Planning for post-quantum cryptography

First published: July 2022

Last updated: September 2025

Introduction

A cryptographically relevant quantum computer (CRQC), when it becomes available, will threaten the security of systems that rely on traditional asymmetric cryptographic algorithms. Notably, the security of both authentication flows and data in transit will be vulnerable. For example, web applications that use Transport Layer Security (TLS) to authenticate users and encrypt communications may be vulnerable to cyber attacks that seek to compromise the integrity or confidentiality of data.

Post-quantum cryptography

Post-quantum cryptography (PQC) involves the creation and analysis of quantum-resistant cryptographic algorithms, known as post-quantum cryptographic algorithms. These algorithms derive their security from mathematical problems that are considered difficult for both classical and quantum computers. In principle, these algorithms offer a low-cost and practical path to maintaining the security of data in the presence of a CRQC.

The Australian Signals Directorate (ASD) produces the *Information security manual* (ISM) which contains detailed advice on ASD-approved cryptographic algorithms, key sizes and parameters. ASD will continue to update the ISM as post-quantum cryptographic algorithms undergo scrutiny and as use cases arise that existing cryptographic algorithms may not address.

ASD encourages research, testing and practical trials of post-quantum cryptographic algorithms. Further research and development of these algorithms offers a practical and cost-effective step towards securing real-world communications in the presence of a CRQC. More broadly, ASD encourages industry to continue research and development of quantum technologies. This includes practical vulnerability research to understand the risks associated with employing quantum technologies.

Quantum key distribution

ASD will also continue to monitor methods of securing communications in the presence of a CRQC, such as quantum key distribution (QKD). However, practical limitations of QKD (including specialised hardware, and concerns around availability and native authentication) mean that ASD does not support its use for secure communications.

Reasons to address the threat of a CRQC now

Organisations should prioritise the protection of their information technology (IT) environment against the threat of a CRQC now, even though a CRQC may not exist for some time. Early action is crucial because:

- deploying protections against a CRQC may take longer than expected
- estimating the timeline to achieve a CRQC is uncertain as quantum computing is an active area of research
- storing highly sensitive or classified data using classical encryption methods may be vulnerable to 'harvest now, decrypt later' attacks.

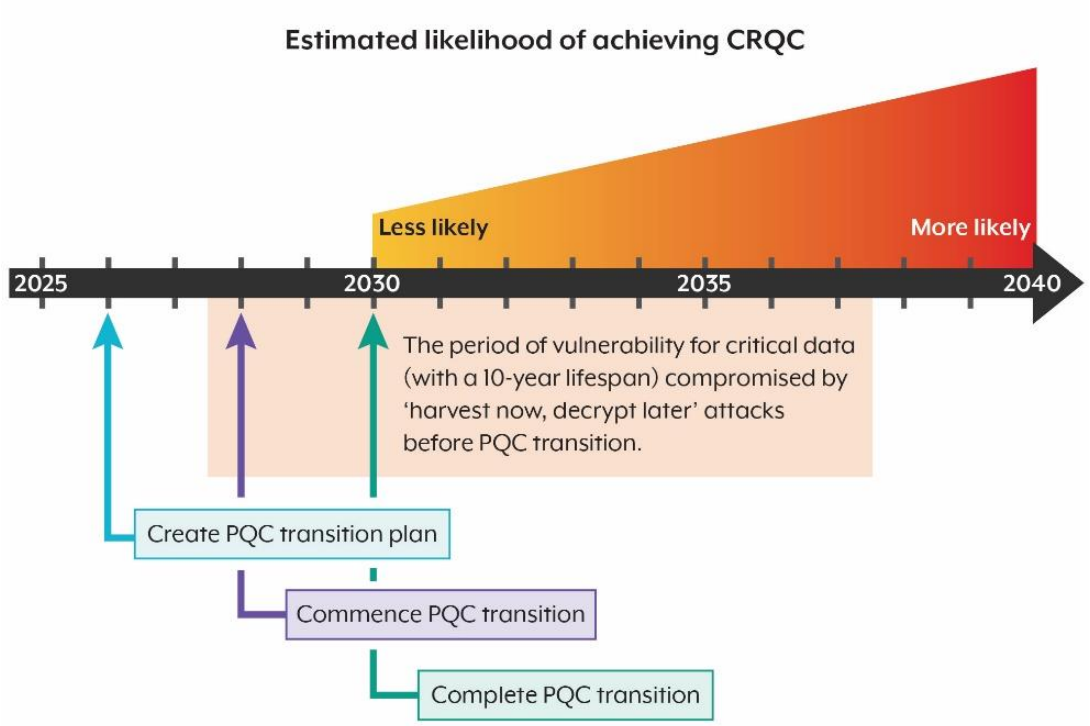
Some service providers and vendors have begun their transition to PQC, with some offering PQC-only solutions and products. The shift to PQC will happen at different speeds and will depend on factors such as cost, dependent technology updates and legacy interoperability. This further highlights the need for organisations to start planning for their PQC transition right away.

Transition timeline

In the ISM, ASD recommends ceasing the use of traditional asymmetric cryptography by the end of 2030. This includes cryptographic algorithms such as the Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) primitives. Instead, ASD recommends using post-quantum ASD-approved cryptographic algorithms as described in the ISM's *Guidelines for cryptography*.

Adoption of PQC by the end of 2030 includes contingencies for disruptive technology breakthroughs and other external factors. Organisations should also include additional contingencies to allow for internal factors that may delay their PQC transition.

The diagram below shows ASD's recommended PQC transition timeline against the increasing risk of a CRQC becoming available each year.



Transition milestones

Organisations should consider the scale and nature of their IT environments when planning their PQC transition. To guide organisations in transitioning to PQC by the end of 2030, ASD recommends the following high-level milestones.

By end of 2026: Organisations should have a refined plan for their transition to PQC. The transition plan should account for organisations' security goals, risk tolerances, dependencies and the value of their data.

By end of 2028: Organisations should have commenced their transition to PQC, starting with their critical systems and data. This includes prioritising systems that:

- are critical to the function of the organisation
- handle data that is highly sensitive, classified or has long-lived confidentiality requirements
- are likely to prove difficult or time consuming to update.

By end of 2030: Organisations should have completed their PQC transition.

Post-2030: It is essential that organisations continually monitor and validate their implementation of PQC to ensure they maintain their cyber security posture. This involves ensuring PQC implementations function as intended and are resilient to new and evolving cyber threats. It is crucial that organisations also continuously monitor for vulnerabilities, optimise performance and adapt to potential changes in the quantum threat landscape.

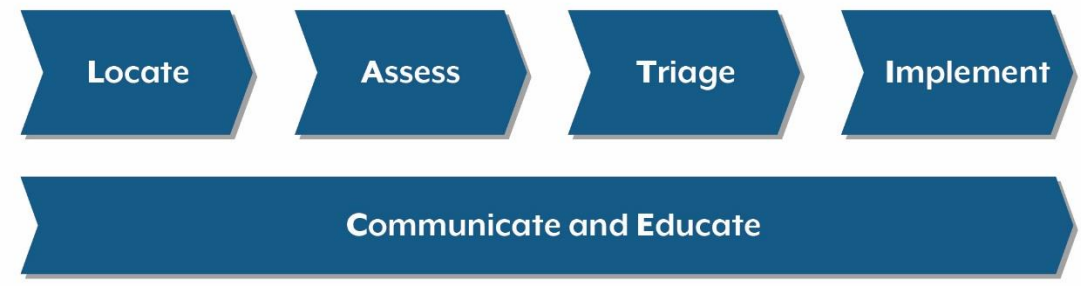
Transition stages

The details of a successful transition to PQC may vary across organisations. Factors that play a role could include the:

- size of their IT environments, and whether system components are mostly commodity or bespoke
- nature of the cyber threats faced
- resources available for transition activities
- presence of business partners or customers who require legacy interoperability.

Organisations are encouraged to consider the LATICE framework when undertaking their PQC transition. LATICE outlines the 5 high-level phases of the PQC transition:

- **Locate** and inventory the use of traditional asymmetric cryptography.
- **Assess** the value and sensitivity of systems and data protected by traditional asymmetric cryptography.
- **Triage** systems using traditional asymmetric cryptography and prioritise individual systems for transition.
- **Implement** post-quantum cryptographic algorithms throughout systems.
- **Communicate** with vendors and stakeholders, and **educate** and train relevant stakeholders on the PQC transition.



While the importance and complexity of these 5 phases will vary across organisations, some common considerations are discussed below.

Locate

The goal of the 'locate' phase is to discover and document where organisations use traditional asymmetric cryptography. Consider all components of IT environments such as:

- cloud services
- applications

- hardware
- operational technology.

Any of these components could potentially rely on traditional asymmetric cryptography for digital signatures, authentication flows or encryption of data in transit.

Cryptographic bill of materials

A cryptographic bill of materials (CBOM) is an effective method for creating an inventory of cryptographic dependencies at environment and system levels. A CBOM serves a similar purpose to a software bill of materials. It captures relevant cryptographic implementations that a product, system or environment relies upon.

A mature CBOM details the cryptographic implementations in the context they are used, and captures information on cryptographic products, software, libraries, algorithms, protocols, parameters, versions and configurations. Initially, organisations' high-level CBOMs may be a simple list of critical systems and components mapped to the critical security functions that they rely on for cryptography to perform.

Assess

The goal of the 'assess' phase is to identify the value and sensitivity of systems within organisations that use traditional asymmetric cryptography. In doing so, organisations should consider the impact that the compromise of system integrity or confidentiality (if realised) would have on their business operations, including any regulatory or legal implications.

Triage

The goal of the 'triage' phase is to consider the risk to organisations from a CRQC, and to identify the relative importance and subsequent priority of PQC transition for different systems. Factors that may play a role in prioritising individual systems for transition could include whether a system:

- handles sensitive or classified data
- interacts with external organisations
- is expected to easily transition
- implements standards for legacy interoperability
- is bespoke or commodity
- has relevant non-cryptographic protections that apply
- follows a specific lifecycle and refresh cadence.

Implement

The goal of the 'implement' phase is to apply post-quantum cryptographic algorithms to systems. Organisations may achieve this through new or existing service providers, or do this in-house. In many cases, this phase may consist of:

- patching existing applications, hardware and operational technology
- changing software libraries according to vendor guidance
- undertaking new procurement actions to replace old system components.

Organisations should use standardised and reputable software libraries when carrying out in-house upgrades to bespoke systems. This also applies when adopting software libraries from service providers and vendors. It is crucial that organisations do not rush ahead of standardised and verified implementations.

Post-quantum/traditional hybrid schemes

ASD does not recommend, but does not prohibit, the use of post-quantum/traditional (PQ/T) hybrid schemes. For interoperability and resiliency reasons, organisations may consider a PQ/T hybrid scheme in their PQC transition. However, the presence of a CRQC will render traditional elements of PQ/T hybrid schemes obsolete. This means that all organisations should expect to transition to purely post-quantum cryptographic algorithms in the future.

Communicate and educate

The goal of the 'communicate and educate' phase is to position organisations to handle the deployment of post-quantum cryptographic algorithms and to manage their sustainment into the future. Ideally, the transition to PQC will occur in a way that is transparent to most stakeholders. The monitoring of the transition will also guide communications to stakeholders.

The transition to PQC will affect some areas of organisations more directly than others. This may include areas that manage the deployment or security for systems that include traditional asymmetric cryptography. More subtly affected areas may be impacted by mild increases in data sizes and the computation needed for post-quantum cryptographic algorithms.

Additional guidance

Many other standards, industry and government bodies have published PQC guidance for their target audiences, fitting the regulatory and policy regimes within which they operate.

Please note, the resources below may suggest recommendations and proposed timeframes that are different from the advice that ASD presents in this publication. However, they share similar considerations behind the challenges and timelines for transitioning to post-quantum

cryptographic algorithms. This publication therefore aims to support organisations that apply the ISM, while the resources below offer additional information.

Standards bodies

The Internet Engineering Task Force (IETF), which has members from across the technology sector and government bodies, produces standards to ensure the interoperability of internet-based communications. For example, the IETF maintains the standard for TLS, which is one of the most important protocols for internet security, and is currently undergoing its own PQC adoption and standardisation process.

The European Telecommunications Standards Institute published *CYBER; Quantum-Safe Cryptography (QSC); A Repeatable Framework for Quantum Safe Migrations*, which details the steps in PQC transition.

Industry bodies

The Post-Quantum Cryptography Coalition comprises not-for-profit and commercial entities in the technology sector, and publishes a variety of informational products and tools to assist with activities such as planning for PQC transition.

Government bodies

The United States' National Institute for Standards and Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA), and National Security Agency provide a range of resources on PQC, including their joint *Quantum-Readiness: Migration to Post-Quantum Cryptography*.

NIST provides further information on post-quantum cryptography standardisation, including their *Transition to Post-Quantum Cryptography Standards* publication.

CISA provide their post-quantum cryptography initiative, along with tailored advice in their *Preparing Critical Infrastructure for Post-Quantum Cryptography* and *Post-Quantum Considerations for Operational Technology* publications for a United States audience.

The United Kingdom's National Cyber Security Centre provide their *Next steps in preparing for post-quantum cryptography* and *Timelines for migration to post-quantum cryptography guidance* publications for a United Kingdom audience.

Canada's Canadian Centre for Cyber Security provide their *Roadmap for the migration to post-quantum cryptography for the Government of Canada* and *Preparing your organization for the quantum threat to cryptography* publications for a Canadian audience.

New Zealand's National Cyber Security Centre provides information on preparing for PQC transition in the Cryptography chapter of their *New Zealand Information Security Manual*.

The Department of Industry, Science and Resources provide Australia's strategy for the quantum industry and quantum technologies in their *National Quantum Strategy*.

Further information

The *Information security manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with its Essential Eight, complements this framework.

Contact details

If you have any questions regarding this guidance, you can write to us or call us on 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 2025

With the exception of the Coat of Arms 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).

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre