Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Post-quantum questions to ask your vendors

Evaluating third-party readiness for post-quantum cryptography

First published: July 2026

Table of contents

Introduction

Future advances in quantum computing will render traditional asymmetric cryptography vulnerable. A quantum system capable of breaking widely used public-key cryptography is referred to as a cryptographically relevant quantum computer (CRQC).

Post-quantum cryptography (PQC) provides a practical and effective way to mitigate risks posed by a CRQC. Achieving a timely and secure transition to PQC will depend on effective organisational planning and on vendors whose products and services align with those plans and timelines.

Many organisations rely on third-party vendor products, managed services and cloud services to deliver core business and cyber security functions. In these environments, vendors often implement and control cryptographic mechanisms rather than the organisation. As a result, vendor readiness plays a crucial role in an organisation's ability to transition to PQC.

Cryptographic exposure also exists beyond cloud and vendor-managed environments. In systems such as industrial control, access control and network devices, cryptography is often embedded, difficult to update and tied to long asset lifecycles. This can constrain transition timelines and may require vendor support or hardware replacement. These environments include:

- on-premises systems
- legacy systems
- operational technology
- Internet of Things
- building management systems
- physical access and security systems.

To support organisations in their PQC transition, this publication provides a set of vendor-neutral readiness questions to use during procurement activities, contract renewals or ongoing vendor assurance processes. These questions help organisations assess how well a vendor:

- understands quantum-related risks
- maintains transparency over its cryptographic implementations
- supports a secure, cost-effective and timely transition to PQC.

This publication is intended for cyber security leaders, procurement and vendor management teams, and technical stakeholders responsible for assessing third-party readiness for PQC.

In this publication, the term 'vendor' refers to third-party suppliers of products or services. The term 'product or service' includes any vendor-supplied software, hardware, managed service or cloud-based capability that implements or relies on cryptography.

Early engagement on post-quantum readiness

Reliance on vendors means that an organisation's transition to PQC will often depend on the readiness, transparency and roadmaps of its vendors. Even where an organisation has strong cryptographic expertise and a refined PQC transition plan, weaknesses or delays within the supply chain can undermine these efforts and introduce residual risk.

Engaging vendors early on PQC readiness helps organisations:

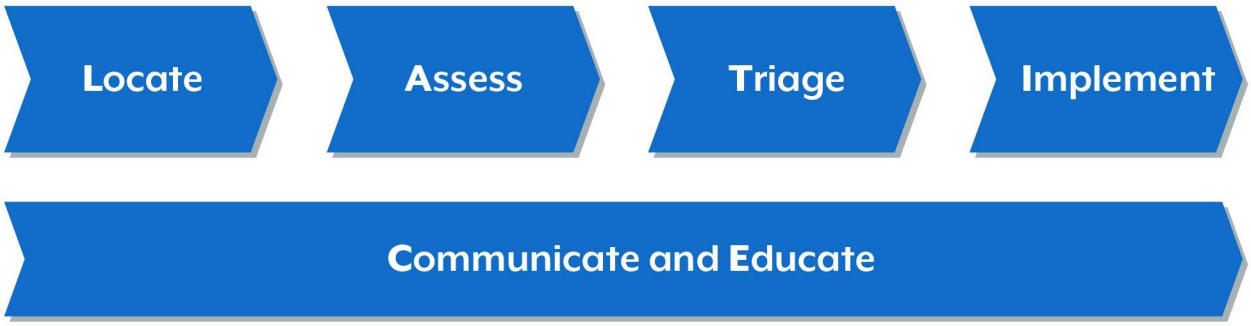
- understand vendor awareness and maturity levels
- identify potential risks or misalignments
- ensure vendor roadmaps support organisational transition plans
- support consistent expectations across procurement, contract management and vendor assurance activities.

Early and structured engagement also reduces the likelihood of late-stage surprises. For example, finding that a critical product, service or dependency cannot support PQC within required timeframes.

Questions to ask vendors

The following questions align to the high-level phases of an organisation's PQC transition, as outlined in the Australian Signals Directorate's (ASD) LATICE framework in *Planning for post-quantum cryptography*:

- **Locate** and inventory cryptographic dependencies.
- **Assess** risk to individual systems.
- **Triage** and prioritise systems for transition.
- **Implement** post-quantum cryptographic algorithms.
- **Communicate** with vendors and **educate** relevant stakeholders.



These questions are intended as a practical tool to support structured engagement with vendors. Organisations can apply them across different vendor types and risk profiles, and adapt them to reflect the risk level of products and services that the vendor provides.

Organisations are not expected to ask every question of every vendor. Instead, apply the questions based on the:

- risk level of the product or service
- degree of cryptographic control exercised by the vendor
- sensitivity and longevity of data involved
- organisation's current stage of PQC transition.

Not all vendors may be able to provide detailed responses initially. However, a vendor's willingness to engage transparently, discuss constraints and demonstrate progress can indicate maturity in both PQC and overall cyber security.

Each question includes an explanation of its relevance, along with key considerations to help evaluate vendor responses.

Locate and inventory cryptographic dependencies

The goal of this phase is to identify where and how a vendor uses cryptography within their products and services, including for authentication, key exchange, signing, data in transit and data at rest. This may include vendor-managed or cloud-based services that rely on cryptography to authenticate, protect or access organisational systems, such as:

- Software as a Service
- managed service providers
- identity services
- backup services
- other third-party platforms.

Gaining early visibility of cryptographic dependencies helps organisations avoid unexpected constraints during PQC transition. Particularly where dependencies are embedded, inherited or difficult to change.

Organisations should prioritise these questions early in vendor engagement. This is particularly important during the early stages of PQC planning, or before entering long-term contracts or cloud service agreements, where cryptographic choices may be difficult to change.

Question	Why it matters	Key response considerations
Do you maintain a current inventory of cryptographic dependencies, such as a cryptographic bill of materials (CBOM) or equivalent artefacts?	Inventorying cryptographic dependencies helps identify and manage algorithms, libraries, protocols, parameters and configurations across a system. This includes where cryptography underpins authentication, signing, and data protection (in transit or at rest).	A complete and current inventory (such as a CBOM) that lists algorithms, protocols, libraries, parameters and configurations, including third-party and embedded components. The inventory should be actively maintained and kept up to date.
Where is cryptography implemented?	Cryptography may exist across multiple layers such as application, operating system, middleware, hardware and firmware. Understanding where it is implemented helps assess PQC transition complexity and feasibility.	Clear identification of cryptographic use across all layers, with no reliance on assumptions.
Is any cryptography hardcoded, fixed or hardware bound?	Cryptography embedded in software, firmware, or hardware can be difficult to replace and may dictate transition timelines. Identifying these dependencies early reduces the risk of delays or forced system replacement.	Confirmation that no such hard-coded, fixed or hardware-bound cryptography exists. Otherwise, identification of affected components across products or services, along with a feasible remediation roadmap such as patching, firmware upgrades, or replacement.
Do third-party dependencies introduce cryptography?	Supply chain components frequently define cryptographic behaviour. Visibility of inherited cryptography helps prevent hidden blockers, support coordination across dependencies, and reduce PQC transition complexity.	Transparent disclosure of all dependencies that introduce cryptography, including the cryptographic libraries they rely on. Standardised libraries are preferred over bespoke or proprietary implementations and should be tracked within a CBOM or equivalent inventory.

Question	Why it matters	Key response considerations
How is cryptography updated?	Patch-based cryptographic updates support cryptographic agility, reduce operational disruption and help avoid large-scale system replacements during PQC transition.	Updates delivered through supported patches or maintenance releases, with clear long-term support commitments.
Do your products or services rely on hardware roots of trust?	Hardware trust anchors can lock in cryptographic choices and constrain transition pathways, particularly where cryptographic functions depend on fixed hardware capabilities.	Identification of hardware trust anchors and their role in cryptographic operations. For example, Trusted Platform Module, Hardware Security Module, and secure enclave usage.
How is firmware authenticity verified?	Firmware signing mechanisms are long-lived and difficult to change, making them a key constraint for PQC transition.	Clear description of firmware signing mechanisms, such as Secure Boot or Unified Extensible Firmware Interface.
Are firmware and boot processes updatable to support PQC signature schemes?	Firmware and boot-chain cryptography may require device replacement if not designed for cryptographic agility.	Evidence that firmware and boot processes can be updated without hardware replacement. Otherwise, a roadmap for supporting PQC-compatible signature schemes.

Assess risk to individual systems

The goal of this phase is to understand which data and trust decisions rely on traditional asymmetric cryptography, how sensitive and long-lived that data is, and how the vendor assesses the risks posed by a CRQC.

Organisations should use these questions to assess how quantum-related risks apply to a vendor's products or services. This phase is particularly relevant for systems that protect sensitive or long-lived data, or that are externally exposed.

Question	Why it matters	Key response considerations
Which customer data flows rely on traditional asymmetric cryptography?	Explicit mapping of authentication, key exchange, and signing pathways is needed to assess exposure, select appropriate transition approaches and identify edge cases during testing.	Clear mapping of customer data flows that use traditional asymmetric cryptography across interfaces and protocols, including whether those flows protect authentication, key establishment or data integrity.
What data lifetime assumptions does your product or service make for the data it processes or stores, and how can customers configure or manage those lifetimes?	Data with long-lived confidentiality requirements is at risk from future CRQC-enabled attacks, such as 'harvest now, decrypt later', and may require earlier transition to PQC.	Clear articulation of data lifetime assumptions, default retention behaviours and customer controls. These are reflected in the vendor's PQC roadmap and customer configuration guidance.
Do you have a documented, product- or service-specific assessment of risks posed by a CRQC?	Demonstrates that the vendor understands quantum-related cryptographic risks, anticipated timelines and mitigation strategies in line with ASD guidance.	A documented internal assessment that clearly states scope, assumptions and outcomes. It also demonstrates consideration of authoritative guidance.
Do you distinguish between signing, encryption and authentication risks?	Signing, encryption and authentication failures have different impacts and timelines. Integrity and authentication risks may require different transition sequences and controls compared to confidentiality risks.	Clear separation of signing, encryption and authentication use cases, with distinct risk assessments, transition timelines and mitigation strategies for each.
Can customers choose stronger cryptographic settings today?	Using stronger traditional cryptographic settings, such as larger key sizes, may provide marginal, short-term risk reduction. However, these measures do not mitigate the impact of a CRQC and are not a substitute for PQC transition.	Higher security strength options are available as supported, documented configurations rather than bespoke or one-off implementations.

Question	Why it matters	Key response considerations
What authentication mechanisms rely on traditional asymmetric cryptography?	Authentication systems often have long replacement cycles and may become critical bottlenecks.	Identification of authentication mechanisms, such as certificates, smartcards and tokens, including their lifecycle and replacement timelines.

Triage and prioritise systems for transition

The goal of this phase is to ensure that the vendor's transition sequence aligns with organisational risk priorities and ASD's recommended PQC milestones. This should be guided by a risk-based approach to prioritisation.

This phase includes identifying hard blockers early and ensuring that any use of post-quantum/traditional (PQ/T) hybrid approaches is limited to a short-term transition period.

Organisations should prioritise these questions once they understand key cryptographic dependencies and risks. This helps determine whether vendor transition plans and timelines align with organisational risk-based priorities and PQC transition milestones.

Question	Why it matters	Key response considerations
Which products or services will be PQC-ready early enough to support customer rollout before the end of 2030?	Concrete vendor readiness dates enable organisations to plan testing, transition and procurement activities in time to complete PQC transition by the end of 2030.	Product- or service-specific and versioned commitments for PQC-ready releases. Offerings should be available in advance of 2030 to allow for customer testing, staged transition, and production rollout.
Which components require hardware replacement or re-architecture?	Components requiring hardware replacement or re-architecture, rather than straightforward updates, are typically long-lead items and can significantly affect timelines, cost and interoperability during PQC transition.	Transparent disclosure of components requiring hardware replacement or re-architecture, including the reasons for redesign, known constraints or bottlenecks, and any resulting impacts on delivery timelines.

Question	Why it matters	Key response considerations
Do you support PQ/T hybrid modes as a temporary transition mechanism, and how and when will you transition to PQC-only?	PQ/T hybrid schemes may support short-term interoperability or resiliency, but are not recommended as a long-term solution. The presence of a CRQC would render the traditional elements obsolete, requiring transition to purely post-quantum cryptographic algorithms.	Hybrid schemes, if supported, are clearly defined as a transitional measure only. Responses should include a documented plan and timeline for de-hybridisation and transition to PQC-only.
How do you consider customer risk when prioritising PQC transition activities?	Risk-based prioritisation helps ensure that customers with higher exposure or more sensitive data are not delayed due to purely commercial or operational considerations.	A documented and risk-based prioritisation approach that considers factors such as system exposure, data sensitivity and transition complexity, rather than customer size or revenue.
What internal governance arrangements oversee your PQC transitions?	Clear governance and executive accountability reduce implementation risk and support consistent prioritisation across products or services. This includes products and services delivered through managed or shared platforms.	Defined governance structures with executive ownership, documented decision forums, and regular review cycles overseeing PQC planning, delivery and customer impact across products or services.

Implement post-quantum cryptographic algorithms

The goal of this phase is to ensure post-quantum cryptographic algorithms are implemented securely. This includes:

- avoiding premature, proprietary or experimental cryptography
- adopting standardised and reputable libraries
- planning for performance, key management and safe rollback.

Organisations should apply these questions when evaluating a vendor's technical readiness to deliver PQC in production. This phase is particularly important before enabling PQC in live environments or committing to major upgrades that would be difficult to reverse.

Question	Why it matters	Key response considerations
Which post-quantum cryptographic algorithms will you support, and when will support be generally available to customers?	Support for standards-based post-quantum cryptographic algorithms underpins interoperability, assurance and the long-term sustainability of PQC deployments.	A clear commitment to standards-based, ASD-approved algorithms with defined timelines outlining when support will be available to customers.
Is your PQC implementation production-ready and available for customer use?	Production-ready implementations minimise operational risk and help organisations avoid relying on preview, experimental or unsupported cryptographic functionality during PQC transition.	Availability as a supported, customer-deployable release, with defined support arrangements (such as service-level agreements) and documented guidance for production deployments and operation.
How do you validate and maintain cryptographic libraries?	Using reputable and well-maintained cryptographic libraries reduces security, compliance and long-term maintenance risks, and supports the secure adoption of PQC.	Use of reputable and actively maintained cryptographic libraries with evidence of validation or independent scrutiny. Bespoke or proprietary cryptographic implementations should be avoided, where possible.
How will key management, certificate sizes and lifecycle processes change under PQC?	PQC can increase key and certificate sizes, affecting operational processes and system performance. Poor planning may lead to performance or compatibility issues.	Clear explanation of changes to key and certificate sizes, lifecycles and operational processes, including any impacts on existing systems and how these will be supported in production.
How do customers enable PQC in your product or service?	Clear and supported enablement processes reduce deployment risk and help ensure predictable and safe transitions to PQC.	Documented configuration and deployment steps, including prerequisites and known compatibility or interoperability considerations for relevant protocols and integrations.

Question	Why it matters	Key response considerations
Is PQC included in base licensing?	Including PQC in base licensing avoids security controls being paywalled, which could delay adoption and lead to uneven risk across customers.	Confirmation PQC functionality is included under standard licensing terms, without additional licensing fees or premium add-ons.

Communicate with vendors and educate relevant stakeholders

This phase helps institutionalise change and sustain security posture beyond initial PQC transition timeframes. The goal of this phase is to ensure:

- clear communication with vendors
- well-defined cryptographic deprecation roadmaps
- appropriately trained support staff.

Organisations should use these questions throughout the PQC transition to maintain effective vendor engagement. This phase is critical for managing cryptographic change, minimising customer impact, and supporting long-term operational readiness.

Question	Why it matters	Key response considerations
How are customers notified of cryptographic changes?	Proactive notification of cryptographic changes enables organisations to assess impact, schedule testing, and maintain security and compliance requirements.	Formal and predictable communication mechanisms, such as security advisories, pre-release notes and transition notices.
Do you provide customer-ready transition guides for PQC?	Clear and practical transition guidance reduces integration effort and errors. This supports safer and more efficient adoption of PQC.	Clear and customer-ready instructions for enabling and validating PQC, including examples and testing guidance.
How will traditional cryptography be deprecated, including any temporary use of PQ/T hybrid approaches?	Phased deprecation with clear notice periods helps avoid abrupt change, supports parallel testing, and ensures hybrid approaches remain temporary during transition.	Clear deprecation timelines covering warning periods, support windows, any interim hybrid use, and final removal of traditional cryptography, with a defined path to PQC-only operation.

Question	Why it matters	Key response considerations
Are your support and engineering teams trained to support PQC?	Trained teams reduce support risk and accelerate incident resolution during transition.	Evidence of staff training, updated runbooks, and documentation of known issues.
Does your roadmap align with ASD guidance and support PQC transition by the end of 2030?	Alignment with authoritative guidance helps avoid dead-ends and ensures customer transition plans can be completed within expected timeframes.	Roadmaps that reference relevant ASD guidance with clear milestones supporting customer testing, transition and production rollout before the end of 2030.
Do you contribute to or track relevant PQC standards bodies, and how does this influence your roadmap?	Engagement with standards bodies supports alignment with emerging PQC standards, reduces incompatibility risks, and enables vendors to share implementation challenges to improve practicality and interoperability.	Evidence of participation in, or tracking of, relevant standards bodies and how this informs product roadmaps and implementation decisions.

Common concerns in vendor responses

When engaging vendors on PQC readiness, organisations may encounter responses that indicate differing levels of maturity, visibility or preparedness. These concerns do not necessarily indicate unacceptable risk. However, they may warrant additional follow-up, risk treatment or attention depending on the risk level of the vendor and the products or services provided.

Organisations should consider these concerns in context, including the risk level of the vendor, the sensitivity and lifetime of data involved, and the vendor's willingness to engage transparently. Used alongside the questions in this publication, these considerations support risk-informed decisions when managing cryptographic dependencies across the supply chain.

Some common concerns in vendor responses may include:

- limited visibility of cryptographic use
- reliance on general assurances
- unclear or deferred transition timelines
- use of proprietary or opaque cryptography
- treatment of PQC as an optional or premium function
- over-reliance on compensating controls
- lack of governance or ownership.

Summarised list of post-quantum questions to ask vendors

Use these questions, which align to the key phases of ASD's LATICE framework, to assess vendor readiness for PQC.

Organisations are not expected to ask every question of every vendor. Instead, apply the questions based on the vendor's risk level, the degree of cryptographic control exercised by the vendor, data sensitivity and longevity, and the organisation's current stage of PQC transition.

Locate

- Do you maintain a current inventory of cryptographic dependencies, such as a CBOM or equivalent artefacts?
- Where is cryptography implemented?
- Is any cryptography hardcoded, fixed or hardware bound?
- Do third-party dependencies introduce cryptography?
- How is cryptography updated?
- Do your products rely on hardware roots of trust?
- How is firmware authenticity verified?
- Are firmware and boot processes updatable to support PQC signature schemes?

Assess

- Which customer data flows rely on traditional asymmetric cryptography?
- What data lifetime assumptions does your product or service make for the data it processes or stores, and how can customers configure or manage those lifetimes?
- Do you have a documented, product- or service-specific assessment of risks posed by a CRQC?
- Do you distinguish between signing, encryption and authentication risks?
- Can customers choose stronger cryptographic settings today?
- What authentication mechanisms rely on traditional asymmetric cryptography?

Triage

- Which products or services will be PQC-ready early enough to support customer rollout before the end of 2030?
- Which components require hardware replacement or re-architecture?
- Do you support PQ/T hybrid modes as a temporary transition mechanism, and how and when will you transition to PQC-only?
- How do you consider customer risk when prioritising PQC transition activities?
- What internal governance arrangements oversee your PQC transitions?

Implement

- Which post-quantum cryptographic algorithms will you support, and when will support be generally available to customers?
- Is your PQC implementation production-ready and available for customer use?
- How do you validate and maintain cryptographic libraries?
- How will key management, certificate sizes and lifecycle processes change under PQC?
- How do customers enable PQC in your product or service?
- Is PQC included in base licensing?

Communicate and educate

- How are customers notified of cryptographic changes?
- Do you provide customer-ready transition guides for PQC?
- How will traditional cryptography be deprecated, including any temporary use of PQ/T hybrid approaches?
- Are your support and engineering teams trained to support PQC?
- Does your roadmap align with ASD guidance and support PQC transition by the end of 2030?
- Do you contribute to or track relevant PQC standards bodies, and how does this influence your roadmap?

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre