

Quantum Risk and Post-Quantum Cryptography Standard

How to find, assess, prioritise and replace quantum-vulnerable public-key cryptography, in line with ASD's recommendation to cease traditional asymmetric cryptography by the end of 2030 and APRA's expectations. Ready to adapt for your organisation.

Version 1.0 · October 2026 · Free template from Risk Frameworks Australia (riskfa.com) · No membership or sign-up

How to use this industry standard. Adopt the structure, terms and ratings as written, so that your organisation speaks the same language as the rest of the industry. Fill in the text in **[square brackets]** with your organisation's details, set the dates, thresholds and targets to match your size, systems and risk appetite, delete requirements that do not apply to you, and approve the Standard through your governance process. Regulatory requirements and government guidance are summarised as at October 2026. Cryptographic guidance changes often (the ASD *Information Security Manual* is updated quarterly): confirm the current position before relying on it. This template is general information only, provided free of charge, and is used at your own risk (see the disclaimer at the end).

Document control

Item	Detail
Document	Quantum Risk and Post-Quantum Cryptography Standard
Organisation	[Organisation name]
Document owner	[Chief Information Security Officer]
Approved by	[Board Risk Committee]
Version / date approved	[1.0] / [date]
Review cycle	At least [annually], and after any change to the ASD <i>Information Security Manual</i> cryptography guidelines, a new NIST post-quantum standard, a material change in regulator expectations or a material change in the quantum threat environment
Parent policy	[Information Security Policy / Risk Management Framework]

1. Purpose

This Standard sets the minimum requirements for managing the risk that a **cryptographically relevant quantum computer (CRQC)** will break the public-key cryptography that [Organisation] relies on, and for the orderly transition to **post-quantum cryptography (PQC)**. It ensures that:

- [Organisation] knows where it uses quantum-vulnerable cryptography, including in systems run by material service providers and other third parties;
- data that must stay confidential for many years is protected now against 'harvest now, decrypt later' attacks;
- critical systems, long-lived trust anchors (such as certificate authorities and code signing keys) and external interfaces are transitioned first;
- new systems and contracts support approved post-quantum algorithms and can change cryptography without being rebuilt;
- the transition is planned, funded, tracked and reported against the ASD milestones, and is completed by [the end of 2030]; and
- the Board and management have accurate information on progress and residual risk.

The Standard supports [Organisation] 's obligations under APRA Prudential Standard CPS

234 *Information Security* (where it applies), in particular maintaining an information security capability that keeps pace with changes in threats (paras 15 and 17), classifying information assets by criticality and sensitivity (para 20), implementing controls commensurate with threats and the stage of an asset's life-cycle (para 21), and testing control effectiveness (para 27). It applies the guidance in the Australian Signals Directorate (ASD) *Information Security Manual* (ISM) and ASD's *Planning for post-quantum cryptography*.

2. Scope

This Standard applies to:

- all employees, contractors, directors and officers of [Organisation] and its subsidiaries;
- all systems, applications, infrastructure, cloud services, operational technology, devices, networks and data that use public-key cryptography, whether built, bought or run by a service provider;
- all uses of cryptography: encryption of data in transit and at rest, key exchange, authentication, digital signatures, code and firmware signing, certificates and public key infrastructure (PKI), hardware security modules (HSMs), payment cryptography and secure messaging; and
- material service providers and other third parties that hold, process or protect [Organisation]'s information assets, or provide cryptographic services to it.

Symmetric cryptography (such as AES) and hash functions are in scope where the ISM sets transition requirements for them (section 13), but the main focus is **asymmetric (public-key)** cryptography, which a CRQC would break.

Cyber security incident response, key management procedures, third-party risk management and technology change management have their own documents. They must stay consistent with this Standard. Incidents and issues found under this Standard are managed under the RiskFA Incident & Issues Management Standard.

3. Authoritative position as at October 2026

The table summarises the guidance this Standard is built on. It is not a complete statement of the law. Confirm the current position before relying on it.

Source	What it says
--------	--------------

Source	What it says
ASD, <i>Planning for post-quantum cryptography</i> (updated September 2025)	'In the ISM, ASD recommends ceasing the use of traditional asymmetric cryptography by the end of 2030.' This includes RSA, Diffie-Hellman (DH), Elliptic Curve Diffie-Hellman (ECDH) and the Elliptic Curve Digital Signature Algorithm (ECDSA). Milestones: by end of 2026 a refined transition plan; by end of 2028 transition commenced, starting with critical systems and data; by end of 2030 transition completed; after 2030, continual monitoring and validation. ASD notes the 2030 date includes contingencies for external factors and that organisations should add contingencies for their own internal delays.
ASD, ISM (September 2026), <i>Guidelines for cryptography</i>	A CRQC does not currently exist, but DH, ECDH, ECDSA and RSA 'will not be approved beyond 2030'. A post-quantum cryptography transition plan is developed, implemented and maintained (ISM-2073). New cryptographic equipment, applications and libraries support ML-DSA-87, ML-KEM-1024, SHA-384, SHA-512 and AES-256 by no later than 2030 (ISM-1917). Approved post-quantum algorithms are ML-KEM (FIPS 203) and ML-DSA (FIPS 204) only (see Appendix B).
ASD, ISM (September 2026), <i>cyber security principles</i>	PRO-17 Cryptographic agility: systems are designed, configured and managed to support timely, prioritised and orderly changes to cryptography, including post-quantum cryptography.
ASD, <i>Post-quantum questions to ask your vendors</i> (July 2026)	Vendor-neutral readiness questions, aligned to ASD's transition phases, for use in procurement, contract renewal and ongoing vendor assurance (see Appendix C).
NIST FIPS 203, 204 and 205 (approved 13 August 2024)	FIPS 203 ML-KEM (key encapsulation), FIPS 204 ML-DSA (digital signatures) and FIPS 205 SLH-DSA (stateless hash-based digital signatures).
NIST, <i>HQC selection</i> (11 March 2025, NIST IR 8545)	HQC selected for standardisation as a second key encapsulation mechanism, as a backup to ML-KEM. It becomes an approved scheme only once its standard is published.

Source	What it says
NIST IR 8547 <i>Transition to Post-Quantum Cryptography Standards</i> (final, 27 October 2026)	Quantum-vulnerable public-key algorithms (RSA, ECDSA, EdDSA, finite field and elliptic curve DH and MQV) are deprecated after 2030 and disallowed after 2035 under NIST standards. Systems protecting data with long-term confidentiality needs warrant the earliest transitions. United States federal high value assets and high impact systems must adopt PQC for key establishment by 31 December 2030 and for digital signatures by 31 December 2031 (EO 14412 and OMB M-26-15).
APRA Corporate Plan 2026-27 (August 2026)	APRA 'will also be increasing its focus on quantum computing risks', notes the ASD recommendation to have a transition plan by the end of 2026 and begin implementing it by the end of 2028, and expects entities 'to make timely progress in implementing these plans, prioritising their most critical information assets and operations'.
APRA Member Therese McCarthy Hockey, AFIA Risk Summit (24 June 2026)	APRA wants regulated entities 'at least starting to map where cryptography is relied upon across their systems, data, and third-party providers, including long-lived data and critical infrastructure', intends to step up supervisory engagement, and will want evidence that boards understand the risk and are advancing plans to meet ASD's recommended timeline.
APRA CPS 234 <i>Information Security</i>	Board ultimately responsible for information security (para 13); capability maintained against changes in threats (paras 15, 17); third-party capability assessed (para 16); information assets classified by criticality and sensitivity (para 20); controls commensurate with threats, criticality, life-cycle stage and consequences (para 21); systematic testing of control effectiveness (para 27); control deficiencies that cannot be remediated in a timely manner escalated to the Board or senior management (para 29); material control weaknesses that cannot be remediated in a timely manner notified to APRA within 10 business days (para 36).
AusPayNet AES Migration Program	Industry program migrating the Australian card payments system from Triple DES (TDES) to AES, planned for completion in 2030/31. This is a symmetric cryptography change; asymmetric cryptography used in payment systems still needs its own PQC transition.

The ISM is not legislation. It applies by policy to Australian Government entities and is the authoritative Australian technical guidance for other organisations. APRA has said it expects regulated entities to progress PQC plans in line with ASD's timeline. Where this Standard says 'must' for an ASD recommendation, that is [Organisation] 's own requirement.

4. Key concepts and definitions

Term	Meaning
Asymmetric (public-key) cryptography	Cryptography that uses a key pair (public and private). Used for key exchange, digital signatures, certificates and authentication. Examples: RSA, DH, ECDH, ECDSA. ASD calls these traditional asymmetric cryptography .
Symmetric cryptography and hashing	Cryptography that uses one shared secret key (for example AES), and hash functions (for example SHA-2). The ISM states the impact of quantum attacks on these is 'unlikely to be felt for some time', but still sets larger sizes for use beyond 2030.
Cryptographically relevant quantum computer (CRQC)	A quantum computer capable of breaking widely used public-key cryptography (for example by running Shor's algorithm). The ISM states a CRQC does not currently exist. When one will exist is uncertain.
Harvest now, decrypt later (HNDL)	An attacker copies encrypted data now and stores it, planning to decrypt it once a CRQC exists. Data that must stay confidential for years is already exposed to this threat.
Post-quantum cryptography (PQC)	Cryptographic algorithms designed to resist attack by both classical and quantum computers, such as ML-KEM and ML-DSA. They run on today's computers; no quantum hardware is needed.
ML-KEM	Module-Lattice-Based Key Encapsulation Mechanism (NIST FIPS 203). Used to agree encryption session keys. Replaces RSA key transport, DH and ECDH.
ML-DSA	Module-Lattice-Based Digital Signature Algorithm (NIST FIPS 204). Used for digital signatures. Replaces RSA signatures and ECDSA.
ASD-Approved Cryptographic Algorithm (AACA)	An algorithm approved in the ISM <i>Guidelines for cryptography</i> , used with the key sizes and parameters set out there.
Post-quantum/traditional (PQ/T) hybrid scheme	A scheme that combines at least one post-quantum algorithm (for example ML-KEM) with at least one traditional algorithm (for example ECDH). ASD does not recommend, but does not prohibit, hybrid schemes. Once a CRQC exists, the traditional part gives no protection.

Term	Meaning
Cryptographic agility	The ability of a system to change its cryptographic algorithms, parameters, keys or certificates in a timely, prioritised and orderly way without major redesign (ISM principle PRO-17).
Cryptographic inventory	[Organisation] 's register of where and how cryptography is used, who owns it and what it protects (section 9, Appendix A).
Cryptographic bill of materials (CBOM)	A list of the cryptographic dependencies of a product, system or environment: libraries, algorithms, protocols, parameters, versions and configurations, mapped to the security function each performs. ASD describes it as an extension of a software bill of materials.
Confidentiality lifetime (shelf life)	How long information must stay confidential, from when it is created or sent until disclosure would no longer cause harm (section 10).
Crypto owner	The person accountable for the cryptography in a system: usually the system owner, supported by a technical owner (section 7).
Trust anchor	A long-lived key or certificate that other trust depends on, such as a root certificate authority key, a code or firmware signing key, or an HSM master key.
Transition	Replacing quantum-vulnerable cryptography with approved post-quantum cryptography, or removing or isolating the system that uses it.

5. Principles

1. **Plan now; do not wait for a date.** When a CRQC will exist is uncertain. [Organisation] plans to the ASD target, not to forecasts.
2. **Know what you have.** You cannot transition what you cannot find. The inventory is the foundation of this Standard.
3. **Protect long-lived secrets first.** Data that must stay confidential beyond [2030] is treated as exposed to harvest now, decrypt later today.
4. **Prioritise by risk.** Critical systems, sensitive and long-lived data, trust anchors, external interfaces and systems that are hard to change go first.
5. **Use standards, not novelties.** Use only approved, standardised algorithms in reputable, maintained libraries and products. Do not build your own cryptography or rush ahead of verified implementations.
6. **Build for change.** Every new system can change its cryptography without redesign.
7. **Third parties are our risk.** Vendor and service provider cryptography is inventoried, assessed and contracted for, as if it were our own.
8. **Clear ownership.** Every system using cryptography has a named crypto owner and a dated transition plan.
9. **Prove it works.** A system is transitioned only when testing shows the approved algorithms are in use and the old ones are disabled.
10. **Keep watching.** The threat and the guidance change. [Organisation] monitors them and adjusts this Standard and its plan.

6. Three lines of accountability

Line	Who	Responsibilities
First line	Technology, system owners, crypto owners, PKI and key management teams, procurement, business owners of data	Build and maintain the inventory; classify data by confidentiality lifetime; deliver transition plans for their systems; ensure new systems and contracts meet this Standard; test and evidence transitions.
Second line	Information security governance and Risk (Technology and cyber risk)	Own the risk assessment method; review and challenge inventory completeness, priorities and transition dates; oversee exceptions; report on progress, KRIs and residual risk; assess whether delays are control weaknesses that need escalation or notification.
Third line	Internal Audit	Independently assess the design and operating effectiveness of this Standard and of the transition program, including third-party cryptography (CPS 234 para 32).

Many organisations place the CISO function in the first line and an independent technology risk function in the second line. Map the roles above to your own operating model and record it here: **[operating model]** .

7. Roles and responsibilities

Role	Responsibilities
Board	Ultimately responsible for information security (CPS 234 para 13). Sets risk appetite for quantum risk; approves the transition plan, target dates and funding; oversees progress against the ASD milestones; holds management to account.
Board Risk Committee	Approves this Standard; receives reporting (section 20); approves exceptions beyond [the end of 2030] and exceptions for Critical-rated systems.
CEO and executive team	Fund and resource the transition; make sure their business areas meet their dates; own the business risk of systems that cannot transition in time.
Accountable persons (FAR, where applicable)	Take reasonable steps, within their areas of accountability, to make sure the transition is planned and delivered and that risks are escalated.
Chief Information Security Officer (CISO)	Owns this Standard and the cryptographic policy; sets approved algorithms in line with the ISM; owns the inventory method and tooling; leads the transition program [or: jointly with the CTO]; reports progress and residual risk.
Chief Technology Officer	Delivers the transition in technology platforms, infrastructure, applications and PKI; builds cryptographic agility into architecture standards; funds and schedules upgrades and replacements.
Chief Risk Officer (CRO)	Ensures quantum risk is in the risk register and risk appetite; provides independent challenge of ratings, priorities and exceptions; reports residual risk to the Board Risk Committee.
Head of Compliance / General Counsel	Advise on regulatory expectations, contract clauses, record-keeping obligations that create long confidentiality lifetimes, and any APRA notification of control weaknesses (CPS 234 para 36).
Head of Procurement / third-party risk owner	Includes this Standard's requirements in sourcing, due diligence and contracts; tracks vendor PQC readiness (section 15).
Crypto owner (system owner)	Accountable for the cryptography in their system: keeps its inventory entry accurate; sets its transition plan and date; manages exceptions; evidences completion.

Role	Responsibilities
Data owner	Sets the confidentiality lifetime of the data they own (section 10).
PKI and key management owner	Manages certificate authorities, certificates, HSMS and keys; plans the PKI transition (section 17).
Architects and developers	Design systems to be cryptographically agile; use only approved libraries and algorithms; produce CBOMs for software they build.
All staff	Report suspected weak or unapproved cryptography and compromised keys to the [CISO].

8. Risk assessment

8.1 Quantum risk in the risk register

Quantum risk must be recorded in [Organisation]'s risk register as an information security risk, with the CISO as risk owner, linked to the controls in this Standard. It is rated Critical, High, Medium or Low on the highest of the six impact categories in the RiskFA Risk Management Framework (Financial; Customers; Regulatory and legal; Operations and critical operations; Information security and privacy; Reputation), using the realistic worst case if the cryptography were broken.

8.2 Planning tool: shelf life plus transition time

A widely used planning tool, known as **Mosca's inequality**, compares three periods:

Symbol	Period	Who sets it
X	Shelf life: how long the data or signature must stay secure	Data owner (section 10)
Y	Transition time: how long it will take to move the system to post-quantum cryptography, including procurement, testing and the vendor's own roadmap	Crypto owner, with Technology
Z	Time until a CRQC exists	Uncertain. Not estimated by [Organisation]

If **X + Y is greater than Z**, data will still need protection after it can be broken, so the system is already at risk. Because Z is uncertain, [Organisation] does **not** forecast it. Instead it uses the ASD target as the planning horizon:

- **Transition time:** every system must be able to finish its transition by [the end of 2030]. If Y means a system cannot finish by then, start now or plan its replacement or retirement.
- **Confidentiality:** any data sent or stored under traditional asymmetric cryptography that must stay confidential beyond [2030] is treated as exposed to harvest now, decrypt later **now**, and its systems are prioritised.
- **Signatures and authentication:** harvest now, decrypt later does not apply in the same way, but a CRQC could forge signatures and impersonate systems. Keys and certificates that will still be trusted after [2030] (root and intermediate certificate authorities, code and firmware signing, long-term signed records) are prioritised by how long they will be trusted and how hard they are to replace.

Mosca's inequality is a planning aid, not a prediction. Do not use it to justify delaying past the ASD target. ASD notes that its 2030 date already includes contingency for technology breakthroughs, and that organisations should add contingency for their own delays.

8.3 System-level rating

Each inventoried system is given a **quantum risk rating** to set its priority:

Rating	Typical characteristics
Critical	Supports a critical operation, or protects highly sensitive data with a confidentiality lifetime beyond [2030], or is a trust anchor (root CA, code signing, HSM master keys), or is externally facing and carries such data; and is hard to change.
High	Protects sensitive customer, financial or market data with a confidentiality lifetime beyond [2030]; or is an external interface with customers, counterparties, payment networks or regulators; or depends on a vendor with no PQC roadmap.
Medium	Internal system with sensitive data of shorter lifetime, or with other protections (for example segregated networks), that can be transitioned through normal upgrades.
Low	Data of low sensitivity or short lifetime, and the system can be patched easily or will be retired before [2030].

9. Cryptographic inventory

[Organisation] must maintain a single cryptographic inventory in [the configuration management database / GRC system / crypto inventory tool]. It must:

- cover all components of the IT environment: cloud services, applications, hardware, operational technology, network devices, endpoints, HSMs and PKI, and services provided by third parties;
- record, for each use of cryptography, at least the fields in Appendix A;
- map each use to the security function it performs (encryption in transit, encryption at rest, key exchange, authentication, signing) and to the data and critical operations it protects;
- be built from more than one source: discovery tools (network and certificate scanning, code and library scanning), system owner attestations, vendor CBOMs and questionnaires, and key and certificate management systems;
- include cryptography that is hard-coded, embedded in firmware or hardware, or inherited from third-party libraries;
- be updated through change management whenever cryptography is added or changed, and reviewed by crypto owners at least **[every 6 months]**; and
- be complete for all Critical and High systems by **[30 June 2027]**, and for all in-scope systems by **[31 December 2027]**.

Start simple. ASD notes that an initial CBOM may be a list of critical systems and components mapped to the security functions they rely on cryptography for. Mature it over time to libraries, algorithms, protocols, parameters, versions and configurations.

Software that **[Organisation]** builds must produce a CBOM, and CBOMs supplied for third-party components must be used to check that they support standardised implementations of ASD-approved algorithms (ISM-2083, ISM-2082). Where a vendor cannot supply a CBOM, record the gap and use the vendor questionnaire (Appendix C).

10. Data classification by confidentiality lifetime

Data owners must set a **confidentiality lifetime** for each information asset class, as part of CPS 234 para 20 classification. The confidentiality lifetime is how long disclosure would still harm customers, **[Organisation]** or others, which is often longer than the retention period.

Lifetime band	Typical examples (adapt to your organisation)	Treatment
---------------	---	-----------

Lifetime band	Typical examples (adapt to your organisation)	Treatment
Beyond [2035]	Identity documents and identity verification data; tax file numbers; health and claims information; superannuation member records; long-term loan, mortgage and insurance policy records; biometrics; litigation and regulatory investigation records; long-term strategic or M&A information; master keys	Treat as exposed to harvest now, decrypt later now. Highest priority for post-quantum key exchange on any network path, and for re-encryption or key replacement where data at rest is protected by asymmetric key wrapping.
[2030] to [2035]	Customer account and transaction history; credit files; most personal information; trading strategies; contracts; board papers	High priority. Transition by the ASD milestones.
Up to [2030]	Session data, short-lived tokens, operational logs, published or soon-to-be-published information	Normal priority. Transition through planned upgrades by [the end of 2030] .

Legal and regulatory retention obligations (for example under the *Corporations Act 2001*, *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, *Privacy Act 1988* and tax laws) set minimum retention periods. Data owners must consider these, and how long the data stays sensitive after retention ends if it is not destroyed, when setting the lifetime. Compliance confirms the retention periods: [\[link to records retention schedule\]](#).

11. Prioritisation

Systems are prioritised for transition using their quantum risk rating (section 8.3) and the factors ASD lists for triage. Priority goes to systems that:

- support a **critical operation** or are critical to the functioning of **[Organisation]**;
- handle **highly sensitive data or data with a long confidentiality lifetime**;
- are **trust anchors**: root and intermediate certificate authorities, code and firmware signing, HSMs, identity providers and single sign-on;
- **interact with external organisations**: customer channels, internet-facing services, APIs, connections to payment networks, clearing and settlement systems, market infrastructure, regulators and other financial institutions, and VPNs;
- are **payment systems**, including card, real-time and high-value payments, and their HSMs and key management. Note that the industry migration of card payments from TDES to AES (planned by AusPayNet for completion in 2030/31) is a symmetric change;

asymmetric cryptography in payment systems must still be inventoried and transitioned;

- depend on **material service providers** or vendors whose cryptography [Organisation] cannot change itself;
- are **likely to be difficult or slow to update**: bespoke or legacy systems, embedded devices, operational technology, long-life hardware, or systems with long refresh cycles; and
- lack other protections that would reduce exposure (for example network segregation, or symmetric encryption with pre-shared keys).

Systems due to be retired before [the end of 2030] do not need to transition, but their retirement date becomes a tracked commitment. If retirement slips, the system re-enters the transition plan.

12. Transition plan and roadmap

[Organisation] must have a PQC transition plan that is developed, implemented and maintained (ISM-2073), approved by the [Board Risk Committee], and aligned to ASD's milestones. The plan follows ASD's five phases: Locate, Assess, Triage, Implement, and Communicate and educate.

Phase	What must happen	Target date
0. Mobilise	Appoint the program owner and crypto owners; approve this Standard; record quantum risk in the risk register; brief the Board; set budget.	[Immediately, if not already done]
1. Locate	Build the cryptographic inventory (section 9), including third parties.	Critical and High systems [30 June 2027]; all [31 December 2027]
2. Assess	Set confidentiality lifetimes (section 10); rate each system (section 8); identify legal, regulatory and customer impact of compromise.	[31 December 2026] for Critical systems; then in step with phase 1
3. Triage	Prioritise systems (section 11); choose the path for each: upgrade, configure, replace, retire or exception; confirm vendor roadmaps.	Refined plan approved by [31 December 2026] (ASD milestone)

Phase	What must happen	Target date
4. Implement	Transition systems in priority order: test, deploy, disable traditional algorithms, evidence completion. Start with Critical systems and trust anchors.	Started by [31 December 2028] (ASD milestone); Critical systems complete by [31 December 2029] ; all complete by [31 December 2030]
5. Communicate and educate	Engage vendors and counterparties; train technology staff; tell customers where they must act (for example to update apps or devices).	Throughout
6. Sustain	Monitor and validate PQC implementations; manage vulnerabilities; keep the inventory current; adjust for changes in guidance or threat.	Ongoing, after 2030

The plan must include, for each system: owner, quantum risk rating, chosen path, dependencies (including vendors), budget, start and finish dates, and the evidence required for completion. Appendix D is a template. Original target dates are kept; changes are approved under section 21 and reported.

ASD's milestones are the outside dates. Set earlier internal dates to allow for slippage, vendor delays and testing, as ASD recommends. If your organisation is starting late, compress phases 1 to 3 and start Critical systems in parallel.

13. Approved cryptography

- Only ASD-approved cryptographic algorithms (AACAs), with the key sizes and parameters in the ISM, may be used by cryptographic equipment, applications and libraries (ISM-0471). Disable unapproved algorithms wherever possible, as ASD prefers. Appendix B lists the position as at October 2026.
- For **key establishment**, transition to **ML-KEM**, preferably **ML-KEM-1024**. ASD approves ML-KEM-768 but will not approve it beyond 2030 (ISM-1995).
- For **digital signatures**, transition to **ML-DSA**, preferably **ML-DSA-87**, using the hedged variant whenever possible. ASD approves ML-DSA-65 but will not approve it beyond 2030 (ISM-1991, ISM-1992).
- For **symmetric encryption and hashing**, new systems intended for use beyond 2030 must support **AES-256, SHA-384 and SHA-512** (ISM-1917). ASD will not approve AES-128, AES-192, SHA-224 or SHA-256 beyond 2030.
- **SLH-DSA, LMS, XMSS and HQC** are NIST post-quantum standards or selections but are **not** ASD-approved algorithms in the September 2026 ISM. Do not use them without CISO approval and a recorded exception.
- **Hybrid schemes** (PQ/T) are permitted only as a temporary transition measure, where needed for interoperability, with CISO approval, a recorded date for moving to post-quantum only, and with at least one component an AACA (ISM-1996). ASD does not recommend them, and once a CRQC exists they give only the protection of the post-quantum part.
- Use standardised, reputable and maintained libraries and products. FIPS 140-3 validated modules are preferred (ISM-1990). Do not use experimental, pre-standard or proprietary post-quantum implementations in production.
- **Quantum key distribution (QKD)** is not used for secure communications. ASD does not support it because of practical limitations.
- Larger traditional key sizes are not a substitute for transition. ASD notes they may give marginal, short-term risk reduction only.

14. Cryptographic agility for new systems

All new systems, major changes and new technology purchases approved after [the date this Standard is approved] must:

- support ML-KEM-1024, ML-DSA-87, AES-256, SHA-384 and SHA-512, or have a vendor-committed, dated roadmap to support them in time for [Organisation] to complete testing and transition before [the end of 2030];

- allow algorithms, key sizes, certificates and keys to be changed through configuration or supported patches, without code rewrites or hardware replacement;
- not hard-code algorithms, keys or certificates, and centralise cryptographic functions in shared, approved libraries or services;
- support larger keys, signatures, certificates and messages that post-quantum algorithms use (for example in protocols, databases, message formats, smart cards and network devices);
- have firmware and secure boot that can be updated to post-quantum signature schemes;
- produce or come with a CBOM, and be entered in the cryptographic inventory before go-live; and
- pass a cryptography review by [Security Architecture] as part of design approval.

Architecture standards, secure development standards and procurement templates must be updated to include these requirements by [date].

15. Third parties, vendors and material service providers

Third parties often control the cryptography that protects [Organisation]'s information assets, so their readiness decides [Organisation]'s own. Under CPS 234 (paras 16, 22 and 28) and CPS 230 (material service providers), [Organisation] must:

- identify every third party that holds, processes, transmits or protects [Organisation]'s information assets using public-key cryptography, starting with material service providers and providers of critical operations;
- ask them about PQC readiness using Appendix C, scaled to the risk of the service, at due diligence, renewal and at least [annually] for Critical and High services;
- record their answers, roadmap dates and gaps in the inventory and the third-party risk system;
- treat a provider with no credible roadmap to complete before [the end of 2030] as a third-party risk issue, with a remediation plan or exit plan; and
- include the clauses below in new and renewed contracts.

15.1 Contract clauses (minimum)

Clause	Requirement
Approved cryptography	The provider uses cryptography consistent with the ASD ISM <i>Guidelines for cryptography</i> as updated from time to time, and supports [ML-KEM-1024, ML-DSA-87, AES-256, SHA-384 and SHA-512] for services delivered to [Organisation] by [date, no later than 31 December 2030 less testing time] .
Roadmap and transparency	The provider gives [Organisation] a dated, product-specific PQC roadmap, and a CBOM or equivalent description of the cryptography used in the service, and updates both at least [annually] .
Notification of change	The provider notifies [Organisation] at least [90 days] before material changes to cryptography, and promptly of any cryptographic vulnerability or key compromise affecting the service.
Agility	Cryptographic changes are delivered through supported patches or configuration within the standard licence, without extra fees for PQC functionality.
Hybrid and deprecation	Any hybrid scheme is transitional, with a dated plan to move to post-quantum only; traditional algorithms are removed on a published timeline.
Testing and assurance	The provider supports [Organisation] 's testing of PQC configurations, and provides independent assurance of its cryptographic controls on request.
Subcontractors	The provider flows these requirements down to subcontractors that handle [Organisation] 's information assets.
Exit	If the provider cannot meet the agreed dates, [Organisation] may terminate without penalty and the provider supports transition to another provider.

Adapt the wording with your legal team. ASD lists common concerns in vendor responses: limited visibility of cryptographic use, reliance on general assurances, unclear or deferred timelines, proprietary or opaque cryptography, PQC treated as an optional or premium function, over-reliance on compensating controls, and lack of governance or ownership.

16. Testing and interoperability

- Each transition must be tested before production for: correct algorithms and parameters in use; interoperability with all counterparties, clients and devices; performance (latency, throughput, message and certificate sizes); and safe rollback.
- Test in non-production environments first. Use vendor-supported, production-ready releases; do not run preview or experimental cryptography in production.
- After go-live, verify through scanning or configuration review that traditional algorithms are disabled, or limited to an approved hybrid scheme, and record the evidence in the inventory.
- Coordinate testing with external counterparties (payment networks, other financial institutions, regulators, market infrastructure) in good time; record their dates as dependencies.
- Include post-quantum configurations in the systematic testing program for information security controls (CPS 234 para 27), including penetration testing and configuration assurance.
- Test failure modes: what happens when a counterparty does not support post-quantum algorithms. Systems must not silently fall back to unapproved cryptography.

17. Key management and PKI

- Cryptographic key management processes and procedures must cover key generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction (ISM-0507). Update them for post-quantum keys by [date].
- Plan the PKI transition early. Certificate authorities, certificate profiles, HSMs, certificate lifecycle tools, relying applications and devices must all support post-quantum certificates. Allow for larger keys and signatures.
- Root and intermediate certificate authorities, code signing and firmware signing keys whose validity extends beyond [2030] are Critical priority. New long-lived trust anchors must not be created using only traditional algorithms after [date].
- Confirm that HSMs support ML-KEM and ML-DSA, or have a supported firmware path to them, and plan replacement where they do not.
- Shorten certificate and key lifetimes where practical, so that changes can be made faster.
- Where data at rest is protected by symmetric keys that are wrapped or transported with RSA or ECDH, identify it; long-lifetime data may need re-wrapping with approved algorithms.
- Report the compromise or suspected compromise of cryptographic equipment or keying material to the CISO as soon as possible, and change the keying material (ISM-0142, ISM-1091). Manage it as an incident under the RiskFA Incident & Issues Management Standard.

18. Monitoring the threat environment and guidance

CPS 234 para 17 requires [Organisation] to maintain its information security capability as vulnerabilities and threats change. The [CISO] must:

- monitor, at least [quarterly], changes to the ASD ISM (published quarterly), ASD publications, NIST standards and transition guidance, APRA and other regulator statements, and the guidance of payment networks and industry bodies;
- track credible developments in quantum computing and in attacks on post-quantum algorithms and their implementations, using authoritative sources such as ASD, NIST and threat intelligence providers, rather than media forecasts;
- assess each material change for its effect on approved algorithms, priorities and target dates, and update this Standard, Appendix B and the transition plan as needed; and
- report material changes to the [Board Risk Committee] promptly, with a recommendation (for example to bring dates forward).

After transition, monitor post-quantum implementations for vulnerabilities and performance, and keep them current, as ASD recommends for the period after 2030.

19. Key risk indicators

KRIs are reported [quarterly]. Set thresholds in line with risk appetite. Suggested indicators:

KRI	Typical target / threshold
Inventory coverage: % of in-scope systems with a complete inventory entry (Appendix A)	Critical and High [100%] by [30 June 2027]; all [100%] by [31 December 2027]
% of systems with a named crypto owner and a confidentiality lifetime set	[100%]
% of Critical and High systems with an approved, dated transition plan	[100%] by [31 December 2026]
% of Critical systems transitioned (by count and by data volume protected)	Rising to [100%] by [31 December 2029]
% of all in-scope systems transitioned	On track to [100%] by [31 December 2030]
% of external interfaces using approved post-quantum key establishment	Trending up; [100%] by [31 December 2030]
Trust anchors (CA, code and firmware signing) on post-quantum algorithms	[100%] by [date]
% of material service providers with a credible, dated PQC roadmap	[100%] of Critical/High by [30 June 2027]
Systems with no viable transition path (needing replacement or exception)	Number and trend; each with an owner and plan
Transition milestones overdue against original dates	≤ [5%]; no Critical milestone overdue more than [90 days]
New systems or contracts approved without meeting section 14 or 15	[0]

KRI	Typical target / threshold
Open exceptions, and exceptions beyond [the end of 2030]	Number and trend; [0] beyond 2030 without Board Risk Committee approval

These measures and targets are common practice, not regulatory requirements. Set your own in line with your risk appetite.

20. Reporting to the Board

The [CISO], with the [CRO], reports to the executive [monthly] and to the [Board Risk Committee] at least [quarterly]. APRA has said it will want evidence that boards understand the risk and are advancing plans to meet ASD's recommended timeline. Board reports must cover at least:

- status against the ASD milestones (plan by end 2026, commenced by end 2028, complete by end 2030) and [Organisation]'s internal dates;
- the KRIs in section 19, with trends;
- Critical and High systems not on track, and the reasons;
- material service providers and vendors without credible roadmaps, and the actions taken;
- exceptions, risk acceptances and residual risk;
- budget and resourcing against plan;
- material changes in guidance or the threat environment, and what they mean for the plan; and
- any matter that may need notification to APRA, such as a material control weakness that cannot be remediated in a timely manner (CPS 234 para 36).

The Board should receive a briefing on quantum risk and this program at least [annually], so that directors understand the risk and their oversight role.

21. Exceptions and risk acceptance

- Any departure from this Standard (for example a system that cannot meet its transition date, use of an unapproved algorithm, or a hybrid scheme) must be recorded as an exception, with the reason, the risk rating, compensating controls, a remediation or retirement plan and an expiry date of no more than [12 months].
- Approvals: Low and Medium, the [CISO]; High, the [CISO] and [CRO]; Critical, or any exception extending beyond [the end of 2030], the [Board Risk Committee].
- Compensating controls may include network segregation, limiting data held or sent, shorter retention, additional symmetric encryption with securely distributed keys, or moving the data to a transitioned system. They reduce but do not remove the risk.
- A missed transition date is an issue, rated and managed under the RiskFA Incident & Issues Management Standard. Original dates are never overwritten.
- Compliance assesses whether an exception or delay is a material information security control weakness that must be notified to APRA within 10 business days (CPS 234 para 36).
- Exceptions are reviewed at expiry and reported to the [Board Risk Committee] [quarterly].

22. Training and assurance

- Technology, architecture, development, procurement and third-party risk staff complete PQC awareness training by [date] and when guidance changes materially.
- The Board and executive receive the briefing in section 20.
- Second line tests inventory completeness and accuracy, and samples transition evidence, at least [half-yearly].
- Internal Audit reviews the design and operating effectiveness of this Standard and the transition program at least every [2 years] while the transition is under way, including third-party cryptography (CPS 234 paras 32 to 34).

23. Related documents

- the RiskFA Cyber Security Policy, [Cryptography and Key Management Standard] and [Secure Development Standard]
- [Third-Party Risk Management Policy] and [Material Service Provider Standard]
- [Data Classification and Handling Standard] and [Records Retention Schedule]
- [Technology Architecture Standards] and [Change Management Policy]
- The RiskFA Incident & Issues Management Standard and the RiskFA Risk Management Framework
- APRA: CPS 234 *Information Security*, CPS 230 *Operational Risk Management*, CPG 234 *Information Security*
- ASD: *Information Security Manual* (Guidelines for cryptography; Guidelines for software development, 'Cryptographic bill of materials'), *Planning for post-quantum cryptography*, *Post-quantum questions to ask your vendors*, *Managing cryptographic keys and secrets*
- NIST: FIPS 203 *Module-Lattice-Based Key-Encapsulation Mechanism Standard*, FIPS 204 *Module-Lattice-Based Digital Signature Standard*, FIPS 205 *Stateless Hash-Based Digital Signature Standard*, SP 800-227 *Recommendations for Key-Encapsulation Mechanisms*, IR 8547 *Transition to Post-Quantum Cryptography Standards*, SP 800-57 Part 1 *Recommendation for Key Management*
- Standards: ISO/IEC 27001 *Information security management systems* (control on use of cryptography), ISO/IEC 19790:2025 *Security requirements for cryptographic modules*, ISO/IEC 24759:2025 *Test requirements for cryptographic modules*

Appendix A. Cryptographic inventory fields

Field	Description	Required for
Inventory ID, system / service name	Unique reference and name	All
Crypto owner and technical owner	Named accountable owner and technical contact	All
Business service and critical operation supported	Link to the critical operations register (CPS 230)	All
Provider	Built in-house, vendor product, cloud or managed service; vendor and product name	All
Location of cryptography	Application, operating system, middleware, database, network device, HSM, firmware, hardware, third-party service	All
Security function	Encryption in transit, encryption at rest, key exchange, authentication, digital signature, code or firmware signing, certificate issue	All
Protocol and version	For example TLS 1.2 / 1.3, SSH, IPsec / IKEv2, S/MIME, proprietary	All
Algorithms and parameters	For example RSA-2048, ECDH P-256, ECDSA P-384, AES-128-GCM, SHA-256, ML-KEM-1024	All
Library or module and version	For example cryptographic library, HSM model and firmware, FIPS 140-3 validation status	Critical and High; all when available
Keys and certificates	Key types and sizes, certificate issuer, validity end dates, where keys are stored	All
Hard-coded or hardware-bound	Whether cryptography can be changed by configuration, patch, or only by replacement	All
Data protected	Information asset classes, classification and confidentiality lifetime (section 10)	All

Field	Description	Required for
Exposure	Internet-facing, partner-facing, internal; counterparties connected	All
Quantum risk rating	Critical, High, Medium or Low (section 8.3) with rationale	All
Vendor PQC readiness	Roadmap dates, supported algorithms, CBOM provided (yes / no)	Vendor and service provider systems
Transition path and dates	Upgrade, configure, replace, retire or exception; original and current target dates; status	All
Evidence of transition	Test results and post-deployment verification	When transitioned
Linked exceptions, issues and risks	References	If applicable
Date last reviewed	By the crypto owner	All

Appendix B. Algorithm position as at October 2026

Summary of the ASD ISM (September 2026) *Guidelines for cryptography* and NIST IR 8547 (October 2026). Requirements shown are for non-classified, OFFICIAL: Sensitive and PROTECTED data; higher classifications have stricter requirements. Always check the current ISM.

Algorithm	Use	ASD ISM (September 2026)	NIST
RSA	Signatures; transporting session keys	Approved: modulus at least 2048 bits, preferably 3072 (ISM-0476). Not approved beyond 2030.	Deprecated after 2030; disallowed after 2035
Diffie-Hellman (DH)	Agreeing session keys	Approved: modulus at least 2048 bits, preferably 3072 (ISM-0472). ECDH preferred over DH. Not approved beyond 2030.	Deprecated after 2030; disallowed after 2035

Algorithm	Use	ASD ISM (September 2026)	NIST
ECDH	Agreeing session keys	Approved: at least 224 bits, preferably NIST P-384 (ISM-0474). Not approved beyond 2030.	Deprecated after 2030; disallowed after 2035
ECDSA	Signatures	Approved: at least 224 bits, preferably P-384 (ISM-0475). Not approved beyond 2030.	Deprecated after 2030; disallowed after 2035
EdDSA	Signatures	Not listed as an ASD-approved algorithm	Deprecated after 2030; disallowed after 2035
ML-KEM (FIPS 203)	Encapsulating session keys	ML-KEM-768 or ML-KEM-1024, preferably ML-KEM-1024 (ISM-1995). ML-KEM-768 not approved beyond 2030. ML-KEM-512 not approved.	All three parameter sets approved; NIST recommends ML-KEM-768 as default
ML-DSA (FIPS 204)	Signatures	ML-DSA-65 or ML-DSA-87, preferably ML-DSA-87 ; hedged variant whenever possible; pre-hashed variants only if performance requires, with at least SHA-384 / SHA-512 (ISM-1991 to ISM-1994). ML-DSA-65 not approved beyond 2030. ML-DSA-44 not approved.	All three parameter sets approved
SLH-DSA (FIPS 205)	Signatures	Not listed as an ASD-approved algorithm	Approved
LMS / HSS, XMSS (SP 800-208)	Stateful hash-based signatures	Not listed as an ASD-approved algorithm	Approved
HQC	Key encapsulation	Not listed as an ASD-approved algorithm	Selected March 2025; approved once its standard is published
AES	Symmetric encryption	AES-128, AES-192 or AES-256, preferably AES-256 (ISM-1769). AES-128 and AES-192 not approved beyond 2030. No ECB mode (ISM-0479).	Approved

Algorithm	Use	ASD ISM (September 2026)	NIST
SHA-2	Hashing	At least 224-bit output, preferably SHA-384 or SHA-512 (ISM-1766). SHA-224 and SHA-256 not approved beyond 2030. SHA-3 and SHAKE approved only inside ML-DSA and ML-KEM.	Approved
PQ/T hybrid schemes	Key establishment or signatures	Not recommended, not prohibited; at least one component must be an AACA (ISM-1996).	A composite (hybrid) key establishment can be FIPS 140-validated if at least one input comes from an approved scheme

ISM-1917: new cryptographic equipment, applications and libraries must support ML-DSA-87, ML-KEM-1024, SHA-384, SHA-512 and AES-256 by no later than 2030. 'Not approved beyond 2030' is ASD's wording; ASD recommends ceasing traditional asymmetric cryptography by the end of 2030. Protocol-specific requirements (TLS, SSH, IPsec, MACsec and others) are in the ISM 'Cryptographic protocols' and related sections.

Appendix C. Vendor PQC questionnaire

Based on ASD's *Post-quantum questions to ask your vendors* (July 2026). Scale the questions to the risk of the service, the vendor's control over cryptography, the sensitivity and lifetime of the data, and your stage of transition.

Phase	Question	What a good answer looks like
Locate	Do you maintain a current inventory of cryptographic dependencies, such as a CBOM, and will you share it with us?	A complete, maintained CBOM covering algorithms, protocols, libraries, parameters and configurations, including third-party and embedded components
Locate	Where is cryptography implemented, and is any of it hard-coded, fixed or hardware-bound?	Clear identification by layer; no hard-coded cryptography, or a remediation roadmap

Phase	Question	What a good answer looks like
Locate	Do third-party components introduce cryptography? How is cryptography updated?	Full disclosure of dependencies; standardised libraries; updates through supported patches
Locate	Do you rely on hardware roots of trust (TPM, HSM, secure enclave)? Can firmware and boot processes be updated to post-quantum signatures?	Trust anchors identified; updatable without hardware replacement, or a roadmap
Assess	Which of our data flows rely on traditional asymmetric cryptography, and what data lifetime assumptions does your service make?	Clear mapping of flows; data lifetime reflected in your roadmap
Assess	Do you have a documented assessment of CRQC risk for this product or service, separating signing, encryption and authentication?	Documented assessment referencing authoritative guidance, with separate treatment of each
Triage	Which products or services will be PQC-ready early enough for us to test and roll out before the end of 2030?	Product-specific, versioned release dates well before 2030
Triage	Which components need hardware replacement or re-architecture?	Transparent disclosure with reasons and timelines
Triage	Do you support hybrid modes, and when will you move to post-quantum only?	Hybrid as a transitional measure only, with a dated plan to move to post-quantum only
Triage	How do you prioritise customers, and what governance oversees your PQC transition?	Risk-based prioritisation; executive ownership and regular review
Implement	Which post-quantum algorithms and parameter sets will you support, and when?	Standards-based, ASD-approved algorithms (ML-KEM-1024, ML-DSA-87) with dates
Implement	Is your PQC implementation production-ready and supported? How do you validate your cryptographic libraries?	Supported release with service levels; reputable, validated libraries (for example FIPS 140-3)

Phase	Question	What a good answer looks like
Implement	How will key, certificate sizes and lifecycle processes change, and how do we enable PQC?	Documented impacts and enablement steps, with known compatibility issues
Implement	Is PQC included in the base licence?	Yes, with no premium add-on fees
Communicate	How will you notify us of cryptographic changes, and will you provide transition guides?	Formal advisories and release notes; customer-ready guides with testing guidance
Communicate	How and when will traditional cryptography be removed? Does your roadmap align with ASD guidance?	Dated deprecation timeline; roadmap referencing ASD guidance and completion before end of 2030
Communicate	Are your support teams trained in PQC, and do you track or contribute to PQC standards bodies?	Evidence of training, runbooks and standards engagement

Appendix D. Transition roadmap template

Field	Entry
System / service and inventory ID	[name, ID]
Crypto owner / technical owner	[names]
Quantum risk rating and rationale	[Critical / High / Medium / Low] ; [reason]
Data protected and confidentiality lifetime	[asset classes] ; [beyond 2035 / 2030 to 2035 / up to 2030]
Current cryptography	[protocols, algorithms, key sizes, libraries, certificates]
Target cryptography	[for example TLS 1.3 with ML-KEM-1024; ML-DSA-87 certificates; AES-256]
Path	[upgrade / configure / replace / retire / exception]
Dependencies	[vendor roadmap dates, counterparties, PKI, HSMs, other systems]
Milestones (original dates kept)	Assessment complete [date] ; design approved [date] ; testing complete [date] ; production [date] ; traditional algorithms disabled [date]
Interim controls until transition	[for example segregation, reduced data retention]
Budget and funding source	[\$X] ; [project / BAU]
Evidence of completion	[test results, configuration scan, inventory updated]
Status and RAG	[not started / in progress / complete] ; [green / amber / red]
Exceptions and issues	[references]

Program-level roadmap: summarise all systems by rating and target year against the ASD milestones.

Milestone	ASD milestone	[Organisation] target	Status
-----------	---------------	-----------------------	--------

Milestone	ASD milestone	[Organisation] target	Status
Refined transition plan approved	End of 2026	[31 December 2026]	[status]
Inventory complete: Critical and High systems	Not specified	[30 June 2027]	[status]
Inventory complete: all systems	Not specified	[31 December 2027]	[status]
Transition commenced, starting with critical systems and data	End of 2028	[date, earlier than 31 December 2028]	[status]
Critical systems and trust anchors transitioned	Not specified	[31 December 2029]	[status]
All systems transitioned	End of 2030	[31 December 2030 or earlier]	[status]
Ongoing monitoring and validation	Post-2030	Ongoing	[status]



[Risk Taxonomy](#)
[Operations](#)
[Library](#)
[Obligations Register](#)
[Why a standard](#)
[About](#)

Disclaimer

© 2026 Risk Frameworks Australia

Free general information only, provided free of charge. Not legal, financial or other professional advice, and used at your own risk. [Read the full disclaimer.](#)