

Post-quantum questions to ask your vendors

Evaluating third-party readiness for post-quantum cryptography



Australian Government

Australian Signals Directorate

cyber.gov.au





Table of contents

Introduction 4

Background 4

Early engagement on post-quantum readiness 5

Questions to ask vendors 6

- Locate and inventory cryptographic dependencies 7
- Assess risk to individual systems 9
- Triage and prioritise systems for transition 11
- Implement post-quantum cryptographic algorithms 13
- Communicate with vendors and educate relevant stakeholders 15

Common concerns in vendor responses 17

More information 18

Introduction

This publication provides vendor-neutral questions that organisations can use during procurement activities, contract renewals or ongoing vendor assurance processes to assess post-quantum cryptography (PQC) readiness. Key topics covered in this publication include:

- the importance of vendor engagement and transparency
- phased questions for evaluating vendor readiness, aligned to PQC transition milestones
- common concerns in vendor responses and how to address them.

Aimed at cyber security leaders, procurement and vendor management teams, and technical stakeholders responsible for assessing third-party PQC preparedness, these questions help organisations evaluate whether a vendor:

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

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) authored this publication in partnership with the United States' Cybersecurity and Infrastructure Security Agency (CISA) and National Security Agency (NSA). Throughout this publication, these organisations are referred to as the 'authoring agencies'.

Background

Advances in quantum computing will change the security landscape for digital communications. Traditional asymmetric cryptography, which protects sensitive data, will be vulnerable to attacks from a cryptographically relevant quantum computer (CRQC). These quantum systems can break widely deployed public-key cryptography.

To manage this risk, organisations should plan and execute a transition to PQC, which includes algorithms designed to remain secure against both quantum-enabled and classical computing threats.

Many organisations rely on third-party vendor products, managed services and cloud services where the vendors choose and implement the cryptographic mechanisms. In this context, a vendor is a third-party supplier of products or services. A product or service includes any vendor-supplied software, hardware, managed service or cloud-based capability that implements or relies on cryptography. 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. These issues 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.

Early engagement on post-quantum readiness

Reliance on vendors means that an organisation's transition to PQC will depend on vendor readiness, transparency and roadmaps. Even when an organisation has strong cryptographic expertise and a refined PQC transition plan, weaknesses or delays in the supply chain can affect progress 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
- maintain consistent expectations across procurement, contract management and vendor assurance activities related to PQC.

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

Questions to ask vendors

The questions in the following section align to the high-level phases of an organisation's PQC transition, as outlined in ASD's ACSC's LATICE framework[1] in *Planning for post-quantum cryptography*:

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



Use these questions to structure engagement across different vendor types and risk profiles. Tailor depth based on the risk level of the product or service, the degree of cryptographic control exercised by the vendor, data sensitivity and longevity, and the organisation's current stage of PQC transition.

Some vendors may not 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 broader cyber security practices.

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

1 This publication uses ASD's ACSC's LATICE framework as an organising construct. The authoring agencies include similar transition activities in their PQC guidance.

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. This includes authentication, key exchange, signing, data in transit and data at rest. It also may cover vendor-managed or cloud-based services that rely on cryptography to authenticate, protect or access organisational systems. Examples include:

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

Understanding cryptographic dependencies early on helps organisations avoid unexpected constraints during PQC transition, especially where dependencies are embedded, inherited or difficult to change.

Prioritise these questions early in vendor engagement, particularly 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.

Refer to **Table 1** for structured discovery and inventory questions.

Table 1: Locate and inventory cryptographic dependencies

Question	Why it matters	Key response considerations
Do you maintain a current inventory of cryptographic dependencies, such as cryptographic bills of materials (CBOM)[2] or equivalent artefacts?	Inventorying cryptographic dependencies helps identify and manage algorithms, libraries, protocols, parameters and configurations across systems. This inventory should include where cryptography underpins authentication, signing, and data protection (in transit or at rest).	Complete and current inventories (such as CBOMs) that lists algorithms, protocols, libraries, parameters and configurations, including third-party and embedded components. The inventory should be actively maintained.
Where is cryptography implemented?	Cryptography may exist across application, operating system, middleware, hardware and firmware layers. Knowing where it is used helps determine how difficult a PQC transition will be.	Clear identification of cryptographic use across all layers, with no reliance on assumptions.

2 A CBOM is an extension of a software bill of materials, with additional elements beyond those defined in CISA's *2026 Minimum Elements for a Software Bill of Materials (SBOM)* publication. These additional elements document the algorithms implemented by cryptographic libraries and configurations.

Question	Why it matters	Key response considerations
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.
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. Embedded certificates or other cryptographic material within these trust anchors may be difficult to replace or update.	Identification of hardware trust anchors and their role in cryptographic operations. Responses should include any PQC transition constraints, affected components, and feasible remediation approaches such as patching, firmware upgrades or replacement.
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.
Can the firmware and boot processes be updated 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.

Use these questions to assess how quantum-related risks apply to a vendor's products or services, particularly for systems that protect sensitive or long-lived data, or that are externally exposed.

Refer to **Table 2** for focused assessment questions.

Table 2: Assess risk to individual systems

Question	Why it matters	Key response considerations
Which customer data flows rely on traditional asymmetric cryptography?	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, specifying whether those flows protect authentication, key establishment or data integrity.
What assumptions does your product or service make about the lifespan of the data it processes or stores, and how can customers configure or manage those lifespans?	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 are reflected in the vendor's PQC roadmap and customer configuration guidance. These factors should be weighed against customer data lifespans and their required cryptographic needs from the product or service.
Do you have a documented, product- or service- specific assessment of CRQC risks?	This demonstrates the vendor understands quantum-related cryptographic risks, anticipated timelines and mitigation strategies, aligned with relevant guidance[3].	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.

3 In this publication, 'relevant guidance' refers to guidance published by the authoring agencies and other national cyber security authorities, as applicable to an organisation's jurisdiction, sector and risk environment.

Question	Why it matters	Key response considerations
Can customers choose stronger cryptographic settings today?	Using stronger traditional cryptographic settings, such as larger key sizes, may offer only marginal, short-term risk reduction. However, these measures do not address the risks posed by a CRQC and are not a substitute for transitioning to PQC.	Higher security strength options are available as supported, documented configurations rather than bespoke or one-off implementations.
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 the vendor's transition sequence aligns with organisational risk priorities and PQC milestones recommended by the relevant authoring agency for your organisation. Identify hard blockers early and ensure any use of post-quantum/traditional (PQ/T) hybrid approaches is temporary. Prioritise these questions once cryptographic dependencies and risks are understood.

Refer to **Table 3** for prioritisation and governance questions.

Table 3: Triage and prioritise systems for transition

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?[4]	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?	Hardware changes are long-lead items and can significantly affect timelines, cost and interoperability.	Transparent disclosure of components requiring hardware replacement or re-architecture, including reasons for redesign, known constraints or bottlenecks, and any resulting impacts on delivery timelines.
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 pure PQC 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.

4 References to a 2030 timeframe reflect PQC transition objectives set out in ASD's *Information security manual* and *Planning for post-quantum cryptography*, and are included as a planning milestone for vendor readiness discussions. Align transition activities with guidance applicable to your organisation's jurisdiction, sector and risk environment.

Question	Why it matters	Key response considerations
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 that oversee PQC planning, delivery and customer impact across products or services.

Implement post-quantum cryptographic algorithms

The goal of this phase is to ensure PQC 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.

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

Refer to **Table 4** for implementation-focused questions.

Table 4: Implement post-quantum cryptographic algorithms

Question	Why it matters	Key response considerations
Which PQC algorithms will you support, and when will support be generally available to customers?	Support for standards-based PQC algorithms underpins interoperability, assurance and the long-term sustainability of PQC deployments.	A clear commitment to standards-based algorithms, approved by the appropriate authoring agency for your organisation, 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.

Question	Why it matters	Key response considerations
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.
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 that 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 support:

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

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

Refer to Table 5 for communication and education-focused questions.

Table 5: Communicate with vendors and educate relevant stakeholders

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?	Clear timelines for retiring old cryptography helps organisations avoid abrupt change, plan testing, and make sure hybrid methods are used only briefly.	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.
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.

Question	Why it matters	Key response considerations
Does your roadmap align with relevant guidance and support PQC transition by the end of 2030?	Alignment with authoritative guidance helps avoid dead-ends and helps ensure customer transition plans can be completed within expected timeframes.	Roadmaps that reference relevant 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.

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.

More information

To empower organisations in navigating the transition to PQC further, authoritative resources from the authoring agencies provide practical guidance and actionable frameworks. Leveraging these resources enables organisations to make informed decisions, demand transparency from vendors, and ensure a secure, cost-effective and timely transition to PQC.

Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC)

- *Planning for post-quantum cryptography*
  Advice to assist organisations prepare for PQC with recommended transition timelines, milestones, and a framework to map transition stages.
- Guidelines for cryptography
  Practical cryptography guidance on how organisations can protect their information technology and operational technology (OT) systems from cyber threats.
- *Choosing secure and verifiable technologies*
  Provides practical guidance for assessing the security, transparency and trustworthiness of technology vendors, products and services throughout their lifecycle.

Cybersecurity and Infrastructure Security Agency (CISA)

- *Post-Quantum Cryptography Initiative*
  Offers technical strategies and risk management advice for preparing critical infrastructure and government networks for quantum-enabled threats.
- *Secure by Design*
  Encourages technology providers and customers to prioritise security from the outset, ensuring products are resilient against evolving cyber risks.
- *Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products*
  Outlines key questions and criteria for evaluating vendor readiness and product security maturity, especially for OT environments.
- *Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem*
  Provides actionable guidance for software customers to drive a secure technology ecosystem by demanding security as part of the procurement process.

National Security Agency (NSA)

- *Quantum-Readiness: Migration to Post-Quantum Cryptography* [PDF 545 KB]
  Outlines practical steps for achieving PQC readiness, including cryptographic discovery, risk assessment, supply chain engagement, and discussions with technology vendors.
- *The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ* [PDF 432 KB]
  Answers numerous questions about PQC and how to prepare for the transition to PQC.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au

1300 CYBER1 (1300 292 371)

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

© Commonwealth of Australia 2026

With the exception of the Coat of Arms, the entity's logo, third party content, and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license https://creativecommons.org/licenses/by/4.0/

For the avoidance of doubt, this means this license only applies to material as set out in this document.

The details of the relevant license conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 license https://creativecommons.org/licenses/by/4.0/legalcode.en

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