

Guidelines to Sector Leads and CIIOs for Adoption of Quantum-safe Requirements and Migration Plan Outline

1. Quantum computing poses a fundamental threat to the cryptographic standards that underpin today's digital infrastructure. A cryptographically relevant quantum computer (CRQC) — one powerful enough to break widely used algorithms such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) — is expected to emerge within the next decade, rendering current security measures obsolete and exposing critical systems to significant risk.

[1] [RSA \(Rivest-Shamir-Adleman\) and ECC \(Elliptic Curve Cryptography\) are widely used public key cryptographic algorithms that are vulnerable to quantum computing attacks](#)

2. To ensure that Critical Information Infrastructure (CII) systems delivering Essential Services remain resilient against this threat, Critical Information Infrastructure Owners (CIIOs) are required to implement or migrate their CII computer and computer systems to quantum-safe solutions in accordance with the timelines set out in this guidance.

3. CSA recognises that quantum-safe migration is a non-trivial undertaking. It requires Senior Management commitment, multi-year planning, and sustained resourcing. The solution space continues to mature, and quantum-safe options remain limited in certain areas, particularly for Operational Technology (OT) systems. Nonetheless, delaying the planning process increases the risk of failing to meet migration timelines and widens the window of exposure for sensitive data and communications.

4. CIIOs should also account for the technical implications of Post-Quantum Cryptography (PQC) algorithms, which require larger key sizes, increased computational overhead, and greater memory requirements compared to current RSA and ECC implementations. CII systems operating under strict latency or high-throughput requirements may encounter performance impacts that could affect operational effectiveness and the reliable delivery of Essential Services. These considerations should be factored into migration planning from the outset.

5. CIIOs are required to submit their quantum-safe migration plans to CSA via their Sector Leads in accordance with the timelines below. CSA may also conduct interim check-ins to monitor progress and understand challenges faced.

6. By 31 March 2027 – Submission of CIIO's quantum-safe migration plan to CSA via their Sector Leads.

6.1. The quantum-safe migration plan submission shall be completed in accordance with the attached template. At minimum, the submission must include the following:

6.1.1. Names of the dedicated personnel overseeing migration, as well as the responsible board member or senior leader accountable for quantum-safe migration.

6.1.2. List of CII assets (e.g. VPN, authentication systems, OT protocols requiring firmware signing, databases, backup systems, etc) using vulnerable cryptography. Details include but are not limited to the following:

6.1.2.1. Service provided by the asset;

6.1.2.2. Cryptographic protocols and algorithms in use;

6.1.2.3. Source of the assets, i.e. commercial off-the-shelf, government-provided, or other (e.g. in-house developed);

6.1.2.4. Dependencies on the asset;

6.1.2.5. Migration approach including the timeline, choice of quantum-safe solution(s), partnership with third-party vendors, potential risks, etc.; Or if not migrated, interim mitigation controls and justifications.

6.1.3. Incorporation of quantum-related risks and considerations into risk management frameworks and procurement policies.

6.1.4. Potential challenges and support needed.

7. From 1 January 2028 – Procurement and implementation of new CII computer and computer systems to include quantum-safe considerations.

7.1. All contracts to procure and implement new CII computer and computer systems that have a digital component² from 1 January 2028 must either (a) support quantum-safe algorithms/technologies; and/or (b) be quantum-safe ready, i.e. capable of supporting quantum-safe algorithms/technologies by 31 December 2031.

[\[2\] Refers to any hardware, software, or embedded system that processes, stores, transmits, or controls data and communications essential to the operation, monitoring, or management of the CII computer and computer system to deliver Essential Services.](#)

7.2. CII computer and computer systems that do not incorporate cryptographic assets are exempt from the requirements under Section 7.1.

8. By 31 December 2031 – Completion of quantum-safe migration for CII computer and computer systems.

8.1. Quantum-safe migration of CII computer and computer systems must be completed by 31 December 2031. From this date, vulnerable cryptography (i.e. RSA and ECC implementations) should no longer be used in CII computer and computer systems to deliver Essential Services.

Frequently Asked Questions

1. Completeness of CIIOs' submission of migration plan

a. Is there a template for submission of the migration plan?

A template for the submission of the migration plan is attached with these guidelines. Organisations may also submit in alternative formats, provided that all sections of this template are fully addressed. CIIOs may attach supporting documents and reference them accordingly in the submission.

b. What if a CIIO is unable to address all required details in the migration plan?

CIIOs should provide as much detail as possible at the point of submission. The primary intent of the migration plan is to support progressive planning, not to require a complete and finalised roadmap upfront. Where information cannot be provided, CIIOs must notify CSA with reasons, and CSA will review and address gaps on a case-by-case basis.

c. What if a CIIO is unable to meet the 31 Mar 2027 submission deadline?

CIIOs that are unable to meet the submission deadline must inform their respective Sector Leads in advance, providing a proposed extension date and reasons for the delay. Extensions are subject to CSA's review and approval.

d. What if migration progress deviates from the submitted plan?

Migration plans are not expected to be static. CSA recognises that CIIOs may need to adjust their approach as implementation progresses. CIIOs should update their plans accordingly and flag material deviations to CSA and their Sector Leads.

e. Are air-gapped systems required to be included in the migration plan?

Yes. CIIOs must assess whether air-gapped systems contain cryptographic assets. Where a CIIO determines that an air-gapped system need not be included in the migration plan, this determination must be documented and justified in the submission.

2. Scope

- a. Do the quantum-safe migration requirements apply to non-CII systems?*

The requirements apply to CII systems only. However, CIIOs are strongly encouraged to ensure that systems connected to or interfacing with CII systems are adequately protected, given the potential for lateral risk exposure.

- b. Is there flexibility to extend beyond the 31 December 2031 migration deadline?*

CSA does not intend to extend the migration deadline. CIIOs should plan to meet the timeline, as doing so directly reduces the window of risk exposure. Where genuine technical impediments exist, CSA will engage the relevant CIIO on a case-by-case basis.

- c. How should CIIOs develop migration plans when quantum-safe solutions for their systems are not yet available?*

CIIOs should document known gaps in their migration plans, including systems or components for which quantum-safe solutions are not yet available. This allows CSA to provide targeted support, including engaging vendors to signal market demand for specific technical capabilities.

- d. Do these guidelines carry regulatory force?*

These guidelines set out CSA's quantum-safe expectations for CII systems. CSA will monitor migration progress and reserves the right to strengthen interventions where CII preparedness is assessed to be inadequate.

- e. What is the purpose of the 1 January 2028 procurement requirement, given that all CII systems must be quantum-safe by 31 December 2031?*

The procurement requirement serves two purposes. First, it establishes an interim milestone to maintain momentum over the five-year migration timeline. Second, it ensures that vendors proactively build quantum-safe capabilities into new systems from the point of procurement, rather than deferring development to the final migration deadline.

- f. Does the procurement requirement apply to contracts already awarded prior to 1 January 2028?*

Contracts awarded prior to 1 January 2028 are not subject to the procurement requirement, including those with implementation

commencing after this date. However, where such contracts extend beyond 31 December 2031, the relevant systems must meet the quantum-safe migration requirements by that date.

3. Recommended solutions

a. What quantum-safe solutions do CSA recommend?

CSA recommends two primary categories of quantum-safe solutions: (a) the three NIST Post-Quantum Cryptography (PQC) standards, given their extensive testing and broad international acceptance; and (b) existing symmetric cryptographic algorithms and hash functions — specifically AES and SHA at sufficiently large key sizes — which are considered quantum-safe. Quantum Key Distribution (QKD) may be considered for niche, high-security point-to-point applications but is not a primary recommendation. CIIOs should select solutions appropriate to their specific use cases. CSA's Quantum-Safe Handbook will be updated to provide further guidance on recommended options.

b. What if CSA's recommendations on quantum-safe algorithms or technologies are updated?

The solution space continues to evolve, and CSA will update its guidance to reflect material developments to PQC standards and quantum-safe solutions. CSA's recommendations are aligned with international and industry approaches. CIIOs are encouraged to build flexibility into their migration strategies to accommodate future developments, and to engage CSA as new developments emerge.

c. What is CSA's position on the use of QKD?

QKD is a complementary technology suited to niche use cases, such as high-security point-to-point links. PQC and quantum-safe classical algorithms remain the primary recommended options for CII migration.

d. Will CSA provide a list of recommended vendors that CIIOs can engage?

CSA does not maintain a list of recommended vendors. Existing cybersecurity consultancies and vendors are developing capabilities in this space and may serve as a useful resource for CIIOs.

e. Will CSA accept non-NIST PQC algorithms?

Should CIIOs choose to adopt alternative PQC algorithms, they should indicate this in their migration plan and CSA will review and assess them accordingly.

4. Support initiatives

- a. *How will CSA be providing support to CIOs during this 5-year timeline?*

CSA's guidance and advisory resources, including the Quantum-Safe Handbook and Quantum Readiness Index, will be updated progressively to provide practical considerations and reference material for migration planning. CSA will also continue to engage industry and international partners to advance understanding of the quantum-safe solution space and explore practical support mechanisms, including training and workshops. Further details on support initiatives will be communicated to CIOs and Sector Leads in due course.