that must be fixed before the system reaches the end of its life. Four requirements belong in every procurement template, including those used by engineering and facilities teams for operational technology:

- a CBOM and a post-quantum transition roadmap from every technology vendor
- quantum readiness as part of third-party risk assessment
- approved algorithms as a condition of contract
- confirmation that the vendor protects the data it holds on the organisation's behalf with post-quantum cryptography.

The risk this commitment addresses is the set of vendor risks that are visible only across the whole vendor base.

Chapter 6 develops this commitment in full: what ASD's guidance asks of vendors, where it is incomplete, how to test vendor claims, and the risks the board should see across its vendor base.

6. Application and infrastructure lifecycle

This commitment carries out the migration: replacing vulnerable cryptography through existing development and infrastructure processes. Its organising method is ASD's LATICE method, which has five phases: Locate, Assess, Triage, Implement, and Communicate and Educate.[3] For non-corporate Commonwealth entities, PSPF Requirement 0223 requires a transition plan, and the PSPF says it should apply this method.[36]

For each system or use, the roadmap should show three dates:

1 when post-quantum cryptography is introduced

2 when old cryptography stops being added to new work

3 when old cryptography is retired.

The transition is not finished when the first post-quantum algorithm is deployed. It is finished when the last vulnerable algorithm is turned off. The third date is the one most often missing from roadmaps, and the one least often funded.

Hybrid modes can become permanent. A hybrid mode runs a post-quantum algorithm alongside an older one during the transition. Retiring the older algorithm delivers no new capability, so no one has a reason to fund it. Running both algorithms, designed to be temporary, then becomes permanent unless someone acts. A migration that stops there looks complete on a dashboard while the vulnerable algorithms keep running beside their replacements. The ISM says hybrid modes are "not recommended", although they are not prohibited.[4]

The risk this commitment addresses is the system with no planned refresh. Migration usually happens through upgrades and rebuilds. A system with no planned lifecycle event has no natural migration path. Unless it is identified and funded separately, it stays vulnerable.

Operational technology is the most serious case. OT is often replaced every 15 to 25 years, far longer than IT, and equipment installed today may still be running after ASD's 2030 milestone. A roadmap built on IT refresh cycles will leave out the assets with the longest exposure. OT often comes late in the sequence because it is hard to change. That does not make it less urgent.

QUESTIONS FOR MANAGEMENT

- Does the roadmap cover every vulnerable system, including OT outside the CISO's scope, with three dates for each?
- Are systems without a planned refresh funded separately?
- Is certificate renewal automated?

7. Observability

Conventional security monitoring detects active attacks. It cannot detect cryptography that weakens without any alert: a certificate renewed onto a vulnerable algorithm, a setting that reverts to an unapproved state, or harvesting of encrypted traffic. A board relying on conventional security reporting for cryptographic assurance is relying on reports that cannot show this risk.

This commitment provides continuous, automated discovery of which algorithms are in use, where, and whether they meet current standards. It should be reported in the same way as vulnerability exposure and patching are reported today.

A hard external deadline. The CA/Browser Forum is the industry body that sets rules for publicly trusted website certificates. It has set a timetable to shorten their maximum life to 200 days from March 2026, 100 days from March 2027 and 47 days from March 2029.[50] At 47 days, manual certificate management is not workable for any organisation of real size. Automation becomes a condition of staying online. Organisations that automate certificate management for this reason also gain the deployment capability post-quantum migration needs.

Machine identity and signatures. The integrity threat (Chapter 2) is concentrated in machine identities, such as the keys that sign firmware and software. It is most serious for firmware-signing keys on OT assets with service lives of 15 to 25 years. CNSA 2.0 gives priority to post-quantum firmware signing for this reason.[46] Without monitoring that reaches machine identities, these assets have no inventory and no owner for their migration.

Harvesting and privacy. If harvesting is a notifiable data breach, detecting and assessing it becomes a compliance task. Each suspected event should be checked against the CBOM, to see which algorithm protected the data at the time. It should also be checked against the classification register, to see how long the data must stay confidential. Together they show how long the exposed data will stay sensitive.

The risk this commitment addresses is assurance that goes out of date. The CBOM, policy, roadmap and training records were correct on the day they were approved. From that day, a certificate renewed onto the wrong algorithm, a reverted setting or a vendor update can undo them without anyone noticing. Continuous observability turns management assurance into evidence: dated, reviewable reports the board can point to if it is later asked what it knew and what it did.

QUESTIONS FOR MANAGEMENT

- Is the state of our cryptography monitored continuously, covering algorithms, systems that move away from their approved settings, certificate renewal, signs of harvesting and machine identities?
- Are suspected harvesting events checked against the CBOM and classification register?
- Has legal counsel advised on whether harvesting already under way could trigger notifiable data breach obligations?
- Does board reporting show that controls are working, not only that policies exist?

When an update misses a commitment

The seven commitments are not seven projects. They are one program, built into processes the organisation already runs. When a program update reaches the board without covering all seven, the director's response matters. Minute the gap. Ask which commitments are not addressed and when they will be. Ask for them to appear in the next update as standing items. A record of what the director asked for, and when, is what shows the director exercised oversight.

Post-quantum migration is a new discipline. Few organisations anywhere have completed a meaningful transition, and Australian experience is more limited still. That is not a reason to wait. The specialist capability every organisation will compete for by 2028 is being built now, inside the programs that started first.

QUESTIONS TO TAKE FROM THIS CHAPTER

- Does each program update cover all seven commitments? (Questions 2, 3, 5 and 6)
- Does the roadmap show three dates for every use, including OT? (Question 5)
- Is cryptographic assurance continuous, or a snapshot? (Question 6)

06 The supply chain

Most of the encryption that protects an Australian organisation is built into products and services it buys, and the organisation usually cannot change it without the vendor. Its transition can therefore move only as fast as its vendors. This chapter sets out where Australia's vendor guidance is incomplete and the steps a buyer should take to test vendor claims. It ends with the risks the board should see across its whole vendor base.

Four documents shape Australia's guidance

Document	What it does	Who it applies to
ASD, CISA and NSA, *Post-quantum questions to ask your vendors* (2026) [51]	Lists questions to ask vendors at each stage of a transition, and describes a good answer to each	Any organisation that buys technology
ASD and partners, *Choosing secure and verifiable technologies* (2024) [52]	General procurement guidance on vendor transparency, supply chain, data location, vendor access and geopolitical risk. It does not mention PQC.	Any organisation; reflected in PSPF Requirement 0048
Information Security Manual, Guidelines for cryptography [4]	Lists approved algorithms and requires new purchases to support specific PQC algorithms by 2030	Mandatory for federal agencies; widely used as a benchmark
Protective Security Policy Framework, Release 2026 [36]	Requires newly bought cryptographic products to support approved PQC algorithms (Requirement 0212) and a transition plan (Requirement 0223)	Non-corporate Commonwealth entities; suppliers through contracts

Table 7. Australian guidance on quantum risk in the supply chain

The documents point the same way. The ISM will not approve RSA or elliptic curve cryptography after 2030, so any product bought now and still in use then needs a clear path to post-quantum cryptography.

What ASD's vendor questions do well

ASD's vendor questions are a practical starting point for any organisation. They follow the five phases of ASD's LATICE method, so vendors' answers feed directly into the buyer's own plan. They begin by asking for a CBOM. They identify products that are hard to change, such as those with encryption built into firmware or hardware. They ask how long data stays in a vendor's products, which targets the harvesting threat. They cover governance, staff training and whether post-quantum support is included in standard licensing or sold as an extra.

Six limitations

The guidance tells buyers what to ask. It leaves six problems for buyers to solve.

Limitation	What it means for a buyer
1. No standard of proof	Each question describes a good answer, but not the evidence that proves it. A vendor can say its product "supports post-quantum cryptography" and the buyer has no way to test the claim.
2. Required algorithms not named	The questions refer buyers to the ISM. The ISM approves ML-KEM-768 and ML-DSA-65 only until 2030 and requires the stronger ML-KEM-1024 and ML-DSA-87 after that. A vendor that says "we support ML-KEM" may meet today's rules and still miss the 2030 requirement.
3. No way to compare or track vendors	Written answers give no common scale. Buyers cannot compare vendors or measure progress during a contract.
4. Roadmaps are not commitments	A roadmap shows intent, not delivery. The guidance offers no contract wording to turn a vendor's dates into obligations.
5. Mixed messages on 2030	The PSPF calls 2030 the ISM's "recommended" deadline, and ASD's vendor questions treat it as a target. The ISM itself ends approval of the older algorithms after 2030. Buyers and vendors may treat the same date as a goal or as a firm deadline.
6. No question of control	No question asks who owns the vendor, which governments can compel it, or who holds the encryption keys. ASD's procurement guidance covers some of this, but the two documents are not linked.

Table 8. Six limitations of Australia's vendor guidance

How the PQC Maturity Model helps

The PKI Consortium is an international non-profit industry body. Its members include technology vendors, certificate authorities, banks, government bodies and universities. Its Post-Quantum Cryptography Maturity Model (PQCMM) rates a product from Level 0 (no post-quantum support) to Level 5 (post-quantum on by default and independently certified).[53] Each level sets criteria and the evidence required. Products can be self-assessed, independently assessed or certified.

PQCMM fully addresses three of the six limitations and partly addresses one more.

Limitation	How PQCMM helps	Extent
No standard of proof	Every claim needs supporting evidence, such as test certificates and results of tests with other products. Unsupported claims are recorded as "vendor-stated, not independently verified".	Addressed
Required algorithms not named	Vendors must state the exact strength supported, such as "ML-KEM-768". PQCMM does not check this against the ISM.	Partly
No way to compare or track vendors	Six levels give a common scale for comparing vendors, setting a tender minimum and tracking progress.	Addressed
Roadmaps are not commitments	Vendors must give target dates for the next level. PQCMM's procurement guidance includes contract clauses that commit a vendor to a level by a date. Remedies for missed dates are left to the buyer.	Addressed
Mixed messages on 2030	PQCMM sets no dates.	Not addressed

Limitation	How PQCMM helps	Extent
No question of control	PQCMM assesses the product, not who owns or controls the vendor.	Not addressed

Table 9. How far PQCMM addresses each limitation

Buyers should also know four limits of PQCMM. A high level does not mean ISM compliance, because PQCMM does not specify algorithm strengths. It counts hybrid support as a sign of maturity, where the ISM does not recommend hybrids. It has no official standing in Australia. And it is new: version 1.0.1 is recent and few products have been assessed.

> DISCLOSURE
>
> The author is a member of the PKI Consortium PQC Working Group, which develops PQCMM.

Six steps for buyers

Buyers should combine ASD's vendor questions, PQCMM evidence and the ISM's algorithm list in six steps.

1. **Specify the algorithms.** Require ML-KEM-1024 and ML-DSA-87, with SHA-384 or SHA-512 and AES-256, either now or by a contracted date no later than 2030. Accept ML-KEM-768 and ML-DSA-65 only as an interim measure.
2. **Ask the vendor questions.** Use ASD's questions, scaled to how critical the product is and how long its data must stay confidential. Ask them of new vendors before contract, and of existing vendors at each renewal.
3. **Ask for evidence in PQCMM form.** Request exact algorithm strengths, a CBOM, release notes and test certificates. Level 2 (production-ready and standards-based) is a reasonable minimum for most new products.
4. **Ask who controls the cryptography.** Add the questions on data location, vendor access and geopolitical risk from *Choosing secure and verifiable technologies*. Also ask which governments can compel the vendor, who holds the keys, and where the cryptography was designed and tested. Record each supplier's country and ownership in the CBOM (Chapter 7).
5. **Put roadmaps in the contract.** Include post-quantum release dates, the move from hybrid modes to post-quantum only, and removal of older algorithms as contract milestones that can be checked. PQCMM's procurement guidance includes clause wording that can be adapted.
6. **Record what cannot be verified.** Where a vendor cannot support an answer, record the gap as a risk with an owner and a review date, not as a completed item.

> Use ASD's vendor questions to structure the discussion, PQCMM to test the answers, and the ISM to set the required algorithms. Then ask who controls the cryptography.

These steps are management's work. The board's role is to ask whether they are being followed, using Question 3 in Chapter 8.

Cloud software and operational technology

Software as a service (SaaS). For cloud software, the organisation has no technical control. If the vendor has not migrated, the data is not protected, whatever the organisation does elsewhere. Every high-sensitivity SaaS application should be covered by a recorded decision: a vendor commitment with a date, a reduction in the data entrusted to the service, or an explicit risk acceptance with a named owner.

Operational technology. OT is often bought by engineering and facilities teams outside the standard IT process. Those teams are unlikely to apply post-quantum requirements unless told to. The same requirements should be written into OT procurement templates, with a named owner for that change.

Risks the board should see across its vendor base

Some vendor risks are visible only when the board looks at its vendors as a whole, not one contract at a time. Others come from changes in law that affect many vendor relationships at once. A rigorous vendor-by-vendor process can miss both.

- **Concentration.** A small number of cloud key management platforms, hardware security module makers and certificate authorities supply most of the market. An organisation can diversify its vendor list and still depend on the same cryptographic supplier as its competitors. In June 2026, APRA Chair Lonsdale named concentration in the technology supply chain as something that makes shocks worse.[25] The Bank for International Settlements has found that poorly protected institutions can put the whole financial system at risk.[54]
- **Jurisdiction.** A vendor can meet every readiness requirement and still expose the organisation to a jurisdiction it never assessed. Each vendor's jurisdiction can be checked, but the board also needs to see how much of its total exposure sits under any one country's laws. Screening must happen before the contract is signed. Chapter 7 explains what to screen for.
- **Regulation reaching further into the supply chain.** The PSPF and APRA's prudential standards already reach suppliers. SOCI Act "Tranche Two" reforms, released for consultation in July 2026, propose a "relevant operator" concept that would extend obligations to some third-party service providers of critical infrastructure operators.[55] If enacted, directors of companies that supply critical infrastructure operators may face direct obligations they do not have today.
- **A broader prudential basis.** For APRA-regulated entities, CPS 230 makes a vendor's cryptographic readiness part of operational risk assessment, not only information security.[33] A vendor that cannot show a transition plan may fail both.

Readiness is now assessed in both directions

Clients, government agencies and APRA-regulated counterparties are adding post-quantum readiness to their own vendor questionnaires. An organisation will need the same evidence, a CBOM, a dated roadmap and confirmed algorithms, to pass their due diligence.

> QUESTIONS TO TAKE FROM THIS CHAPTER
>
> - Are new vendors assessed before contract, and incumbents at each renewal, with no critical contract renewing automatically? (Question 3)
> - Has every high-sensitivity SaaS application been covered by a recorded decision? (Question 3)
> - Is concentration risk visible across the vendor base as a whole? (Question 3)

07 Cryptographic sovereignty

Migrating to post-quantum algorithms answers whether an organisation's cryptography is strong enough. Migration says nothing about who owns the cryptography, who can compel access to it, where it came from, or whether Australia can check any of it independently. This chapter sets out those four questions.

More than data residency

Sovereignty is often equated with data residency: keep the servers in Australia. That captures only part of the question. The risks that follow from not asking the wider question are concrete:

- A foreign government compels a vendor to hand over keys or help decrypt data, without the organisation's knowledge.
- A foreign government suspends access to a critical service at short notice. In June 2026, the United States used export control powers to suspend access by non-US persons to two remotely accessed AI models for a period, before restoring it.[56]
- A vendor supplies information about the organisation's systems to a foreign government through an arrangement the organisation cannot see.
- Ownership of the infrastructure changes hands after contracts are signed, leaving the organisation without recourse.

None of these risks depends on whether the cryptography is technically strong.

Microsoft, IBM and SAP each divide digital sovereignty into the same three categories.[57] Data sovereignty asks whose law governs the data. Operational sovereignty asks who runs and maintains the systems. Technological sovereignty asks how much control the organisation has over the technology itself. Cryptography is present in all three at once. A board that addresses each category separately will find that cryptography falls between them.

The four questions

Question	What it asks	Australian instruments
1. Ownership	Who owns and controls the infrastructure the cryptography runs on, and could that change?	SOCI Act ownership register; Hosting Certification Framework
2. Compulsion	Which governments can legally compel the vendor to disclose or decrypt data?	Privacy Act (APP 8); Assistance and Access Act; foreign laws such as the US CLOUD Act
3. Provenance	Which jurisdiction designed, implemented and evaluated the cryptography?	ISM approved algorithms; AISEP evaluation
4. Capacity	Can Australia set, test and staff any of this independently?	Standards Australia; ASD milestones; the SOCI review

Table 10. The four questions of cryptographic sovereignty

1. Who owns and controls the infrastructure

The SOCI Act is the closest Australian law comes to answering the ownership question, though only for the entities it covers. Owners and operators of critical infrastructure assets must report ownership and control information to the Register of Critical Infrastructure Assets. The government has powers to act where a change of control threatens national security.[35] Ownership is treated as a national security matter, not only a commercial one.

The Hosting Certification Framework is now run by the Department of Home Affairs. It defines sovereignty as the government's ability to set and keep "stringent ownership and control conditions" over a service provider.[58] The government learned the cost of not having such conditions. In December 2016, a Chinese consortium bought a 49 per cent stake in the data centre operator Global Switch, rising to majority control by 2018. Commonwealth agencies' protection came from Foreign Investment Review Board conditions on the operator, not from their own contracts. Defence's main option was the expiry of its lease in September 2020. The scale of its holdings made that date impractical. It did not complete its move until June 2024.

The Framework binds only Commonwealth procurement. Its approach, ownership and control conditions set and kept by contract rather than assumed from location, is still a sound test for any board's own vendors.

2. Whose laws can compel access

Australian privacy law creates accountability, not protection. Australian Privacy Principle 8 allows personal information to go to overseas vendors if the organisation takes reasonable steps to protect it, such as contract terms.[59] The Australian organisation stays accountable if the overseas recipient mishandles it. This protection fails when a foreign government compels the vendor. The vendor discloses because another government requires it, not by choice, and the accountability stays with the Australian organisation.

Compulsion works in both directions. Australia's Assistance and Access Act 2018 lets agencies require communications providers to help access encrypted communications, short of building a mandated backdoor. This includes software developers and device makers, wherever they are based.[60] Any vendor supplying cryptographic infrastructure into Australia falls within its reach.

The reverse exposure is the one boards miss. The US CLOUD Act lets US law enforcement, with a warrant or other valid legal order, compel a US-based provider to produce data it controls, wherever that data is stored.[61] A key management service or certificate authority run by a US-headquartered vendor can be compelled to produce Australian data even when every server is in Sydney under an Australian contract. Data residency answers where data is stored. It does not answer whose law can reach the company that holds the data.

New routes for disclosure. In August 2026, a US presidential memorandum authorised vetted US private companies, under the direction of the US Departments of Justice and Homeland Security, to carry out cyber surveillance and operations against foreign criminal networks.[62] Participating companies can enter commercial agreements with other private entities to receive threat intelligence those entities gather in their normal business. Any US vendor, or one of its subcontractors, could share intelligence with a participant. Data about a client could flow into that program without the client knowing.

Other jurisdictions. China's National Intelligence Law requires organisations and citizens to support intelligence work on demand, without court process.[63] Australia has acted on this risk. In February 2025, the Government banned DeepSeek from government systems because its data collection exposed government data to "extrajudicial directions from a foreign government".[64] That is a formal finding that compulsion risk alone justifies removing a product. India's Information Technology Act allows the Central Government to

direct interception or decryption, and to require providers to hand over keys, with ministerial approval and no independent judicial review.[65] A close strategic relationship is not a substitute for legal assessment.

3. Where the cryptography comes from

The post-quantum algorithms on both Australia's and Europe's approved lists were designed and standardised by one foreign body, NIST, in August 2024.[8] Australia and the European Union are each deciding independently whether to approve algorithms designed elsewhere. That is a narrower kind of independence than it sounds.

ASD's ISM defines ASD-approved cryptographic algorithms and protocols, and requires High Assurance Cryptographic Equipment for the most sensitive government data.[4] Products are evaluated through the Australian Information Security Evaluation Program (AISEP).[66] These requirements bind government agencies and vendors selling into government. They do not bind private organisations, which may choose to adopt them as good practice.

Europe keeps its own list. The European Cybersecurity Certification Group publishes *Agreed Cryptographic Mechanisms*, now in its second version, with a third released for public review in mid-2026.[67] The Australian and European lists are not identical and are maintained by different governments. "Approved cryptography" is never a universal fact. It is always a claim made within a jurisdiction.

Some governments are reducing their dependence on US standards. China and Russia are developing domestic post-quantum algorithms, reportedly in part from concern that Western standards could carry undisclosed access.[68][69] South Korea, a close US ally, selected its own national algorithms in January 2025 to keep independent standards.[70] Organisations operating in those markets may run cryptography designed by a different government and evaluated against different criteria.

"Sovereign" and "government-grade" encryption are marketing phrases with no fixed legal meaning outside a named certifying body's framework. A board that hears such a claim should ask which government approved it, for what classification of data, and through which named evaluation process.

4. Australia's independent capacity

The first three questions assume Australia has some capacity to act on the answers. That assumption deserves scrutiny.

- **Standards.** Standards Australia mirrors international post-quantum work through its IT-012 committee. Its January 2025 position paper recommends adopting international standards, which describes a country that adopts standards rather than sets them.[71]
- **Testing.** The standard the ISM relies on for validating cryptographic modules, FIPS 140-3, is run by NIST and the Canadian Centre for Cyber Security. Australia has no domestic equivalent, and no local equivalent of the NIST centre that tests post-quantum migration with industry.[72]
- **Workforce.** Federal workforce programs are general. The Growing and Professionalising the Cyber Security Industry Program is a two-year, $1.9 million grant with no post-quantum focus.[73] Boards should not assume the market will supply specialists on their preferred schedule.
- **A link to law.** ASD's timeline is more demanding than comparable UK and EU guidance, but nothing in statute enforces it. The SOCI Act review recommended only that Home Affairs examine the gap.[19]

On 22 June 2026, US Executive Order 14412 set a fixed migration schedule for federal high-value assets and high-impact systems: post-quantum key establishment (exchanging encryption keys) by the end of 2030 and digital signatures by the end of 2031. It also directed that federal contractors be required to comply with

NIST's standards, including the post-quantum standards, by the end of 2030.[74] Every major vendor selling into the US federal market will align with those dates. The timeline for the cryptography most Australian organisations will run has, in practice, been set by the US Government.

There is no post-quantum statute in Australia and no direct penalty for missing ASD's milestones. There is also no safe harbour. Several existing duties reach foreseeable risk whether or not a statute sets a date. They include the duty of care under section 180, CPS 234 for APRA-regulated entities, and the risk management program for SOCI operators. ASD approval or AISEP certification is a minimum, not independent assurance: both rest on standards, testing and algorithms Australia does not control.

The financial sector's version of the ownership question

CPS 230 requires APRA-regulated entities to keep a register of material service providers and to notify APRA before entering a material offshoring arrangement.[33] Where key management is outsourced to an offshore-controlled cloud provider, that should be assessed against the same threshold. In practice it rarely is. Key management is treated as a technical control, and organisations ask where the data centre is, not who controls the keys.

Boards of regulated entities should ask management to assess whether offshore-controlled key management meets the notification threshold, and to record the conclusion either way. In a supervisory review, an assessment never made looks the same as an exposure never noticed. Meeting CPS 230 is necessary. Because the Bank for International Settlements has found the risk is system-wide (Chapter 6), it is not sufficient.[54]

Why the transition is the time to act

Most organisations running a post-quantum transition will build or refresh a cryptographic inventory, because an algorithm cannot be replaced until it has been found. That makes the transition the broadest chance to address sovereignty, across every dependency at once rather than one contract at a time.

FS-ISAC already recommends a supplier field in cryptographic inventories.[42] Extending it to record each vendor's country of incorporation and compulsion exposure turns a routine task into a sovereignty assessment. Boards that leave sovereignty for later are still making a decision: to accept the exposure.

Moving key management away from a US-headquartered platform is not always possible, and is often not the right fix. The exposure is legal, not technical, and control over who holds the keys addresses it more directly than moving the platform. What every organisation can do is make the exposure visible, ranked by what a compelled disclosure would reveal.

> Full sovereignty is not achievable for most Australian organisations in the time a post-quantum transition takes. The choice is between managed and unmanaged dependence.

Where sovereignty fits in existing governance

None of this needs a new governance framework. Each part fits an existing process:

- the cryptography policy, where ownership and compulsion exposure can be recorded against the instruments that create it

- the exceptions register, which can record a vendor's foreign-law exposure, with a date to fix it, as it does for a delayed migration
- existing committees, such as an architecture review board or third-party risk committee, which can take on a sovereignty mandate without structural change.

QUESTIONS TO TAKE FROM THIS CHAPTER

- Which of our key management vendors are subject to foreign compulsion powers, and does our CBOM record vendor jurisdiction and ownership? (Question 3)
- Have we tested "government-grade" claims against a named evaluation process? (Question 3)
- For APRA-regulated entities, has offshore key management been assessed under CPS 230? (Question 7)

08 The questions boards should ask

The earlier chapters explain the risk, the obligations and what a credible response contains. This chapter turns them into eight questions a board can put to management. The questions are those a board would ask about any material risk. What changes is the evidence a board should demand before it accepts an answer. Questions raised in earlier chapters are included under the eight, so there is one list to work from.

Why eight questions

Risk oversight has seven tasks a board cannot skip: know the exposure, name the owner, stop adding to it, test the plan and its cost, check the reporting, know existing obligations, and protect the board itself. Quantum risk adds an eighth: the two threats a program focused on encryption tends to miss. Any experienced director could ask the first seven unprompted. What they may not know is what an adequate answer looks like. Each question below sets out the evidence a credible answer contains, and what to do when it is missing. A board that can answer only Questions 1 and 2, what is at stake and who owns it, has awareness. It does not yet have oversight.

Three features of quantum risk raise the standard of evidence:

- **The harm cannot be undone.** A board cannot treat this as a risk to monitor until it occurs.
- **There are three threats.** All three need attention now. Two of them, forged signatures and planted access, are often left out of the program (Chapter 2).
- **The evidence base is weaker than usual.** Cost benchmarks vary widely, with no consistent method behind them.

1. Do we hold data or systems that would be seriously damaging if exposed, and do we know where they are?

Any long-lived sensitive data protected by vulnerable encryption is already a target. Health records, legal advice, financial transactions, research and strategic plans all qualify.

A credible answer includes:

- the data classification register itself, not a summary, showing how long each dataset must stay confidential (Chapter 4)
- a CBOM showing where vulnerable algorithms protect that data, including in OT and vendor products
- evidence that retention policies have been reviewed, so the organisation is not protecting more data than it needs
- quantum readiness on the due diligence checklist for mergers and acquisitions.

Also ask: Which of our data must stay confidential long enough that harvesting is already a risk, and has it been prioritised for migration?

IF THE ANSWER IS INADEQUATE

Minute that neither record exists. Without a classification register and a CBOM, the program has no verified basis. Set a date for both to be tabled. Do not approve major program spending until they exist. If management cannot commit to a date, commission independent assurance rather than wait for a self-reported update.

2. Who owns this risk, and is it managed or only recorded?

The program reaches into cyber security, technology, risk, legal, privacy, procurement and the business. A risk owned entirely by IT or security is not adequately governed.

A credible answer includes:

- the three lines of defence in APRA's CPG 220 (Chapter 3)
- a risk appetite the program can make decisions against, such as how much long-lived sensitive data the board will accept under vulnerable protection, and for how long
- a named committee owner. A risk committee is the usual place for appetite and progress reporting. The audit committee should commission independent assurance. A board without separate committees should assign both roles in its terms of reference.

Being on the risk register is a threshold, not the full answer. An entry rated low likelihood and high impact, assigned to the CISO and reviewed once a year, is acknowledgment. It is not management.

IF THE ANSWER IS INADEQUATE

Minute that the structure does not meet the CPG 220 standard. For APRA-regulated entities, this is a named individual's exposure under the FAR. Require a three-lines structure and a named Accountable Person by a date the board sets. The audit committee should not accept self-certification.

3. Are we still creating new exposure through what we buy and what we build?

This is one discipline in two forms: do not buy new exposure, and do not build it.

A credible answer includes:

- post-quantum requirements in every procurement template, including OT, with new vendors assessed before contract and incumbents at each renewal (Chapter 6)
- algorithm strengths specified against the ISM, and vendor claims tested with evidence, using a tool such as PQCMM
- every high-sensitivity SaaS application covered by a recorded decision
- concentration risk visible across the vendor base as a whole
- a cryptographic policy built into architecture review and procurement approval, with an exception register the board can see
- Mosca's inequality applied to data already held (Chapter 5).

Also ask about sovereignty (Chapter 7):

- Which of our key management vendors are subject to compulsion powers that reach data they control, wherever it is stored?
- Could a foreign government suspend a cryptographic service we depend on, and which services are most exposed?
- Could any vendor be supplying information about us to a foreign government through an arrangement we cannot see, and do our contracts address this?
- Does our CBOM record vendor jurisdiction and ownership, or only algorithms and key types?
- Where a vendor claims "government-grade" or "sovereign" encryption, have we asked which government approved it, for what data, and through which named process?
- Have we tested whether the ownership and control conditions in the Hosting Certification Framework should apply to our own critical vendor contracts?

> IF THE ANSWER IS INADEQUATE
>
> Minute which procurement categories lack post-quantum requirements. Set a date for templates to be updated and vendor assessments completed. For APRA-regulated entities, an unassessed material vendor is a current CPS 234 and CPS 230 gap. Ask for the exception register. If it does not exist, the policy is not enforced, and that is the finding. Do not accept "we are working on it" without a named owner and a date.

4. Are we governing forged signatures and planted access, not only harvested data?

Signature forgery. Every record signed under today's algorithms, including contracts, audit logs and code-signing certificates, will be forgeable once a quantum computer exists. A forged record that looks genuine is more dangerous than a missing one. Moving to post-quantum signatures for new records does nothing for records already signed. Firmware-signing keys on OT are the most exposed case.

Planted access. State actors use ordinary intrusion methods to plant hidden access in critical systems, for use in a future crisis. Migration does not remove this access. The change migration requires, new systems, new vendors and integration work, creates the conditions attackers use to plant it.

A credible answer includes:

- a named owner for each threat, not only for the confidentiality migration
- an inventory of signatures that must stay valid for years: contracts, patents, intellectual property transfers, audited records and software releases
- controls for periods of elevated trust, such as mergers, new builds and vendor onboarding
- for SOCI-regulated entities, explicit coverage of both threats in the risk management program.

Also ask: Given that planted access needs no quantum computer at all, who makes sure nothing is being planted in the systems we are building, buying or onboarding now?

IF THE ANSWER IS INADEQUATE

Minute that the program names no owner for forged signatures or planted access. Require one for each. For SOCI-regulated entities, confirm the risk management program covers both explicitly, rather than assuming the migration program covers them.

5. Is there a credible roadmap and cost estimate?

ASD's first milestone, a refined plan by the end of 2026, is weeks away. The next is transition started for critical systems by the end of 2028.

A credible answer includes:

- three dates for each major use: when post-quantum cryptography starts, when old cryptography stops being added to new work, and when old cryptography is retired (Chapter 5)
- separate funding for systems with no planned refresh, including OT
- a cost estimate anchored to the inventory, phased, with a confidence range and an owner who tracks actual spend, and passing the four tests in Chapter 5
- the skills gap reported as a number, with an owner and a closing date
- evidence of active participation in the relevant sector coordination body, with sequencing tested against peers' timelines.

Do not accept an estimate expressed as a percentage of IT security spend. Published figures of that kind vary widely, with no consistent method.

IF THE ANSWER IS INADEQUATE

A roadmap without three dates per use is incomplete. A roadmap without a CBOM behind it cannot be verified. If a credible plan will not exist by the end of 2026, require an interim position: what the board can show a regulator or counterparty today, and the credible path to the 2028 milestone. A percentage-of-budget figure is not a program budget.

6. Can we trust what we are told?

ASIC v FIIG Securities established that sustained under-investment in controls breaches licensee obligations even where written policies exist. A board therefore needs evidence that controls actually work. Cryptography can weaken without any alert, so for this risk that evidence has to be continuous, not a periodic snapshot.

A credible answer includes:

- automated, continuous monitoring of algorithms, systems that move away from their approved settings, certificate renewal, signs of harvesting and machine identities (Chapter 5)
- progress reported by domain: enterprise IT, OT, cloud services and third parties. An organisation 90 per cent migrated in IT but 10 per cent in OT should not report one combined figure.
- automated certificate management, ahead of the 47-day certificate limit from March 2029
- suspected harvesting events checked against the CBOM and classification register

- an independent test of whether the organisation's cryptography meets its own risk tolerance, rather than treating ASD approval or AISEP certification as independent assurance (Chapter 7).

> IF THE ANSWER IS INADEQUATE
>
> Annual point-in-time assessments cannot show that cryptographic controls are still working. Require confirmation that automated monitoring is in place, and reporting split by domain. One percentage figure is not assurance.

7. What do we already owe under law and contract?

A credible answer includes:

- for listed companies, a considered assessment of whether quantum risk is material for continuous disclosure purposes. An assertion that no disclosure is needed is not an assessment.
- a list of Commonwealth contracts that carry PSPF obligations, and what each requires (Chapter 3)
- legal advice on whether harvesting already under way could trigger notifiable data breach obligations
- for APRA-regulated entities, an assessment of whether offshore-controlled key management is a material offshoring arrangement under CPS 230, recorded either way (Chapter 7)
- for suppliers to critical infrastructure operators, an assessment of how proposed SOCI Act reforms would affect them.

The exposure works in both directions. Government tenders increasingly embed PSPF requirements, and APRA-regulated customers will check vendor readiness under CPS 230.

> IF THE ANSWER IS INADEQUATE
>
> For a listed company, the absence of a considered disclosure assessment is itself a governance gap. Require a written opinion from legal counsel, not a management assurance. Ask the general counsel to review government contracts for PSPF obligations and report at the next meeting.

8. If this goes wrong, what protects us personally?

D&O insurance may not cover personal liability arising from a cyber or quantum-related governance failure (Chapter 3). Section 189 allows directors to rely on management only where that reliance is reasonable. Accepting a presentation that says the risk is managed, without seeing an inventory, a tested roadmap or vendor assessments, is not reasonable reliance.

Reliance is judged after the event. A practitioner framework by Marin Ivezic identifies three records that help a board show it acted reasonably:[75]

- risk acceptance decisions, with reasons and review dates
- budget requests, including those refused, as evidence the risk was raised
- an annual record of how the threat was reassessed.

A documented decision to defer is defensible. Undocumented inaction is not.

IF THE ANSWER IS INADEQUATE

Before the next D&O renewal, ask the broker for a written opinion on whether personal liability from a quantum governance failure is covered. If the answer is uncertain or negative, understand the uninsured exposure before a breach, not after. Commission independent assurance on the program, not because management has failed, but because reasonable reliance cannot rest on the same team attesting to its own work.

A modest minimum for smaller organisations

The standard is about quality, not size. Directors of smaller entities should not read the attention on APRA-regulated institutions as meaning this applies only to large organisations. The section 912A standard was set in proceedings against a financial advice licensee, not a major bank. A minimum credible response is modest:

1. Put the risk on the register with a named owner.
2. Classify records that must stay confidential for 10 years or more.
3. Require post-quantum roadmaps from critical vendors as a standing procurement condition.
4. Review a one-page migration position at board level each year.

What to do when any answer is inadequate

When an answer is inadequate, minute the finding. Set a date for the gap to close. Where it stays unsatisfactory, use the board's ordinary tools: independent assurance, external review and a standing agenda item. Relying on an answer the board had reason to doubt is not reasonable reliance.

> The governance question is narrow and already answerable. Does this organisation hold data, systems, supplier relationships or customer promises that must still be trustworthy when the cryptography that protects them changes? And can the board show, with evidence rather than assurance, that it knows the answer?

Milestones timeline

The timeline brings together the dates that matter for Australian boards. ASD's milestones are recommendations. The ISM and PSPF dates apply to Commonwealth entities and, through contracts, to their suppliers. NIST's dates are proposals in a draft. The US dates will shape vendor roadmaps.

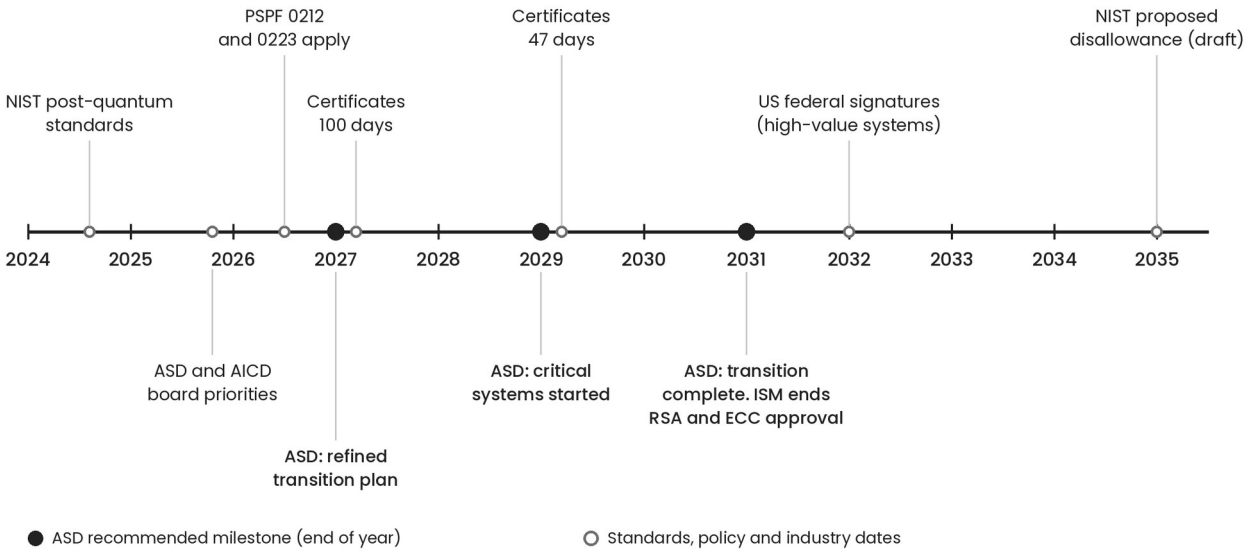


Figure 2. Key post-quantum milestones for Australian boards, 2024 to 2035

Date	Milestone	Status
August 2024	NIST publishes the first post-quantum standards: ML-KEM (FIPS 203), ML-DSA (FIPS 204) and SLH-DSA (FIPS 205)[8]	Final standard
November 2024	NIST proposes deprecating quantum-vulnerable algorithms after 2030 and disallowing them after 2035[76]	Draft proposal
October 2025	ASD and AICD name quantum computing as a board responsibility[2]	Guidance
February 2026	ACSC publishes guidance on the risks of quantum computing[23]	Guidance
March 2026	Public TLS certificate validity limited to 200 days[50]	Industry rule, in force
June 2026	US Executive Order 14412 sets federal migration dates[74]	US federal policy
1 July 2026	PSPF Requirements 0212 and 0223 apply[36]	Policy for Commonwealth entities
August 2026	APRA's Corporate Plan names quantum risk as a supervisory focus[24]	Regulator plan
End of 2026	Refined, organisation-specific transition plan[3]	ASD recommended milestone
January 2027	New US national security system acquisitions must comply with CNSA 2.0[46]	US requirement
March 2027	Public TLS certificate validity limited to 100 days[50]	Industry rule

Date	Milestone	Status
End of 2028	Transition started for critical systems and long-lived sensitive data[3]	ASD recommended milestone
March 2029	Public TLS certificate validity limited to 47 days[50]	Industry rule
End of 2030	Transition complete. RSA, Diffie-Hellman and elliptic curve algorithms no longer approved in the ISM. Key establishment migrated in US federal high-value and high-impact systems.[3][4][74]	ASD milestone; ISM; US policy
End of 2031	Digital signatures migrated in US federal high-value and high-impact systems[74]	US federal policy
2035	NIST's proposed disallowance of quantum-vulnerable algorithms; CNSA 2.0 full migration target[76][46]	Draft proposal; US target

Table 11. Milestones in date order

Glossary

Term	Meaning
ACSC	Australian Cyber Security Centre, part of ASD.
AISEP	Australian Information Security Evaluation Program, ASD's scheme for evaluating IT security products.
APP 8	Australian Privacy Principle 8, which governs sending personal information overseas.
APRA	Australian Prudential Regulation Authority, which regulates banks, insurers and superannuation funds.
ASD	Australian Signals Directorate, Australia's technical authority on cyber security.
CBOM	Cryptographic Bill of Materials: a list of every cryptographic algorithm, library, key and certificate a system or product uses.
Certificate	A digital document that binds a public key to an identity, such as a website or a software publisher.
CNSA 2.0	The US National Security Agency's algorithm requirements for national security systems.
CPS 230	APRA's standard on operational risk management, including material service providers.
CPS 234	APRA's standard on information security.
Cryptographic agility	The ability to change cryptographic algorithms quickly as standards and threats change.
Digital signature	A cryptographic method of proving who created a record and that it has not been changed.
FAR	Financial Accountability Regime, which makes named individuals in APRA-regulated entities accountable.
FIPS 203, 204 and 205	NIST's first post-quantum standards, published in August 2024.
FS-ISAC	Financial Services Information Sharing and Analysis Center, a global industry body.
Hybrid mode	Running a post-quantum algorithm alongside an older one during the transition.
ISM	Information Security Manual, ASD's set of security controls.
LATICE	ASD's five-phase transition method: Locate, Assess, Triage, Implement, and Communicate and Educate.
ML-DSA	Module-Lattice-Based Digital Signature Algorithm, the main post-quantum signature standard (FIPS 204).
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism, the main post-quantum standard for exchanging keys (FIPS 203).
Mosca's inequality	A test of whether data is already at risk: if the years data must stay confidential plus the years migration will take exceed the years until a quantum computer exists, it is at risk now.

Term	Meaning
NIST	US National Institute of Standards and Technology.
OT	Operational technology: systems that control physical equipment, such as power, water and building systems.
PKI	Public key infrastructure: the system of keys and certificates used to establish trust online.
PQC	Post-quantum cryptography: algorithms designed to resist attack by quantum computers.
PQCMM	The PKI Consortium's Post-Quantum Cryptography Maturity Model.
PSPF	Protective Security Policy Framework, the Australian Government's protective security policy.
Public-key cryptography	Cryptography that uses a pair of keys, one public and one private. RSA and elliptic curve cryptography are examples.
SaaS	Software as a service: software run by a vendor and used over the internet.
SOCI Act	Security of Critical Infrastructure Act 2018.
TLS	Transport Layer Security, the protocol that secures web and many other connections.

Table 12. Glossary of terms

Sources

[1] Global Risk Institute, *Quantum Threat Timeline Report 2025* (March 2026). Survey of 26 experts.

[2] Australian Signals Directorate and Australian Institute of Company Directors, *Cyber Security Priorities for Boards of Directors 2025–26* (30 October 2025), cyber.gov.au.

[3] Australian Signals Directorate, *Planning for post-quantum cryptography* (first published July 2022, updated September 2025), cyber.gov.au. Source of the 2026, 2028 and 2030 milestones and the LATICE method.

[4] Australian Signals Directorate, *Information Security Manual*, Guidelines for cryptography (September 2026). Controls ISM-1917, ISM-1990, ISM-1991, ISM-1995, ISM-1996 and ISM-2073.

[5] *ASIC v Hellicar* [2012] HCA 17. High Court decision on James Hardie director liability.

[6] *Financial Accountability Regime Act 2023* (Cth). Applies to banks from 15 March 2024 and to insurers and superannuation trustees from 15 March 2025.

[7] AIVD, CWI and TNO, *The PQC Migration Handbook*, revised and extended second edition (December 2024). Technical handbook; source for Mosca's inequality, adopter categories and the review of migrations at Google, Cloudflare and Meta.

[8] US National Institute of Standards and Technology, FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA) (August 2024).

[9] SWIFT, ISO 20022 migration programme (2022–2025), swift.com. Coexistence period ended November 2025.

[10] US Federal Reserve Board and Office of the Comptroller of the Currency, joint press release (16 September 1999). Reports 99.7 per cent of insured institutions rated satisfactory for Y2K readiness.

[11] Office of Management and Budget, *Report on Post-Quantum Cryptography*, as required by the Quantum Computing Cybersecurity Preparedness Act (July 2024). The cost projection was prepared by the Office of the National Cyber Director with OMB, CISA and NIST.

[12] C. Gidney (Google Quantum AI), *How to factor 2048 bit RSA integers with less than a million noisy qubits*, arXiv:2505.15917 (May 2025).

[13] Cryptographic assessment of an Australian university (2026). Client identity withheld.

[14] Australian Signals Directorate, *Annual Cyber Threat Report 2024–25* (14 October 2025), cyber.gov.au.

[15] Australian Security Intelligence Organisation, Director-General's *Annual Threat Assessment 2024* (February 2024).

[16] PQShield, *The Hidden Threat: Harvest-Now-Forge-Later and the Collapse of Digital Trust* (podcast, December 2025). Vendor-produced source; cited for the argument only.

[17] CVE-2024-3094, XZ Utils backdoor (disclosed March 2024).

[18] CISA, NSA, FBI and international partners, joint cybersecurity advisory on Volt Typhoon (7 February 2024).

[19] Department of Home Affairs, *Independent Review of the Security of Critical Infrastructure Act 2018* (Dr Jill Slay AM, delivered to the Minister for Home Affairs 31 January 2026; tabled in Parliament 24 March 2026). Recommendation 4. Delivery date from Home Affairs, *Consultation on proposed amendments to streamline and modernise the SOCI Act 2018*, homeaffairs.gov.au.

[20] *Corporations Act 2001* (Cth), sections 180, 181, 189 and 912A.

[21] *ASIC v RI Advice Group Pty Ltd* [2022] FCA 496. Declaratory relief and $750,000 costs; no civil penalty.

[22] *ASIC v FIIG Securities Limited* [2026] FCA 92. $2.5 million civil penalty. Also source of ASIC Chair Joe Longo's public statement on director cases.

[23] Australian Signals Directorate, Australian Cyber Security Centre, *Quantum technology primer: Computing* (19 February 2026), cyber.gov.au.

[24] Australian Prudential Regulation Authority, *Corporate Plan 2026–27* (20 August 2026), apra.gov.au. Prepared under the PGPA Act.

[25] J. Lonsdale, APRA Chair, speech to the 2026 ABA Banking Conference (17 June 2026). The speech addresses geopolitical risk; its findings are applied to quantum risk by analogy.

[26] *Privacy Act 1988* (Cth), Australian Privacy Principle 11 and civil penalty provisions.

[27] *Australian Information Commissioner v Australian Clinical Labs Ltd (No 2)* [2025] FCA 1224.

[28] *Australian Information Commissioner v Medibank Private Limited*, Federal Court of Australia (proceedings commenced June 2024); related consumer and shareholder class actions.

[29] *Privacy and Other Legislation Amendment Act 2024* (Cth). Statutory tort for serious invasions of privacy from 10 June 2025.

[30] *Cyber Security Act 2024* (Cth). Ransomware payment reporting from 30 May 2025.

[31] ASX Corporate Governance Council, *Corporate Governance Principles and Recommendations*, 4th edition (February 2019), Recommendations 2.2 and 7.2.

[32] Australian Prudential Regulation Authority, *Prudential Standard CPS 234 Information Security* (in force 1 July 2019), and Prudential Practice Guide CPG 234.

[33] Australian Prudential Regulation Authority, *Prudential Standard CPS 230 Operational Risk Management* (in force 1 July 2025). Replaced CPS 231 Outsourcing.

[34] Australian Prudential Regulation Authority, *Prudential Standard CPS 220* and *Prudential Practice Guide CPG 220 Risk Management* (April 2018).

[35] *Security of Critical Infrastructure Act 2018* (Cth).

[36] Department of Home Affairs, *Protective Security Policy Framework*, Release 2026, section 13.10.2 and Requirements 0040 to 0048, 0212 and 0223 (effective 1 July 2026), protectivesecurity.gov.au.

[37] Australian Signals Directorate, *Information Security Manual*, Guidelines for software development (September 2026). ISM-2082 and ISM-2083 (cryptographic bill of materials), added December 2025.

[38] Directive (EU) 2022/2555 (NIS2 Directive), Article 20.

[39] UK *Network and Information Systems Regulations 2018*; UK Cyber Security and Resilience Bill (introduced 2025).

[40] Australian Prudential Regulation Authority, findings from the tripartite cyber assessment programme (July 2023).

[41] Australian Prudential Regulation Authority, media release on a $250 million capital adjustment for Medibank Private (27 June 2023, effective 1 July 2023).

[42] FS-ISAC Post-Quantum Cryptography Working Group, *Current State (Crypto Agility)* (2023, TLP White). Industry paper; source of the three-tier model and supplier field.

[43] Cyber and Infrastructure Security Centre, *Higher education and research: Security of Critical Infrastructure Act 2018*, cisc.gov.au. Obligations that apply to critical education assets.

[44] Australian Signals Directorate, *Frontier AI models and their impact on cyber security* (first published 9 April 2026, updated May and July 2026), cyber.gov.au.

[45] Venafi and Security Boulevard, *Post-Quantum Cryptography: Lessons Learned from SHA-1 Deprecation* (2022). Vendor-produced source; used for background on the SHA-1 transition only, not for statistics.

[46] US National Security Agency, *Commercial National Security Algorithm Suite 2.0* (September 2022, with later updates).

[47] Entrust, *2024 PKI and Post-Quantum Trends Study*, conducted by the Ponemon Institute. Vendor-commissioned survey.

[48] Australian Signals Directorate, *Annual Cyber Threat Report 2025–26*, cyber.gov.au.

[49] FS-ISAC with the Quantum Safe Financial Forum and the CFDIR Quantum-Readiness Working Group, *The Timeline for Post Quantum Cryptographic Migration* (25 September 2025).

[50] CA/Browser Forum, Ballot SC-081v3, *Introduce Schedule of Reducing Validity and Data Reuse Periods* (approved 11 April 2025), cabforum.org.

[51] ASD's ACSC, CISA and NSA, *Post-quantum questions to ask your vendors* (2026).

[52] ASD's ACSC, CCCS, CISA, NCSC-UK and NCSC-NZ, *Choosing secure and verifiable technologies* (2024).

[53] PKI Consortium, *Post-Quantum Cryptography Maturity Model*, version 1.0.1, including its procurement guidance with tender and contract clauses (pkic.org), and PQCMM source repository on GitHub. The author is a member of the working group that develops it.

[54] Bank for International Settlements, *BIS Papers No 158: Quantum-readiness for the financial system: a roadmap* (7 July 2025).

[55] Department of Home Affairs, *Streamlining and modernising the Security of Critical Infrastructure Act 2018*, consultation paper (3 July 2026; submissions closed 31 July 2026). Proposals only; not enacted.

[56] US Department of Commerce, export control directive suspending foreign-national access to two frontier AI models (12 June 2026; lifted 30 June 2026).

[57] Microsoft, *Digital sovereignty* (Microsoft Learn); IBM, *What is data sovereignty?*; SAP, *What is digital sovereignty?* Vendor sources; cited for their shared three-part definition only.

[58] Department of Home Affairs (formerly Digital Transformation Agency), *Hosting Certification Framework* (March 2021).

[59] *Privacy Act 1988* (Cth), Australian Privacy Principle 8 and section 16C.

[60] *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth).

[61] *Clarifying Lawful Overseas Use of Data Act 2018* (US) (CLOUD Act).

[62] The White House, National Security Presidential Memorandum, *Expanding Capabilities to Combat Transnational Cyber-Enabled Crime* (12 August 2026).

[63] National Intelligence Law of the People's Republic of China (2017, amended 2018), Articles 7 and 14; Cybersecurity Law of the People's Republic of China (2017), Article 28.

[64] Department of Home Affairs, *Protective Security Policy Framework Direction 001-2025* (4 February 2025). Removal of DeepSeek products from Commonwealth systems.

[65] Government of India, *Information Technology Act 2000*, section 69 (as amended 2008).

[66] Australian Signals Directorate, *Australian Information Security Evaluation Program* (AISEP).

[67] European Cybersecurity Certification Group, *Agreed Cryptographic Mechanisms*, version 2 (May 2025); version 3 draft for public review (June 2026).

[68] China State Cryptography Administration, Institute of Commercial Cryptography Standards, call for post-quantum algorithm proposals (February 2025). Motive as reported in industry sources.

[69] Russian post-quantum standardisation work for eventual GOST standards. Reported in industry sources.

[70] National Intelligence Service and National Security Research Institute (South Korea), Korean Post-Quantum Cryptography competition, final selection (January 2025).

[71] Standards Australia, *Cyber Security Standards Position Paper*, developed with committee IT-012 (January 2025).

[72] NIST National Cybersecurity Center of Excellence, *Migration to Post-Quantum Cryptography*, NIST SP 1800-38.

[73] Australian Government, *Growing and Professionalising the Cyber Security Industry Program* (2024–26), business.gov.au.

[74] The White House, Executive Order 14412, *Securing the Nation Against Advanced Cryptographic Attacks* (22 June 2026), Federal Register Vol. 91, No. 121 (25 June 2026), sections 4 and 6.

[75] M. Ivezic, Applied Quantum, *The Applied Quantum PQC Migration Framework*, version 2.1 (June 2026), pqcframework.com (CC BY 4.0). Practitioner source, not a regulator or standards body.

[76] US National Institute of Standards and Technology, *NIST IR 8547 (Initial Public Draft): Transition to Post-Quantum Cryptography Standards* (November 2024). A draft proposal, not settled policy.

About Southern Quantum and the author

Southern Quantum

Southern Quantum helps Australian organisations plan and deliver their transition to post-quantum cryptography. Its focus is cryptographic agility: knowing where cryptography is used, assessing the risk it carries, and being able to change it as standards and threats change.

Stephen Chey, Founder

stephen@southernquantum.au

Stephen Chey is a founder of Southern Quantum and leads its client engagements. He has more than 30 years' experience in technology across Asia Pacific, the Middle East and Africa, including senior roles at IBM and PwC. Since 2023 he has worked with leaders in government, financial services, telecommunications and critical infrastructure on Australia's response to quantum security threats. His current focus includes higher education and superannuation.

Stephen is a Visiting Fellow in the Cyber & Digital Centre at UTS and a NSW Cyber Security Ambassador. He is a member of the PKI Consortium PQC Working Group and has been trialling the PQC Maturity Model with Australian clients. He is the author of the series *Quantum Risk and the Duty of Company Directors*.

> DISCLOSURE
>
> Stephen Chey is a member of the PKI Consortium PQC Working Group, which develops PQCMM.

> DISCLAIMER
>
> This guide is provided for general informational purposes only and reflects publicly available legal, regulatory and technical information current as at 7 November 2026. It does not constitute legal, financial or professional advice and should not be relied upon as a substitute for advice from a qualified professional regarding your organisation's specific circumstances. While reasonable care has been taken to verify the sources cited, laws, regulatory guidance and case law referenced may change or be superseded after publication. Directors and officers should seek independent legal advice before acting, or declining to act, in reliance on any information in this guide.
>
> © 2026 Stephen Chey. All rights reserved.

SOUTHERN QUANTUM

CRYPTOGRAPHIC AGILITY

Talk to us about your quantum risk governance

southernquantum.au

Gold Coast | Sydney

Stephen Chey · stephen@southernquantum.au

SOUTHERN QUANTUM PTY LTD

ABN 78 701 793 026