SOUTHERN QUANTUM

CRYPTOGRAPHIC AGILITY

SOUTHERNQUANTUM.AU

WHITE PAPER

Quantum-safe supply chains

The gaps in Australia's vendor guidance, and how the PKI Consortium's PQC Maturity Model helps address them

Stephen Chey
Founder, Southern Quantum
stephen@southernquantum.au

Narayana Madineni
Founder, Southern Quantum
narayana@southernquantum.au

November 2026

Contents

Executive summary 3
01 Introduction 3
02 Australia's guidance 4
03 Strengths of the guidance 4
04 Six limitations of the guidance 5
05 How PQCMM helps 6
06 Limits of PQCMM 7
07 Recommendations for buyers 7
08 Conclusion 8
References 8
About the authors and Southern Quantum 9

ABOUT THIS PAPER

This paper reviews Australian Government guidance on quantum risk in the technology supply chain, identifies its limitations, and recommends how buyers can address them. It is written for security, procurement, vendor management and risk teams, and for executives, in any Australian organisation that buys technology.

It reflects the PSPF Release 2026, the Information Security Manual (September 2026) and PQCMM version 1.0.1, as at 8 November 2026.

Executive summary

Most of the encryption that protects Australian organisations is built into products and services bought from vendors. When quantum computers can break the public-key encryption in use today, all of those products will need to change. An organisation's transition can only move as fast as its vendors.

Australian Government guidance sets a clear target. ASD's *Post-quantum questions to ask your vendors*[1] ("the vendor questions") sets out what buyers should ask. The Information Security Manual (ISM)[3] withdraws approval of RSA, Diffie-Hellman and elliptic curve algorithms after 2030. It requires new purchases to support the strongest versions of the new post-quantum standards by then. Since 1 July 2026, the Protective Security Policy Framework (PSPF)[4] has required federal agencies to buy accordingly.

The guidance does not give buyers a way to check vendors' answers. This paper identifies six limitations:

1. **No standard of proof.** The guidance gives buyers no way to test vendor claims.
2. **Required algorithms not named.** The vendor questions refer buyers to the ISM, where current approvals differ from the 2030 requirement.
3. **No way to compare or track vendors.** Written answers give no common scale.
4. **Roadmaps are not commitments.** There is no contract wording to turn vendor dates into obligations.
5. **Mixed messages on 2030.** The PSPF, the ISM and the vendor questions describe the 2030 deadline differently.
6. **No question of control.** No question asks who owns the vendor, which governments can compel it, or who holds the encryption keys.

KEY FINDING

The PKI Consortium's PQC Maturity Model (PQCMM)[5] is an open, industry-developed model. It fully addresses three of these limitations and partly addresses one more. It turns vendor claims into evidence and gives buyers a common scale. It does not replace the ISM, and it does not address who controls the cryptography.

Use ASD's vendor questions to structure the discussion, PQCMM to test the answers, and the ISM to set the required algorithms. Buyers must also ask who controls the cryptography they buy.

Section 07 sets out six steps for buyers.

01 Introduction

Post-quantum cryptography (PQC) is encryption designed to resist attack by quantum computers. Moving to it is a supply chain problem, because most organisations do not choose the encryption in the cloud services, software, network equipment and building systems they buy.

This paper sets out what Australian Government guidance asks of buyers, where it falls short, and how the PKI Consortium's PQC Maturity Model (PQCMM) can address some of those gaps.

02 Australia's guidance

Four documents shape how Australian organisations should manage quantum risk in their supply chains.

Document	What it does	Who it applies to
ASD's *Post-quantum questions to ask your vendors* (2026, with the US agencies CISA and NSA)[1]	Lists questions to ask vendors at each stage of a PQC transition, and describes a good answer to each	Any organisation that buys technology
ASD's *Choosing secure and verifiable technologies* (2024, with agencies in Canada, the US, the UK and New Zealand)[2]	General procurement guidance covering vendor transparency, supply chain, data location, vendor access, geopolitical risk and end of life. It does not mention PQC.	Any organisation; reflected in the PSPF requirement that federal agencies use "secure and verifiable" vendors (Requirement 0048)
Information Security Manual (ISM), Guidelines for cryptography[3]	Lists approved algorithms, and requires new purchases to support specific PQC algorithms by 2030	Mandatory for federal agencies through the PSPF; widely used as a benchmark by state agencies, universities, superannuation funds and critical infrastructure operators
Protective Security Policy Framework (PSPF), Release 2026[4]	From 1 July 2026, requires newly bought cryptographic products to support approved PQC algorithms (Requirement 0212) and requires a PQC transition plan (Requirement 0223)	Mandatory for non-corporate Commonwealth entities (most federal agencies); better practice for other Commonwealth bodies; applied to suppliers through contracts

Table 1. Australian guidance on quantum risk in the supply chain

The documents agree on the main point. 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 PQC.

03 Strengths of the guidance

ASD's vendor questions are a practical starting point for any organisation.

- **They follow ASD's transition phases.** The questions follow ASD's five phases: locate, assess, triage, implement, and communicate and educate. Answers feed directly into the buyer's own transition plan.
- **They start with an inventory.** Vendors are asked for a cryptographic bill of materials (CBOM): a list of every algorithm, library and key a product uses, including in third-party components.
- **They identify products that are hard to change.** Encryption built into firmware, start-up processes or hardware may mean equipment has to be replaced. The questions identify this early.

- **They prioritise long-lived data.** Data stolen today could be decrypted once quantum computers are available (known as "harvest now, decrypt later"). The questions ask how long data stays in a vendor's products.
- **They cover governance and cost.** Vendors are asked who is accountable, how they prioritise customers, whether staff are trained, and whether PQC is included in standard licensing or sold as an extra.
- **They value openness.** ASD notes that a vendor willing to discuss its constraints is showing maturity.

04 Six limitations of the guidance

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

1. No standard of proof

Each question describes a good answer, but not the evidence that would prove it. A vendor can say its product "supports post-quantum cryptography", and the guidance gives the buyer no way to test the claim.

2. Required algorithms not named

The vendor questions ask for algorithms "approved by the appropriate authoring agency". The ISM sets out what that means. The two new US standards, ML-KEM for exchanging keys and ML-DSA for digital signatures, each come in several strengths, called parameter sets. The ISM currently approves two of each: ML-KEM-768 and ML-KEM-1024 (ISM-1995), and ML-DSA-65 and ML-DSA-87 (ISM-1991).[3]

The lower strengths lose approval after 2030. ISM-1917 requires new cryptographic equipment, applications and libraries to support ML-KEM-1024, ML-DSA-87, SHA-384, SHA-512 and AES-256 by then. A vendor that says "we support ML-KEM" may meet the current rules and still miss the 2030 requirement.

3. No way to compare or track vendors

The questions produce written answers, not a rating. Buyers cannot compare vendors on the same scale or measure a vendor's progress during a contract. Each buyer runs its own review, and vendors answer the same questions many times.

4. Roadmaps are not commitments

Many questions ask about future plans. A roadmap shows intent, not delivery. The guidance offers no contract wording to turn a vendor's dates into obligations. Federal agencies must already include security terms in contracts under the PSPF (Requirements 0040 to 0047). Most other buyers have no equivalent government requirement.

5. Mixed messages on 2030

The PSPF says ASD *recommends* ending the use of RSA and elliptic curve cryptography by the end of 2030. The vendor questions describe 2030 as a "planning milestone". The ISM states that these algorithms "will not be approved beyond 2030". Buyers and vendors may therefore treat the same date as a target, a guide or a deadline.

6. No question of control

The vendor questions ask whether a vendor's cryptography is strong and ready. They do not ask who owns the infrastructure it runs on, which governments can legally compel the vendor to hand over data or keys, or which country designed and tested the algorithms.

ASD's procurement guidance, *Choosing secure and verifiable technologies*,[2] covers some of this. It asks where data and backups are stored and accessed from, what remote access the vendor needs, whether the vendor operates in high-risk regions, and whether it depends on a single supplier. It does not ask about foreign laws that can compel a vendor, such as the US CLOUD Act, or who holds the encryption keys.

The two documents are not linked. The vendor questions list the procurement guidance only as further reading, so buyers must combine them.

05 How PQCMM helps

The PKI Consortium is an international non-profit industry body. Its members include technology vendors, certificate authorities, banks, government bodies and universities. Its PQC Maturity Model[5] (version 1.0.1) rates a product from Level 0 (no PQC) to Level 5 (PQC on by default and independently certified). Each level sets criteria, questions and the evidence required.

A product can be self-assessed, independently assessed or certified by the Consortium. The model is developed in public on GitHub, where anyone can comment.[6] Its criteria are free to use, so any buyer can apply them. Only independent assessment and certification cost money.

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 documents. PQCMM asks for test certificates, results of tests against other products, and hands-on testing. Claims a vendor cannot support are recorded as "vendor-stated, not independently verified". A product fails if it uses draft algorithm names such as "Kyber", or silently switches back to older algorithms.	Addressed
Required algorithms not named	Vendors must state the exact strength supported (for example "ML-KEM-768", not "PQC"), so buyers can see what they are getting. PQCMM does not check this against the ISM.	Partly
No way to compare or track vendors	Six levels, each building on the last, give a common scale for comparing vendors, setting a minimum in a tender and tracking progress during a contract. One independent report can serve many buyers.	Addressed
Roadmaps are not commitments	Vendors must give target dates for reaching the next level and fixing weaknesses. 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
No question of control	PQCMM assesses the product, not who owns or controls the vendor. Its CBOM lists algorithms, not where suppliers are based.	Not addressed

Table 2. How far PQCMM addresses each limitation

PQCMM works alongside ASD's guidance rather than replacing it. The vendor questions set out what to discuss, and PQCMM sets the evidence for each answer. The vendor questions also cover topics PQCMM does not, including governance, staff training and licensing.

06 Limits of PQCMM

Buyers should be aware of four limits.

- **A high level does not mean ISM compliance.** PQCMM does not specify algorithms. A product could reach a high level using ML-KEM-768, which the ISM approves only until 2030, or reach Level 2 using ML-KEM-512, which the ISM does not approve. Buyers must check algorithm strengths against the ISM themselves.
- **It treats hybrid modes differently.** A hybrid mode combines a PQC algorithm with an older one. The ISM says hybrids are "not recommended" but not prohibited (ISM-1996), and the vendor questions ask for a plan to move to PQC only. PQCMM counts hybrid support as a sign of maturity, although its higher levels require that older algorithms can be turned off.
- **It has no official standing in Australia.** Neither the ISM nor the PSPF refers to PQCMM, and vendors do not have to use it. Its testing requirements rely on US schemes such as FIPS 140-3, which the ISM prefers but does not require (ISM-1990).
- **It is new.** Version 1.0.1 is recent, few products have been assessed, and the certification scheme is still being established.

07 Recommendations for buyers

Buyers should combine the 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.
3. **Ask for evidence in PQCMM form.** Request exact algorithm strengths, a CBOM, release notes and test certificates. Set a minimum PQCMM level for the purchase. 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.
5. **Put roadmaps in the contract.** Include PQC release dates, the move from hybrid modes to PQC only, and the 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.

08 Conclusion

Australian Government guidance sets a clear target, and ASD's vendor questions are a practical starting point. The weakness is the gap between a vendor's answer and evidence that the answer is true.

PQCMM is the most rigorous tool available to fill that gap, but it does not replace the ISM. Buyers still need to specify the algorithms they require, write vendor commitments into contracts, and ask who controls the cryptography they buy.

Use ASD's vendor questions to structure the discussion, PQCMM to test the answers, and the ISM to set the required algorithms.

References

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

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

[3] 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.

[4] Department of Home Affairs, Protective Security Policy Framework, Release 2026, section 13.10.2 and Requirements 0040 to 0048, 0212 and 0223.

[5] PKI Consortium, Post-Quantum Cryptography Maturity Model, version 1.0.1, maturity levels and procurement guidance.

[6] PKI Consortium, PQCMM source repository, GitHub.

DISCLAIMER

This paper provides general information only. It is not legal, regulatory or procurement advice, and should not be relied on as such. Organisations should seek advice specific to their circumstances. Information is current as at 8 November 2026; guidance, standards and models referred to may change.

© 2026 Southern Quantum Pty Ltd. All rights reserved.

About the authors and Southern Quantum

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.

Narayana Madineni, Founder

narayana@southernquantum.au

Narayana Madineni is a founder of Southern Quantum and its technical lead. He is a cyber security architect with more than 20 years' experience in identity management, data protection, encryption and key management.

At IBM, where he was a technical leader in the global cryptography team and a Master Inventor, he helped add post-quantum algorithms to TLS in the cryptographic libraries behind products including IBM DB2, MQ and WebSphere. He holds 33 US patents, including one for hybrid classical and post-quantum key derivation that received an IBM High Value Patent Award. He is a member of the PKI Consortium PQC Working Group.

DISCLOSURE

Stephen Chey and Narayana Madineni are members of the PKI Consortium PQC Working Group, which develops PQCMM.

SOUTHERN QUANTUM PTY LTD

ABN 78 701 793 026 · southernquantum.au