



CCAPAC Annual Report 2026

# Quantum Readiness in Asia: Risks and Opportunities

*A Review of Quantum Developments in  
Australia, China, India, Japan, Singapore, and South Korea*



This year's CCAPAC report is produced with the assistance of Cisco, and the Access Partnership Institute. CCAPAC notes that the views and conclusions expressed herein are those of the author and do not necessarily reflect the official policy or position of Cisco or the Access Partnership Institute. We thank all collaborators and dialogue partners for their valuable input and engagement in the development of this report.



Copyright © Coalition for Cybersecurity in Asia-Pacific (CCAPAC) 2026.

All rights reserved.

The Coalition for Cybersecurity in Asia-Pacific or CCAPAC is a group of dedicated industry stakeholders who are working to positively shape the cybersecurity environment in Asia through policy analysis, engagement, and capacity building.

To find out more on how to join us, visit our website at <https://ccapac.asia>

---

## Table of Contents

|                                                                                                                                                                                                                   |    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Executive Summary .....                                                                                                                                                                                           | 5  |
| Chapter 1 - What is quantum computing, PQC and why the focus now?.....                                                                                                                                            | 7  |
| 1.1    What is quantum computing?.....                                                                                                                                                                            | 8  |
| 1.2    Opportunities from quantum computing and quantum networking .....                                                                                                                                          | 8  |
| 1.3    The risks of quantum computing - the security challenge quantum computing poses to traditional encryption schema .....                                                                                     | 9  |
| 1.4    Is there a future for security after existing encryption schemas collapse? The current state of quantum-resistance - Post-Quantum Cryptography, and resilience planning by governments and the industry 12 |    |
| 1.5    PQC, Q-Day, and the Long Lead Time - Why Asia Pacific needs to make resilience preparations now .....                                                                                                      | 15 |
| Chapter 2 - Multidimensionality of Challenges and Risks in PQC .....                                                                                                                                              | 17 |
| 2.1    Making the move to PQC - Understanding and Managing PQC Security and Systems Risks Gaps 18                                                                                                                 |    |
| 2.2    Assessing and Managing Cryptographic Agility Gaps .....                                                                                                                                                    | 19 |
| 2.3    Balancing Computing Performance and Cost .....                                                                                                                                                             | 21 |
| 2.4    Migration Challenges - Hybrid Phase Benefits and Vulnerabilities .....                                                                                                                                     | 21 |
| 2.5    Decisions for Standards - International Interoperability and Standards Asymmetries .....                                                                                                                   | 23 |
| Chapter 3 - PQC Policy and Regulatory Readiness in Asia Pacific: Australia, China, India, Japan, Singapore, and South Korea .....                                                                                 | 25 |
| Australia .....                                                                                                                                                                                                   | 26 |
| China .....                                                                                                                                                                                                       | 30 |
| India .....                                                                                                                                                                                                       | 36 |
| Japan.....                                                                                                                                                                                                        | 42 |
| Singapore .....                                                                                                                                                                                                   | 47 |
| South Korea .....                                                                                                                                                                                                 | 52 |
| Case Study: Taiwan Market Profile - Quantum-Safe Developments .....                                                                                                                                               | 59 |
| Quantum Readiness in APAC - Comparative Summary Chart.....                                                                                                                                                        | 61 |
| Chapter 4 - Recommendations for the Enterprise .....                                                                                                                                                              | 64 |
| Chapter 5 - Considerations for Government Legislators and Policy Makers .....                                                                                                                                     | 70 |
| Conclusion - The Imperative of Quantum Readiness in Asia Pacific .....                                                                                                                                            | 76 |

---

## List of tables

|                                                                       |    |
|-----------------------------------------------------------------------|----|
| Table 1: Classical Computing vs Quantum Computing Comparison .....    | 8  |
| Table 2: India's Milestones and Timelines for Quantum Migration ..... | 39 |

---

## List of Figures

|                                                                                                                                   |    |
|-----------------------------------------------------------------------------------------------------------------------------------|----|
| Figure 1: Symmetric vs Asymmetric Encryption .....                                                                                | 10 |
| Figure 2: HDNL and TNFL .....                                                                                                     | 11 |
| Figure 3: What is Q-Day (Y2Q)? .....                                                                                              | 16 |
| Figure 4: Barriers to Cryptographic Agility .....                                                                                 | 20 |
| Figure 5: Time to Q-Day/CRQC vs PQC Transition Timelines .....                                                                    | 28 |
| Figure 6: Illustration of QKD Networks in China .....                                                                             | 31 |
| Figure 7: Timeline of Satellite-Based QKD Launches .....                                                                          | 34 |
| Figure 8: Central Bank of China Clearing QKD Data Nodes .....                                                                     | 34 |
| Figure 9: India's Quantum Thematic Hubs, with Lead and Supporting Institutions .....                                              | 36 |
| Figure 10: South Korea's 2026 First Comprehensive Plan for Promotion of Quantum Science and Technology and Quantum Industry ..... | 52 |
| Figure 11: Yonsei University's 127-Qubit Quantum Computer on campus .....                                                         | 54 |
| Figure 12: South Korea's National QKD Network's Data Centres with 16 Encryption Points Establishing up to 127 Secure Links .....  | 55 |
| Figure 13: South Korea Master Plan for PQC Migration .....                                                                        | 58 |

# Executive Summary

## **Overview**

The CCAPAC Annual Report 2026 assesses the quantum computing security threat and post-quantum cryptography (PQC) readiness across six Asia Pacific markets: Australia, China, India, Japan, Singapore, and South Korea, plus a Taiwan case study. The report concludes that while regional progress is steady, Asia Pacific is still underprepared for the cryptographic transition required before quantum computers render current encryption obsolete.

## **The Quantum Threat**

Quantum computers can efficiently solve the mathematical problems that underpin today's widely deployed asymmetric encryption (RSA, ECC), threatening the confidentiality and authenticity of digital communications, financial transactions, and critical infrastructure. The immediate threat is not quantum computers breaking encryption in real-time, but adversaries executing "Harvest Now, Decrypt Later" (HNDL) attacks: capturing and storing encrypted data today for decryption once quantum capabilities mature. "Trust Now, Forge Later" (TNFL) represents an analogous threat to digital signatures, enabling future forgery of documents and transactions signed today.

## **The Solution: Post-Quantum Cryptography**

In August 2024, the US National Institute of Standards and Technology (NIST) finalised the first post-quantum cryptographic standards: ML-KEM (FIPS 203) for key encapsulation, and ML-DSA (FIPS 204) and SLH-DSA (FIPS 205) for digital signatures. These algorithms are quantum-resistant, run on classical hardware, and can be deployed today. However, PQC migration is not a simple software update, it requires systematic identification, prioritisation, and replacement of cryptographic systems across entire organisations, with implementation timelines spanning years to decades.

## **Asia Pacific Readiness Assessment**

*Uneven Progress:* Singapore and Japan demonstrate advanced readiness, combining strong research foundations, operational quantum-secure deployments, and proactive regulatory engagement. South Korea is advancing rapidly through government mandates and industrial capability. Australia has strategic orientation and could work to translate policy into mandatory compliance requirements. India faces a scale challenge, with 1.4 billion people and emerging quantum infrastructure. China is pursuing a dual QKD+PQC strategy with extensive infrastructure deployment but no mandatory PQC deadline.

*Common Gaps:* Cryptographic inventories are incomplete or non-existent in most organisations, with HNDL and TNFL threats underappreciated at the strategic and operational level. Regulatory mandates alone may not be sufficient to drive necessary migration pace in the region. Small and medium enterprises (SMEs), who are critical to regional supply chains, lack awareness and resources. The skilled workforce required to execute PQC migrations correctly is scarce.

## **Key Challenges Observed**

*Hardware Vulnerabilities:* IoT devices, industrial control systems, and embedded hardware with hard-coded cryptography cannot be patched and must be physically replaced.

*Backward Compatibility:* Organisations cannot migrate in isolation; legacy systems remain dependent on classical cryptography, necessitating hybrid approaches that introduce complexity and cost.

*Performance Overhead:* PQC algorithms require significantly larger keys and signatures than classical counterparts, stressing bandwidth, memory, and processing capacity.

*Standards Fragmentation:* India, South Korea, and China are developing indigenous PQC standards, creating interoperability risks and increasing implementation complexity for multinational organisations.

## **Strategic Recommendations**

*For Organisations:* Conduct comprehensive cryptographic inventories; implement hybrid cryptographic schemes for immediate HNDL protection; establish executive-level oversight; prioritise long-lived, sensitive data; mandate PQC-ready procurement.

*For Governments:* Align domestic standards with NIST globally; establish national PQC pilot programmes; require CII operators to report migration progress; provide SME subsidies; fund workforce development; embed PQC requirements in procurement policy.

## **Conclusion**

Asia Pacific's quantum security transition is underway but appears currently insufficient to meet emerging timelines. The technical standards exist, and what remains is urgent mobilisation of government, enterprise, and infrastructure operators to execute systematic PQC migration before quantum computers emerge. CCAPAC urges organisations and governments that the work to quantum security transition must begin now.



# 01

---

## **Chapter 1 – What is quantum computing, PQC and why the focus now?**

---

## 1.1 What is quantum computing?

**Quantum computing** is a new paradigm of computation that harnesses the principles of quantum mechanics to process information in ways that current classical computers cannot (see table below for a comparison between classical computing and quantum computing). Where a classical computer encodes information in binary bits (i.e., either 0 or 1), a quantum computer uses quantum bits, or qubits, which can exist in simultaneous combinations of both states at once. This allows quantum machines to explore vast solution spaces in parallel, giving them an exponential advantage over classical computers for specific problem types.

Table 1: Classical Computing vs Quantum Computing Comparison

| Feature           | Classical Computing                                                                                                            | Quantum Computing                                                                                                                                                                      |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fundamental Unit  | <b>Bit:</b> The basic unit of information, representing a binary state of either 0 or 1.                                       | <b>Qubit (Quantum Bit):</b> The fundamental unit of information that operates based on quantum mechanics.                                                                              |
| Information State | <b>Binary:</b> A bit exists in a single definite state (0 or 1) at any given time, similar to a light switch being on or off.  | <b>Superposition:</b> A qubit can exist in multiple states (0 and 1) simultaneously until it is observed or measured.                                                                  |
| Processing Power  | <b>Sequential:</b> Processes information linearly. Complex problems with massive variables can take exponential time to solve. | <b>Simultaneous:</b> Can explore massive permutations concurrently. This allows for solving specific complex problems (like drug discovery or optimization) in a fraction of the time. |
| Networking Method | <b>Transport:</b> Transmits digital information by moving bits from one location to another.                                   | <b>Teleportation:</b> Exchanges quantum states using entanglement. Information is "teleported" rather than physically moved, leveraging the link between entangled particles.          |
| Robustness        | <b>Stable:</b> Information is robust and can be measured without changing its state.                                           | <b>Fragile:</b> Quantum states are incredibly fragile. Measuring or observing a qubit causes its superposition to collapse into a classical state (0 or 1).                            |

Source: <https://outshift.cisco.com/blog/quantum/quantum-computing-applications-classical-computing>

---

## 1.2 Opportunities from quantum computing and quantum networking

Quantum computers use qubits to process massive, complex datasets simultaneously by existing in multiple states at once. Quantum networking connects quantum computers/quantum computing devices and uses the concept of entanglement<sup>1</sup> to transmit and share information instantly and securely, rather than the classical transmission of bits. This creates a powerful, unified quantum internet capable of solving global challenges that classical networks cannot handle.

Some industrial applications of quantum computing include (but are not limited to):

- **Pharmaceuticals, drug discovery, and healthcare**<sup>2</sup> - where quantum computers simulate molecular and chemical interactions at a rate and accuracy exponentially faster than classical machines, potentially compressing decades of pharmaceutical R&D into years. This includes modelling protein folding, simulating molecular binding to biological targets, and optimising drug formulations at the atomic level - capabilities historically beyond the reach of classical

---

<sup>1</sup> <https://research.cisco.com/quantum-research/quantum-networks-future>

<sup>2</sup> <https://www.weforum.org/stories/2025/01/quantum-technology-business>

computing. Beyond drug discovery, quantum sensing exponentially improves accuracy of patient diagnostics - ultimately leading to better wellness and healthcare for all, patient outcomes, and materials discovery.

- **Financial modelling, risk management, and portfolio optimisation**<sup>3</sup> - quantum algorithms such as quantum Monte Carlo methods<sup>4</sup> allow for more comprehensive, faster, and more accurate assessments in various financial modelling, such as derivative pricing, portfolio optimisation, and fraud detection, giving early-adopting financial institutions and individuals who have access to quantum tools a significant analytical edge in financial markets.
- **Weather predictions and resilience against extreme climate events**<sup>5</sup> - quantum computers are now being deployed in weather-learning approaches that help to accurately forecast extreme weather events, such as typhoon trajectories, in a resource-efficient way by significantly reducing the number of trainable parameters required.

---

## 1.3 The risks of quantum computing – the security challenge quantum computing poses to traditional encryption schema

Quantum computing poses challenges to traditional encryption techniques that secure existing systems, such as the Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) systems, which rely on complex mathematical problems that quantum computers can readily solve.<sup>6</sup> Addressing this threat has driven the development of a new field of cryptography designed to withstand quantum attacks.

Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to be secure against attacks by both classical and quantum computers. Unlike current encryption methods that quantum computers can break, PQC algorithms are built on mathematical problems believed to resist quantum computation. PQC does not require a quantum computer to implement, as it runs on conventional hardware, and is intended to replace or supplement existing encryption standards before cryptographically relevant quantum computers become operational.

In the context of PQC, knowing the distinction between **symmetric and asymmetric encryption** methods is critical because quantum computers affect them differently. **Cryptographically Relevant Quantum Computers (CRQC)** could plausibly break the encryption that secures nearly all of today's internet traffic, digital signatures, and financial transactions that rely on existing encryption techniques: the significance of this threat to governments is substantial, as encryption underpins classified communications, national identity systems, critical infrastructure such as energy grids and hospitals, and the protection of sensitive citizen data. A breakdown in encryption does not merely expose information; it can undermine public trust in digital services, destabilise financial systems, and create vulnerabilities in national defence. Governments are therefore not peripheral stakeholders in this challenge, but among its most exposed.

---

<sup>3</sup> <https://www.bluequbit.io/blog/quantum-computing-use-cases>

<sup>4</sup> <https://aws.amazon.com/blogs/quantum-computing/quantum-monte-carlo-on-quantum-computers/>

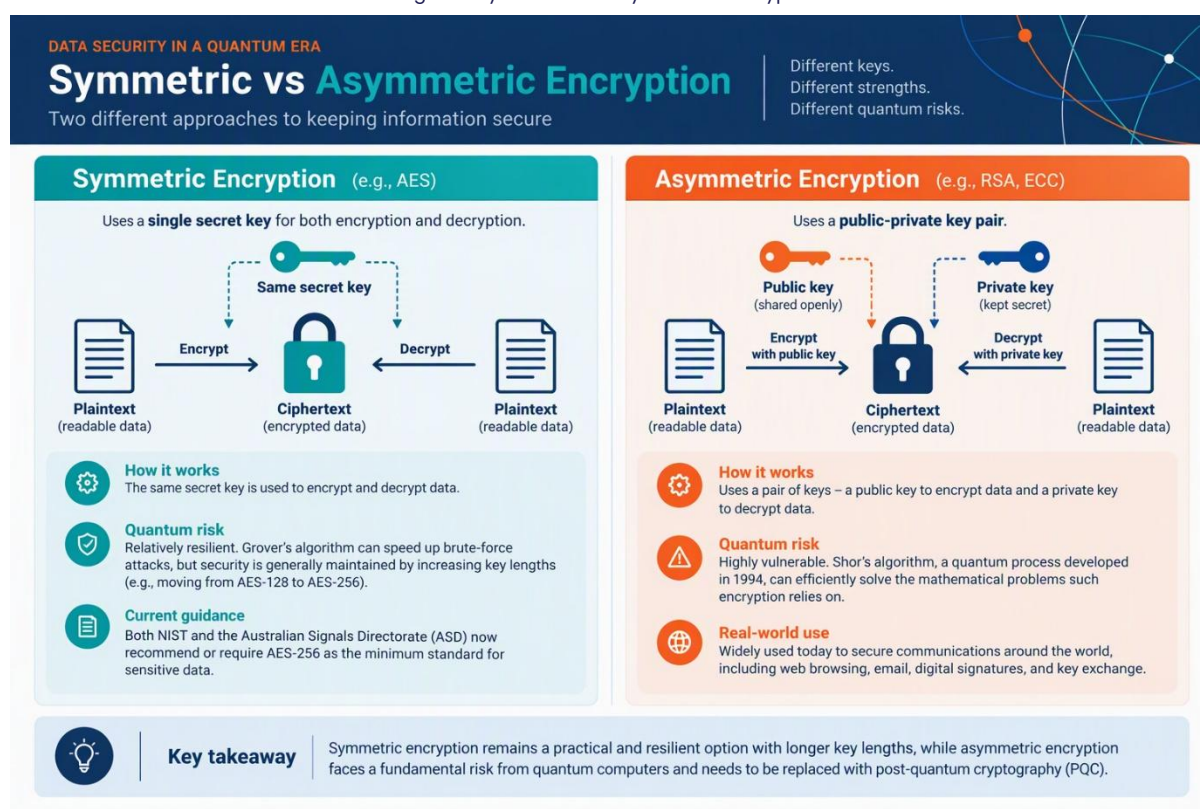
<sup>5</sup> <https://open-quantum-institute.cern/forecasting-extreme-weather-events/>

<sup>6</sup> <https://www.cisco.com/site/us/en/learn/topics/networking/what-is-post-quantum-cryptography.html>

- **Symmetric encryption (e.g., AES)** uses a single secret key for both encryption and decryption. It is relatively resilient to quantum attacks; Grover’s algorithm can speed up brute-force attacks, but security is generally maintained by increasing (e.g., doubling) key lengths (moving from AES-128 to AES-256). This is already reflected in various government guidance - both the US National Institute of Standards and Technology (NIST) and the Australian Signals Directorate (ASD) now recommend or require AES-256 as the minimum standard for sensitive data.<sup>7 8</sup>
- **Asymmetric encryption (e.g., RSA, ECC)** uses public-private key pairs. These are highly vulnerable because Shor’s algorithm<sup>9</sup>, a quantum process developed in 1994, can efficiently solve the mathematical problems such encryption relies on. Asymmetric encryption is widely used to secure communications around the world today.

PQC focuses heavily on replacing existing encryption algorithms with “quantum-resistant” asymmetric primitives-such as lattice-based or hash-based signatures-to secure digital handshakes and identity verification before a quantum adversary can compromise them.

Figure 1: Symmetric vs Asymmetric Encryption



Source: Access Partnership Institute, 2026

<sup>7</sup> [https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-\(evaluation-criteria\)](https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria))

<sup>8</sup> [https://www.cyber.gov.au/sites/default/files/2025-07/22\\_%20ISM%20-%20Guidelines%20for%20cryptography%20\(June%202025\).pdf](https://www.cyber.gov.au/sites/default/files/2025-07/22_%20ISM%20-%20Guidelines%20for%20cryptography%20(June%202025).pdf)

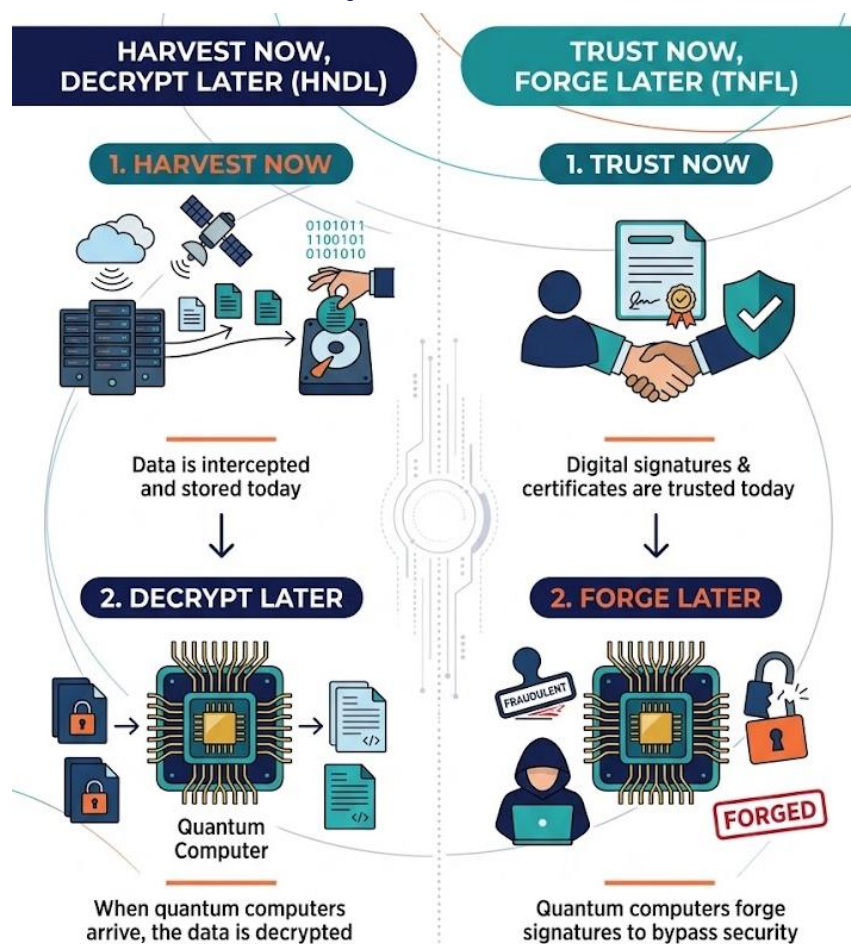
<sup>9</sup> <https://quantum.cloud.ibm.com/docs/en/tutorials/shors-algorithm>

## Strategic Threats to Encrypted Data and Digital Signatures

This leads to new security challenges such as “**Harvest Now, Decrypt Later**” (HNDL), a long-term cyberattack strategy where bad actors capture and store encrypted information today, keeping it for the future where they may be able to break the data encryption and harvest personally identifiable information (PII) or state secrets using quantum computers.<sup>10</sup> It targets long-term sensitive information that remains valuable for years, exploiting the gap between current, vulnerable encryption and future quantum capabilities.

Organisations who have faced HNDL threats should actively conduct analyses on what kind of data has been taken/intercepted, and what the risk and implications are for their organisation should that data be decrypted. Organisations with strict long-term data requirements - such as government bodies holding state secrets and healthcare institutions storing personally identifiable information (PII) - need to prioritise these audits immediately, and use unified quantum risk/resilience models<sup>11</sup> to measure data longevity against future decryption timelines, allowing them to isolate exposed datasets and strategically transition to post-quantum cryptography standards.

Figure 2: HNDL and TNFL



Source: Access Partnership Institute, 2026

<sup>10</sup> <https://ccapac.asia/2026/01/30/harvest-now-decrypt-later-hndl-data-hoarding-and-retention-delayed-impact-of-data-breaches-and-cryptographic-mapping/>,  
<https://www.paloaltonetworks.com/cyberpedia/harvest-now-decrypt-later-hndl>

<sup>11</sup> <https://blogs.cisco.com/security/quantum-resilience-needs-a-common-language>

HNDL has a signature-side counterpart known as “**Trust Now, Forge Later**” (TNFL). Under this long-term attack model, adversaries target signatures generated using today’s asymmetric cryptography, anticipating that a future quantum computer could enable them to forge those signatures. While HNDL threatens the confidentiality of encrypted information, TNFL threatens the integrity and authenticity of digitally signed content. The greatest exposure lies in signatures intended to remain trusted for long periods, such as those protecting firmware, software updates, legal agreements, code-signing certificates, and root certificates.<sup>12</sup>

TNFL could potentially be more disruptive than HNDL. Signature infrastructure is often harder to replace than encryption, the effects of a compromise can propagate across entire ecosystems, and signatures may be verified many years after they were issued. For TNFL threats, the use of post-quantum cryptography on new data will protect it immediately. However, if a signing key is compromised, confidence in everything authenticated with that key may be called into question. Some of these challenges are discussed in the next section on hardware vulnerabilities. To address TNFL, mitigation requires an early transition of signatures to post-quantum cryptography with particular priority given to certificate chains, public-key infrastructure, firmware signing, and code-signing systems rather than focusing solely on bulk-data encryption.

## Hardware Vulnerabilities

Product hardware is particularly vulnerable due to its long lifecycle. Many IoT devices and Industrial Control Systems (ICS) have firmware, public keys, and cryptographic logic hard coded into silicon e.g., secure enclaves or Trusted Platform Modules (TPM).<sup>13</sup> If these systems lack cryptographic agility, they cannot be patched via software and must be physically replaced. Furthermore, PQC algorithms require significantly larger keys and computational power; older hardware may suffer from fatal latency or simply fail to implement the new standards.

---

## 1.4 Is there a future for security after existing encryption schemas collapse? The current state of quantum-resistance – Post-Quantum Cryptography, and resilience planning by governments and the industry

While quantum computers do pose a challenge to existing cryptographic methods, there is much work being done to improve resilience to the threat. On the technical front, work is being done on **Post-Quantum Cryptography (PQC)** to counter this security risk. PQC are mathematical algorithms designed to be resistant against the processing power of both classical computers and CRQCs.

Some key categories of PQC encryption algorithms include:<sup>14</sup>

- **Lattice-based cryptography**<sup>15</sup> - relies on the computational difficulty of finding short vectors in high-dimensional geometric lattices, and forms the basis of NIST’s primary PQC standards, Module-Lattice-Based Key-Encapsulation Mechanism Standard (FIPS 203 ML-KEM)<sup>16</sup> and

---

<sup>12</sup> <https://postquantum.com/quantum-security-reference/what-is-trust-now-forge-later/>

<sup>13</sup> <https://engineering.fb.com/2026/04/16/security/post-quantum-cryptography-migration-at-meta-framework-lessons-and-takeaways/>

<sup>14</sup> <https://www.cisco.com/site/us/en/learn/topics/networking/what-is-post-quantum-cryptography.html>

<sup>15</sup> <https://www.redhat.com/en/blog/post-quantum-cryptography-lattice-based-cryptography>

<sup>16</sup> <https://csrc.nist.gov/pubs/fips/203/final>

Module-Lattice-Based Digital Signature Standard (FIPS 204 ML-DSA).<sup>17</sup> A notable variant, FrodoKEM<sup>18</sup>, offers higher security assurance via unstructured lattices but at significantly greater computational cost.

- **Hash-based signatures**<sup>19</sup> - these derive their security from the collision resistance of cryptographic hash functions, with NIST's Stateless Hash-Based Digital Signature Standard (FIPS 205 SLH-DSA (SPHINCS+))<sup>20</sup> as the standardised scheme.
- **Multivariate quadratic equations**<sup>21</sup> - such equations are behind signature schemes whose security rests on the difficulty of solving large systems of polynomial equations over finite fields.
- **Code-based schemes**<sup>22</sup> - such schemes address the classical problem of decoding a random linear error-correcting code; an example is the Classic McEliece scheme.<sup>23</sup>

Critically, PQC can be implemented on classical computers today, without requiring quantum hardware. This distinguishes PQC from Quantum Key Distribution (QKD), a separate quantum-security approach that relies on dedicated quantum communications infrastructure, rather than on the classical computing hardware that PQC uses. Policy coordination is also underway in various countries to ensure that PQC standards are developed, and cryptographic transitions are being planned and on track.

For example, the United States' National Institute of Standards and Technology (NIST)<sup>24</sup> released its principal PQC standards (Federal Information Processing Standards or FIPS) in August 2024:<sup>25</sup>

- FIPS 203 - Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)
- FIPS 204 - Module-Lattice-Based Digital Signature Standard (ML-DSA)
- FIPS 205 - Stateless Hash-Based Digital Signature Standard (SLH-DSA)
- FIPS 206: FN-DSA (Falcon) - currently in development<sup>26</sup>

A number of countries have also started to establish timelines by which to implement quantum-secure systems, for example:

- **USA** - H.R.7535 - Quantum Computing Cybersecurity Preparedness Act (signed December 2022)<sup>27</sup>, which mandates that federal agencies inventory cryptographic systems vulnerable to future quantum attacks and develop migration plans to PQC, coupled with other supporting legislation like the 2026 US Cyber Strategy (released March 2026), makes PQC a foundation for federal IT procurement. NIST has also detailed<sup>28</sup> how the industry should be deprecating traditional symmetric encryption algorithms using 112 bits of security strength by 2030, and by 2035, NIST recommends disallowing traditional/insecure algorithms completely.<sup>29</sup>
- **EU** - The European Commission's Roadmap for the Transition to Post-Quantum Cryptography (Jun 2025) urges EU Member States to start transitioning to PQC by the end of 2026.<sup>30</sup> At the same

---

<sup>17</sup> <https://csrc.nist.gov/pubs/fips/204/final>

<sup>18</sup> <https://frodokem.org>

<sup>19</sup> <https://blog.cryptographyengineering.com/2018/04/07/hash-based-signatures-an-illustrated-primer/>

<sup>20</sup> <https://csrc.nist.gov/pubs/fips/205/final>

<sup>21</sup> <https://www.cisco.com/site/us/en/learn/topics/networking/what-is-post-quantum-cryptography.html>

<sup>22</sup> <https://ieeexplore.ieee.org/document/8924271>

<sup>23</sup> <https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/pqc-seminars/presentations/18-classic-mceliece-09172024.pdf>

<sup>24</sup> <https://csrc.nist.gov/projects/post-quantum-cryptography>

<sup>25</sup> <https://csrc.nist.gov/projects/post-quantum-cryptography>

<sup>26</sup> <https://csrc.nist.gov/Presentations/2025/fips-206-fn-dsa-falcon>

<sup>27</sup> <https://www.congress.gov/bills/117th-congress/house-bill/7535>

<sup>28</sup> <https://csrc.nist.gov/pubs/sp/800/131/a/r2/final>

<sup>29</sup> [https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547\\_ipd.pdf](https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547_ipd.pdf)

<sup>30</sup> <https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography>

time, the protection of critical infrastructures should be transitioned to PQC as soon as possible, no later than by the end of 2030.”<sup>31</sup> This adds on to an earlier call in Nov 2024 where 18 EU Member States called on industry, critical infrastructure operators, and public bodies to migrate high-risk applications to PQC by the end of 2030.<sup>32</sup>

- The European Cybersecurity Certification Scheme on Common Criteria (EUCC)<sup>33</sup> published the European Cybersecurity Certification Group’s (ECCG’s) Agreed Cryptographic Algorithms v2<sup>34</sup> in April 2025, specifying cryptographic mechanisms which are recognised and accepted by all EU national cybersecurity certification authorities.
- Standards organisations in Europe, e.g., ETSI and ENISA, recommend, whenever possible, the use of symmetric mechanisms with adjusted parameter lengths and the adoption of post-quantum/traditional (PQ/T) hybrid schemes, ensuring protection against potential vulnerabilities in newer post-quantum mechanisms.
- **Australia** has not legislated deadlines for PQC migration so far, but the ASD recommends ceasing the use of traditional asymmetric cryptography by the end of 2030.<sup>35</sup> Australia’s updated Protective Security Policy Framework that sets out the government’s policy across security domains also required approved PQC algorithms to be supported on newly procured cryptographic equipment and software, and for agencies to develop, implement and maintain a PQC transition plan.<sup>36</sup>
- **China** has not yet issued any mandatory timetables for PQC migration.
- **India** is considering a phased PQC migration timeline, as recommended in a recent government report, targeting CII for foundational implementation by 2027, high-priority migration by 2028, full adoption by 2029 and the broader enterprise sector by 2033.
- **Japan** has directed domestic banks to start transitioning to PQC, following the Financial Services Agency (FSA) guidance in May 2025, to counter future quantum threats expected by the mid-2030s.<sup>37</sup>
- **South Korea’s** Ministry of Science and ICT (MSIT) released the PQC Transition Master Plan in Apr 2025, detailing a three-phase roadmap to migrate Korea’s national cryptographic infrastructure to PQC by 2035.<sup>38</sup>
- **Singapore** released formal guidance on migration dates for Critical Information Infrastructure in the Quantum Safe Handbook (Jul 2026). This sets out three milestones, to submit migration plans by 31 March 2027, incorporate quantum-safe considerations into new CII procurements from 1 January 2028, and complete quantum-safe migration for CIIs by 31 December 2031.<sup>39</sup>

<sup>31</sup> <https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography>

<sup>32</sup> [https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/241127\\_PQC-Joint-Statement.html](https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/241127_PQC-Joint-Statement.html)

<sup>33</sup> [https://certification.enisa.europa.eu/document/download/f4657490-9757-4a97-8deb-fd4d6a1358ee\\_en?filename=EUCC\\_guidelines\\_Agreed%20Cryptographic%20Mechanisms%20v2.pdf](https://certification.enisa.europa.eu/document/download/f4657490-9757-4a97-8deb-fd4d6a1358ee_en?filename=EUCC_guidelines_Agreed%20Cryptographic%20Mechanisms%20v2.pdf)

<sup>34</sup> [https://certification.enisa.europa.eu/document/download/a845662b-ae0-484e-9191-890c4cfa7aaa\\_en?filename=ECCG%20Agreed%20Cryptographic%20Mechanisms%20version%202.pdf](https://certification.enisa.europa.eu/document/download/a845662b-ae0-484e-9191-890c4cfa7aaa_en?filename=ECCG%20Agreed%20Cryptographic%20Mechanisms%20version%202.pdf)

<sup>35</sup> <https://www.cyber.gov.au/business-government/secure-design/planning-for-post-quantum-cryptography>

<sup>36</sup> <https://www.protectivesecurity.gov.au/pspf-annual-release>

<sup>37</sup> <https://www.fsa.go.jp/singi/pqc/gijiyousi/20240718.html>

<sup>38</sup> <https://www.msit.go.kr/bbs/view.do?bbsSeqNo=94&nttSeqNo=3185693>

<sup>39</sup> <https://www.csa.gov.sg/resources/publications/quantum-safe-handbook-and-quantum-readiness-index/>

---

## 1.5 PQC, Q-Day, and the Long Lead Time – Why Asia Pacific needs to make resilience preparations now

**Q-Day** is the theoretical point in time when quantum computers will be capable of breaking current encryption standards. While an exact forecast for Q-Day is impossible at present, many actors, including intelligence agencies, standards bodies, and academic researchers, have been revising their estimates in a consistent direction: sooner rather than later. Regardless of when Q-Day arrives, PQC migration will require long lead times, starting in 2026 may be considered “just-in-time” to reach full readiness before Q-Day arrives. Indeed, some estimates for transitioning cryptographic hardware and software are calculating roadmaps by decades.

- For example, the **Canadian Centre for Cyber Security**’s June 2025 Roadmap for the migration to post-quantum cryptography for the Government of Canada estimates a 10-year transition plan (2026-2035) for their federal systems.<sup>40</sup>
- The **United Kingdom’s National Cyber Security Centre** has a similar eight-year estimate from 2028-2035 in their guidance for Timelines for migration to post-quantum cryptography.<sup>41</sup>

As suggested by the government roadmaps, transitioning to PQC is not a simple software update, it requires organisations to inventory every system using cryptography, assess each for quantum vulnerability, update cryptographic libraries, reissue certificates, and validate interoperability across their ecosystem. For large organisations, this can realistically take a decade or more.

Procurement cycles compound this further. Many edge devices, such as IoT sensors, industrial control systems, and network hardware, are procured on cycles of three, five, or ten years and cannot be easily updated once deployed. A device procured today without PQC capabilities may still be operational and vulnerable well into the Q-Day window. Procurement decisions made now carry long-term cryptographic consequences, and organisations that fail to specify PQC-readiness in current contracts risk locking in vulnerability for years to come.

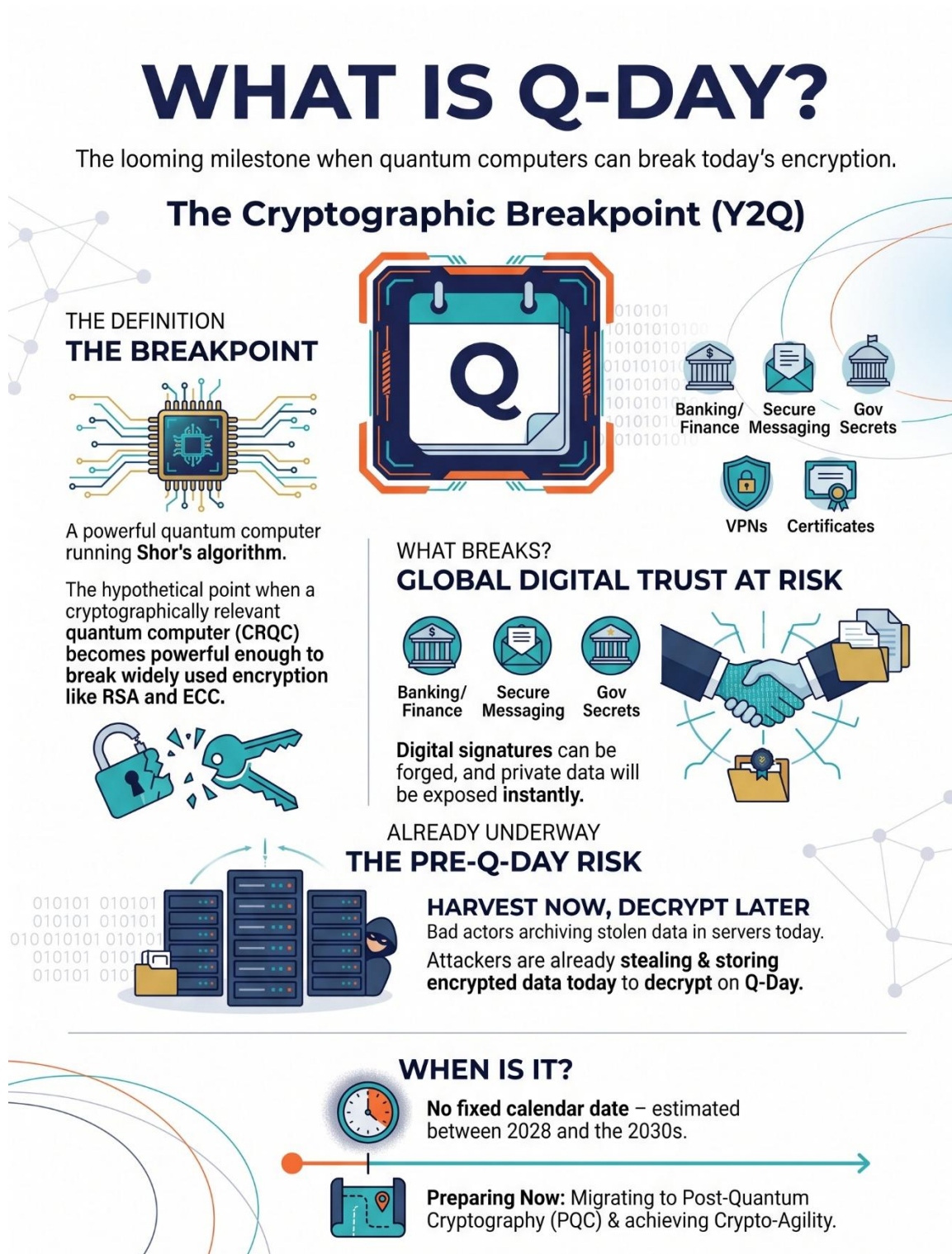
For Asia Pacific markets, there is an opportunity to leapfrog existing technology into quantum computing, converting the cybersecurity risk that quantum computing presents, into deep-rooted trust in the region’s governments and digital systems. Asia Pacific markets can do this by developing strong and transparent PQC transition plans, developing QKD networks with pilots and proof-of-concept tests today, and creating strong use cases for quantum-resilient communication networks with robust digital integrity.

---

<sup>40</sup> <https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001>

<sup>41</sup> <https://www.ncsc.gov.uk/guidance/pqc-migration-timelines>

Figure 3: What is Q-Day (Y2Q)?



Source: Access Partnership Institute, 2026



# 02

---

## **Chapter 2 – Multidimensionality of Challenges and Risks in PQC**

The transition from traditional computing to PQC introduces a unique set of challenges, including decisions around system design, operational resilience, and global interoperability. While moving to PQC makes systems more secure by replacing public-key cryptographic schemes vulnerable to quantum attacks, it also introduces new constraints and challenges related to managing key sizes, performance and computational efficiency, and integration with existing protocols. System designers and policymakers need to balance the complexities of maintaining interoperability between classical and post-quantum systems, as well as ensuring system performance and resource utilisation are factored into transition discussions. In this chapter, some technical, operational, and policy options and challenges associated with transitioning from classical computing to PQC are explored.

---

## 2.1 Making the move to PQC – Understanding and Managing PQC Security and Systems Risks Gaps

**PQC is best understood as a systems risk tied to operational resilience rather than a standalone technical upgrade.** As cryptographic standards underpin core digital functions such as authentication, key exchange, and data integrity, their degradation creates risk across entire systems. Standards bodies typically only mandate transitions when security margins are expected to erode within a defined timeframe. **In that context, policymakers should note that NIST’s decision<sup>42</sup> to deprecate cryptographic systems providing only 112-bit security strength by 2030 and disallow it after 2035 effectively sets a sunset timeline for widely deployed cryptographic baselines.**

As highlighted in the previous chapter, moving to PQC is necessary because public-key cryptographic schemes dependant on mathematical problems that quantum computers are expected to solve efficiently are embedded throughout digital infrastructure, including network protocols and security technology standards that facilitate secure and reliable communication including Transport Layer Security (TLS) and Secure Shell (SSH). By contrast, symmetric key cryptography is considered to be more resilient to quantum attacks and is therefore largely not included in PQC migration efforts except for shorter key lengths, such as 112-bit symmetric standards (e.g., Triple DES).<sup>43</sup>

**Transitioning to PQC is both a lifecycle and supply chain issue.** Classical public-key cryptography is not an isolated software layer that can be easily replaced; it is integrated into hardware, firmware, software libraries, and operational processes, particularly in legacy and embedded systems. Migration is most practical when aligned with existing refresh cycles, procurement decisions, and end-of-life timelines. Large-scale, out-of-cycle replacement efforts are more likely to introduce operational disruption and unnecessary cost. Regardless, organisations at any stage should develop and maintain an **asset inventory** of their entire tech stack with special consideration for legacy components that may delay or outright prevent their migration to PQC.<sup>44</sup>

---

<sup>42</sup> <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

<sup>43</sup> <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

<sup>44</sup> For an example of how to factor PQC into an organisation’s cybersecurity policies, see <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.48.ipd.pdf>

---

## 2.2 Assessing and Managing Cryptographic Agility Gaps

**Cryptographic agility (“crypto agility”)** refers to the ability to upgrade cryptographic systems and retire vulnerable or outdated ones with minimal operational disruptions.<sup>45</sup> While a variety of post-quantum (PQ) algorithms have already been developed, standardised, and made available to implementers, the process of deployment and implementation challenges associated with upgrading cryptographic systems in general could take years to accomplish. This has historically been the case for major migrations to new encryption standards - e.g., the transition of US federal systems from the Triple Data Encryption Standard (Triple DES) to the more secure Advanced Encryption Standard (AES) took 23 years to complete.<sup>46</sup>

Reflecting the difficulty associated with systematically rooting out legacy cryptographic algorithms, most governments across Asia Pacific with mature cryptography policies instead require or recommend more advanced encryption standards be incorporated into new systems moving forward.<sup>47</sup>

The lack of crypto agility can overall be attributed to the fact that decisions around cryptography have often been made without future transitions in mind. Considering the heightened uncertainty around quantum computers and what they will be capable of in the next five to ten years, ensuring crypto agility during the transition to PQC will be crucial for future-proofing systems as the threat landscape evolves.

Examples of barriers to crypto agility include:

- **Larger data sizes:** Most PQ algorithms have larger-sized public keys, signatures, and key-encapsulation ciphertext than their classical counterparts. Whereas an RSA key size of 3072 bits is needed to yield 128 bits of classical security strength, the quantum-resistant ML-DSA needs a 19,360-bit-sized key to achieve roughly the same outcome. While future cryptography research may yield greater efficiencies, anticipating the need to accommodate larger cryptographic data sizes for PQC is most conducive to crypto agility.
- **Backward compatibility and Interoperability:** Even if systems are successfully transitioned to PQC, they cannot be deployed in isolation from the existing cryptographic ecosystem. From both a security and commercial perspective, organisations will be more reluctant to migrate their systems to PQC if doing so compromises their ability to interact with the vast majority of other components that are still dependent on classical cryptographic algorithms. Ensuring backwards compatibility and interoperability therefore reduces the risk of service outages, preserves trust in digital communications, and enables a phased migration aligned with system lifecycles rather than requiring disruptive, system-wide replacements.
- **Hardware:** Crypto agility challenges extend beyond the digital realm to hardware and physical infrastructure as well. Certain assets may be secured by physical components including hardware security modules (HSMs) which, in certain cases, must likewise be physically removed and replaced to accommodate PQ algorithms. Upgrading physical components can be especially challenging if they are deployed in hard-to-reach areas, such as assets launched into space or IoT

---

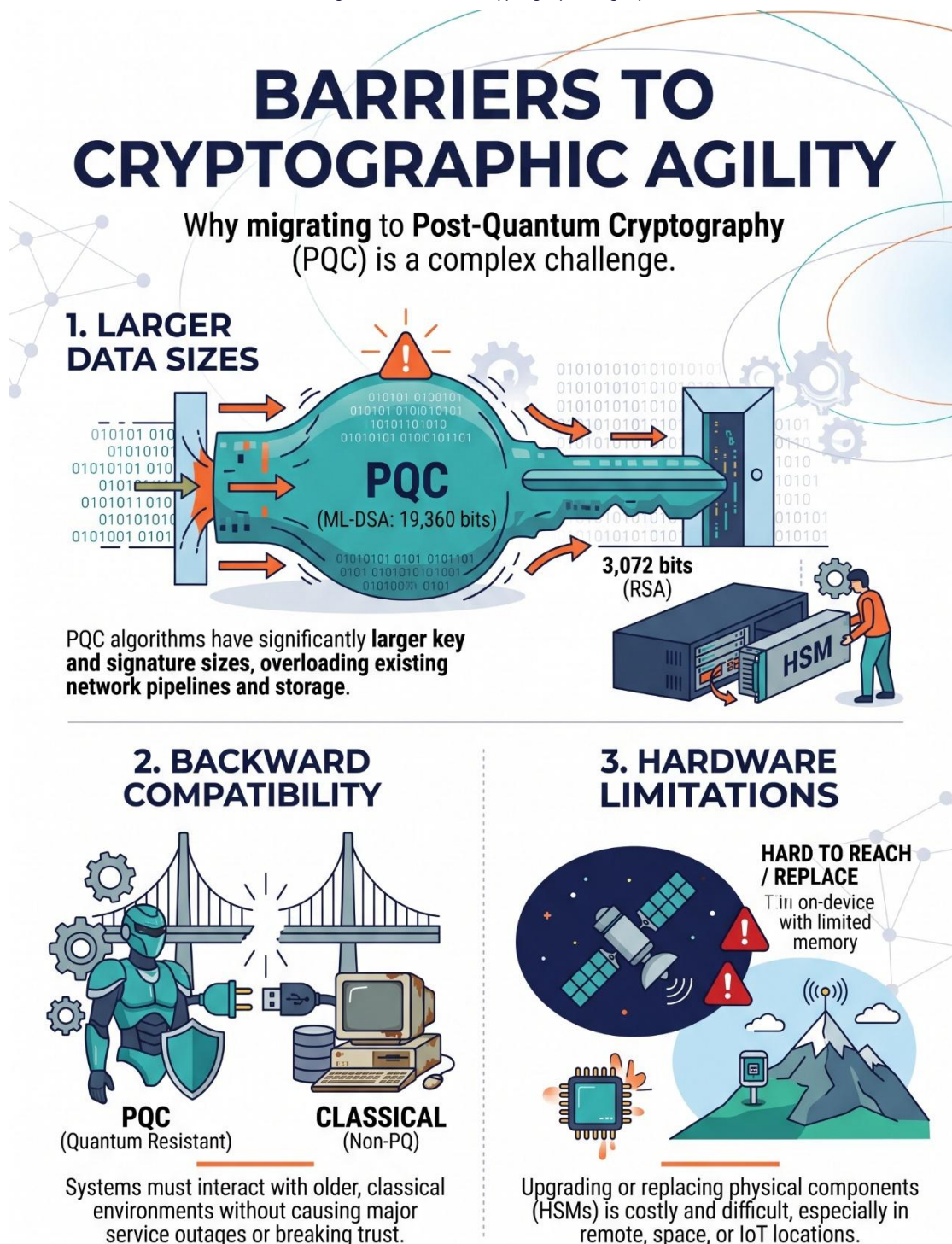
<sup>45</sup> <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST-CSWP-39.pdf>

<sup>46</sup> <https://www.cryptomathic.com/blog/3des-is-officially-being-retired>

<sup>47</sup> For example, Australia's Guidelines for Cryptography provides that AES is the only approved symmetric cryptographic algorithm. <https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cyber-security-guidelines/guidelines-for-cryptography> In Japan, the CRYPTREC e-Government Recommended Ciphers List includes AES while Triple DES is relegated to its Monitored Ciphers List, which is functionally equivalent to NIST's "deprecated" status. <https://www.cryptrec.go.jp/en/list.html>

sensors deployed in especially remote locations.<sup>48</sup> Some products may also have limited capacity to implement multiple algorithms on-device.<sup>49</sup>

Figure 4: Barriers to Cryptographic Agility



Source: Access Partnership Institute, 2026

<sup>48</sup> <https://ieeexplore.ieee.org/document/11171230>

<sup>49</sup> <https://ieeexplore.ieee.org/document/11059928>

---

## 2.3 Balancing Computing Performance and Cost

Performance challenges and cost of using the PQC are the next challenges associated with the move to PQC. As mentioned in the previous section, quantum-resistant algorithms generally have significantly larger public keys, signatures, and ciphertexts than their classical counterparts.<sup>50</sup> This causes PQ algorithms to place pressure on bandwidth, memory, and processing constraints, particularly in environments that were not designed with this overhead in mind. In the worst case, legacy protocols and infrastructure may not be able to handle the increased resource demands at all and must be replaced.

Due to these trade-offs, standards development organisations (SDOs) often consider an algorithm's performance as equally important to its security strength, if not more so. For example:

- In the fourth round of NIST's PQC standardisation process, the Classic McEliece algorithm was ultimately not selected as it had a larger public-key size and slower key generation relative to other candidates, which ultimately made it less attractive for adoption, despite its impressive security track record.<sup>51</sup>

Performance characteristics between algorithms can vary meaningfully depending on deployment contexts as well. For example:

- NIST reflected in its evaluation of PQ Key Encapsulation Mechanisms (KEMs) that the **Hamming Quasi-Cyclic (HQC) KEM** performed best in good network conditions, while the **Bit-Flipping Key Encapsulation (BIKE KEM)** outperformed HQC when network conditions are sufficiently bad.<sup>52</sup>

These examples demonstrate the variability of reviewing PQC algorithms and underscore that there is no single “best” algorithm across all use cases. PQC implementation decisions will need to account for operational context before final decisions are made.

---

## 2.4 Migration Challenges – Hybrid Phase Benefits and Vulnerabilities

*Benefits of a Hybrid Phase.* To aid the transition from traditional cryptography to PQC, hybrid schemes have been proposed, tested, and developed as a means of accelerating the migration process. **Hybrid schemes include hybrid signature algorithms as well as hybrid key-establishment algorithms.** If implemented properly, a hybrid scheme remains secure so long as at least one component (i.e., the traditional or quantum-resistant algorithm) is not compromised.

Existing NIST digital signature standards and guidelines accommodate the generic use of hybrid (dual) signatures. SP 800-56C also allows a generic composite key-establishment technique, and NIST formally announced plans to revise to better accommodate PQ key establishment standards like FIPS 203 in January 2026.<sup>53</sup>

Adopting a hybrid signature algorithm or hybrid key-establishment algorithm provides several benefits.

---

<sup>50</sup> <https://doi.org/10.3390/cryptography9020032>

<sup>51</sup> <https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8545.pdf>

<sup>52</sup> <https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8545.pdf>

<sup>53</sup> <https://csrc.nist.gov/News/2026/nist-to-revise-key-establishment-recommendations>

- Hybrid schemes can **mitigate backward compatibility and interoperability concerns** by allowing legacy systems that do not support PQC to continue establishing secure connections using classical algorithms while newer systems take advantage of the post-quantum component.
- This has the added benefit of **reducing the risk of service interruptions** by using the classical algorithm as a backstop in case interoperability issues arise.

In this way, hybrid schemes offer a **degree of flexibility for governments and organisations to pilot PQC implementation, analyse performance impacts and potential supply chain issues, and make necessary changes while reducing risks of operational disruptions.**

Hybrid schemes will likely prove more attractive to organisations weighing the costs of transitioning to quantum-resistant cryptosystems, particularly considering the uncertainties around when exactly cryptographically relevant quantum computers will render prevailing classical public-key algorithms insecure, as well as how the state-of-the-art for PQC will evolve leading up to and after “Q-Day” occurs.

*Risks and Challenges.* Hybrid algorithms conversely also introduce unique risks and challenges to decision-makers. Classical-PQ hybrid solutions are necessarily **more complex than standalone classical algorithms, which can raise costs and introduce new security risks and vulnerabilities during and after implementation.** For example:

- Incorporating multiple algorithms adds an additional choice in protocols, increasing their attack surface by potentially allowing attackers to carry out “downgrade attacks” and other intrusion methods.<sup>54</sup>
- Transitioning to a hybrid signature algorithm may also require a second transition if the classical component is rendered insecure by future cryptographic advancements.

Hybrid solutions will inevitably **introduce additional costs for implementers.** In addition to requiring **personnel** with specialised knowledge on deploying and maintaining hybrid algorithms, **issuing certificates** using a hybrid signature algorithm (either as a single certificate containing two public keys or by issuing two separate certificates) **adds to operational expenses** that would not otherwise be incurred while implementing either the classical or PQ algorithm alone.

While hybrid algorithms will play an important role in the short-term by expediting the transition process, especially in the face of exigent threats posed such as HNDL attacks, **for decision-makers and policymakers, hybrid solutions only should be viewed as temporary measures on the way towards a full transition to PQC.**

---

<sup>54</sup> A downgrade attack is a form of cryptographic attack in which an adversary manipulates a communication exchange to force both parties to use an older, weaker encryption standard than they are capable of supporting - effectively “downgrading” the security of the connection to one the attacker can more readily compromise.

---

## 2.5 Decisions for Standards – International Interoperability and Standards Asymmetries

Internationally recognised harmonised standards for PQC reduce fragmentation and enable interoperable, scalable deployment across global digital infrastructure. Common standards ensure that systems, devices, and networks in different jurisdictions can securely communicate without requiring bespoke implementations, which lowers integration costs and limits the risk of incompatibilities. They also provide regulatory clarity for industry by aligning procurement, certification, and compliance expectations, allowing vendors to develop once and deploy across multiple markets. From a security perspective, convergence around well-vetted algorithms concentrates scrutiny and testing on a smaller set of implementations, improving assurance and reducing the likelihood of weak or unproven schemes entering critical systems.

As of July 2026, at least 16 countries have added PQC algorithms in government documents, including seven countries in Asia Pacific: Australia, China, India, Japan, New Zealand, Singapore, and South Korea.<sup>55</sup> While many of these countries as well as SDOs like ISO, IETF, and ETSI have pursued their own independent standardisation processes, most have coalesced around algorithms selected or considered by NIST as part of its PQC standardisation process. These processes engage multiple stakeholders from the public and private sectors, heavily emphasising ML-KEM (FIPS 203) for key encapsulation and ML-DSA (FIPS 204) for digital signatures. PQC standardisation across NIST, IETF, IEEE, and the Wi-Fi Alliance, such as in quantum-resistant IKEv2, LMS, SPHINCS+/SLH-DSA, and Wi-Fi PQC certification, are led by private sector companies such as CCAPAC member Cisco Systems.

In Asia Pacific, there are a few markets that are exceptions to this trend.

- In 2021, **South Korea** launched its own KpqC competition, ultimately selecting KEMs NTRU+ and SMAUG-T and signatures AIMer and HAETAE in 2025 after several rounds.
- Earlier, the **Chinese** Association for Cryptographic Research held a PQC standards competition between 2019 and 2020 that reportedly yielded finalists including the lattice-based KEM LAC and signature algorithm Aigis.<sup>56</sup> In February 2025, however, China's Institute of Commercial Cryptography Standards (ICCS), within the State Cryptography Administration, issued a global call for PQ algorithms under a new Next-generation Commercial Cryptographic Algorithms Program (NGCC).<sup>57</sup> Experts have projected that China will potentially finalise its national algorithms by 2029.<sup>58</sup>
- **India's** Telecommunications Engineering Centre (TEC), operating under the Department of Telecommunications, has issued guidance recommending PQC adoption aligned broadly with NIST standards, while signalling India's intent to develop domestic PQC standards suited to its national telecommunications infrastructure.<sup>59</sup>

The implications of these decisions to pursue independent PQC standardisation are complex. On the one hand, a greater variety of thoroughly vetted PQ algorithms based on different mathematical assumptions increases global resilience should a vulnerability be identified in one of them.

---

<sup>55</sup> <https://pqcc.org/international-pqc-requirements/>

<sup>56</sup> <https://postquantum.com/post-quantum/sovereignty-quantum-pqc/#china-pursuing-independent-post-quantum-standards>

<sup>57</sup> <https://www.niccs.org.cn/en/>

<sup>58</sup> <https://www.reuters.com/world/asia-pacific/china-likely-have-standards-post-quantum-cryptography-3-years-expert-says-2026-03-19/>

<sup>59</sup> [https://dst.gov.in/sites/default/files/Report\\_TaskForce\\_PQMmigration\\_4Feb26%20\(v1\).pdf](https://dst.gov.in/sites/default/files/Report_TaskForce_PQMmigration_4Feb26%20(v1).pdf)

Developing national standards also reflects broader digital sovereignty debates and concerns that the PQC standardisation process is too concentrated in US and European bodies.<sup>60</sup>

On the other hand, a fragmented PQC standards landscape increases implementation complexity, raises costs, and creates potential points of failure where systems must bridge incompatible standards. Where systems operating under different national standards must communicate securely, such as across borders or between allied agencies, operators must negotiate common standards, implement costly translation layers, or accept degraded security. For critical infrastructure operators, this further complicates vendor selection and certification, potentially forcing parallel cryptographic environments with separate governance requirements. Perhaps most critically, uneven PQC adoption creates asymmetric vulnerability windows that adversaries could exploit, given a globally connected system but only as secure as its least-protected node.

---

<sup>60</sup> <https://postquantum.com/post-quantum/sovereignty-quantum-pqc/#south-korea-a-parallel-pqc-standardization-effort>



# 03

---

## **Chapter 3 – PQC Policy and Regulatory Readiness in Asia Pacific: Australia, China, India, Japan, Singapore, and South Korea**

This chapter reviews the PQC policy for several Asia Pacific markets, reviewing the existing state of quantum R&D and investment, PQC regulations and roadmaps, specific transitions and involvement of critical infrastructure/critical information infrastructure (CII), and details any dates declared for operational readiness or deadlines for implementation.

---

## Australia

### Existing quantum R&D and investment

*Government policy.* On the national policy front, the **Australia National Quantum Strategy** released 3 May 2023<sup>61</sup> details the long-term vision for how Australia will take advantage of the opportunities of quantum technologies. Five themes run through this document:

- Theme 1: Thriving research and development, investment in and use of quantum technologies
- Theme 2: Securing access to essential quantum infrastructure and materials
- Theme 3: A skilled and growing quantum workforce
- Theme 4: Standards and frameworks that support national interests
- Theme 5: A trusted, ethical and inclusive quantum ecosystem

As part of this strategy, there is a AUD 15 billion (USD 10.5 billion) National Reconstruction Fund earmarked to grow a pipeline of quantum companies and technologies for potential future investment, which has a minimum of AUD 1 billion (USD 0.75 billion) earmarked for investment in critical technologies.<sup>62</sup>

*Public Private Partnerships.* Other investments can also be seen on the public-private collaboration front. For example, the Commonwealth and Queensland Governments will together invest almost AUD 1 billion (USD 0.75 billion) between 2023-2028 in private company PsiQuantum in a joint project to build a Fault-Tolerant Quantum Computer (FTQC).<sup>63</sup>

### PQC regulations and requirements and roadmaps

Australia's approach to PQC readiness and regulation is characterised by a guidance-first, mandate-later framework, allowing government entities to prepare for emerging cryptographic risks before large scale quantum computing capabilities become operational. There are multiple agencies involved in executing this approach.

The **Department of Home Affairs (DHA)** provides overarching policy direction through its protective security, technology and data security responsibilities, and sets the policy and strategy direction.<sup>64</sup> Key mechanisms include the Protective Security Policy Framework (PSPF) for Commonwealth government entities and the Security of Critical Infrastructure Act (SOCIA) for the 11 critical infrastructure sectors.

- The PSPF Release 2026<sup>65</sup> mandates enhanced security for emerging technologies, such as quantum computing. It requires entities to adopt PQC, manage supply chain risks, and align with ASD standards for protecting sensitive data. The PSPF sits within a broader legislative governance structure: the *Public Governance, Performance and Accountability (PGPA) Act 2023* establishes the overarching accountability framework for Commonwealth entities,<sup>66</sup>

---

<sup>61</sup> <https://www.industry.gov.au/publications/national-quantum-strategy>

<sup>62</sup> <https://www.nrf.gov.au/news-and-media-releases/national-reconstruction-fund-bolsters-australias-quantum-computing-and-atomic-scale-semiconductor-manufacturing-capability-20-million-investment-silicon-quantum-computing>

<sup>63</sup> <https://treasury.gov.au/sites/default/files/2024-07/foi-3641.pdf>

<sup>64</sup> <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/technology-and-data-security>

<sup>65</sup> <https://www.protectivesecurity.gov.au/pspf-annual-release>

<sup>66</sup> <https://www.legislation.gov.au/C2013A00123/latest/text>

while the PSPF provides the specific security standards entities must implement to fulfil their duty of managing organisational risk and protecting government resources.

Specifically, the PSPF 2026 requirement 0212 mandates newly procured cryptographic equipment and software to support approved post-quantum cryptographic algorithms in accordance with the Information Security Manual's guidelines for cryptography.<sup>67</sup> PSPF Release 2026 Requirement 0223 also requires entities to develop, implement and maintain a post-quantum cryptography transition plan to support migration away from traditional asymmetric cryptography before quantum computing capabilities create unacceptable risks to government information.

Home Affairs also considers quantum in the context of Australia's development as part of its Technology Foreign Interference Taskforce,<sup>68</sup> raising awareness of and identifying bad-faith actors and investors in high-impact industries such as quantum computing.<sup>69</sup>

The **Australian Signals Directorate (ASD) and their Australian Cyber Security Centre (ACSC)** issue the expert technical advice and control frameworks. In this capacity, the ACSC has focused on awareness raising, guidance publication, and encouraging voluntary early adoption.

The ACSC has issued guidance on post-quantum cryptography through its **Information Security Manual (ISM)**.<sup>70</sup> The ISM (last updated in Jun 2026) is not a quantum-specific document but rather sets cybersecurity standards for Australian government agencies and provides a framework that other organisations can apply. The ISM does highlight cryptographic agility as a key protection principle for system planning, addresses the need for a cryptographic bill of materials, identifies which PQC algorithms ASD supports for use, and provides guidance for transitioning to PQC (including hybrid schemes).

They have also released various explainers and guidance in their Quantum Technology series<sup>71</sup>, with estimations of Q-Day vis-à-vis organisations planning their PQC transition timeline. The series includes:

- Planning for post-quantum cryptography
- Quantum technology primer: Overview
- Quantum technology primer: Computing
- Quantum technology primer: Communication
- Quantum technology primer: Sensing

---

<sup>67</sup> <https://www.protectivesecurity.gov.au/pspf-annual-release>

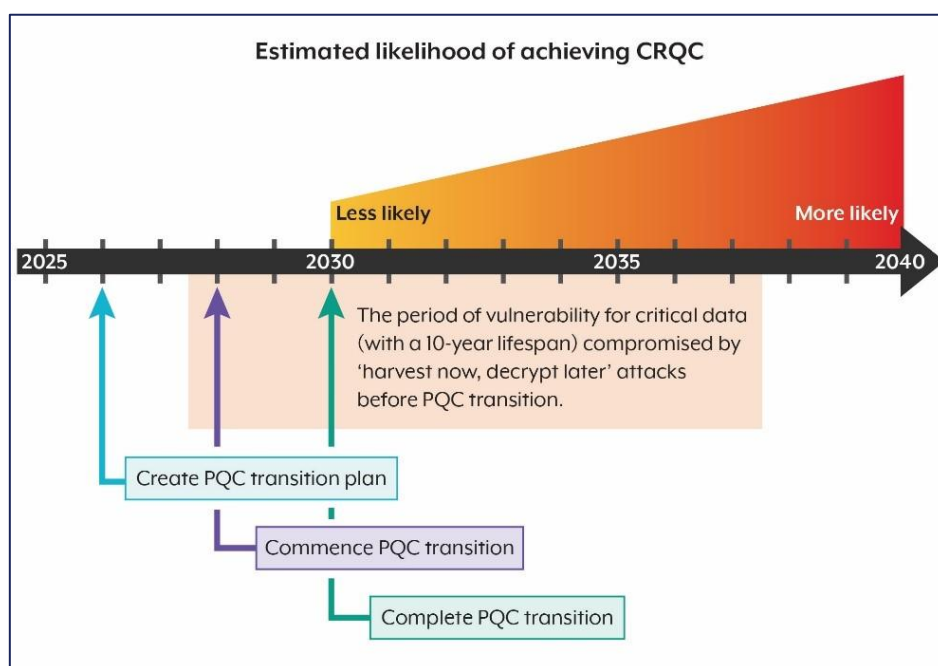
<sup>68</sup> <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/technology-and-data-security/technology-foreign-interference-taskforce>

<sup>69</sup> <https://www.homeaffairs.gov.au/nat-security/files/info-sheet-bad-faith-investors.pdf>

<sup>70</sup> <https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism>

<sup>71</sup> <https://www.cyber.gov.au/business-government/secure-design/quantum>

Figure 5: Time to Q-Day/CRQC vs PQC Transition Timelines



Source: <https://www.cyber.gov.au/business-government/secure-design/quantum/planning-for-post-quantum-cryptography>

Critical Infrastructure sector regulators, for example the **Australian Prudential Regulation Authority (APRA)**, and the Australian Securities and Investments Commission (ASIC) for the financial services sector, issue guidance and also enforce compliance under sector specific legislation.

- APRA has a key Prudential Standard CPS 234 Information Security; however, this does not (yet) have any PQC-specific guidance. Similarly, ASIC does not appear to (yet) have any PQC-specific advice, but from their Oct 2025 Market Integrity Update (MIU), appears to be appraised of the threat and has advised the industry to “act now to protect your systems: Transitioning to post-quantum cryptography”.<sup>72</sup>

Where a critical infrastructure sector does not have a sector regulator, the DHA undertakes this function.

## Critical Information Infrastructure (CII) Considerations

Critical (Information) Infrastructure is governed under Australia’s Security of Critical Infrastructure Act 2018 (SOCI Act).<sup>73</sup> Owners/operators of CII must also comply with the Critical Infrastructure Risk Management Program (CIRMP) (released Feb 2023).<sup>74</sup> The programme provides a framework for managing risks to critical infrastructure across eleven sectors: communications, data storage and processing, defence industry, education and research, energy, financial services, food and grocery, health, space, transport, and water and sewerage. The SOCI Act framework includes mandatory cyber incident reporting, risk management obligations, and government assistance powers.

While the frameworks today do not yet include specific PQC preparation or migration requirements, the need to be quantum-ready would be a risk that falls within the broader scope of developing a risk management approach. Proposed amendments to the CIRMP rules will allow the department to

<sup>72</sup> <https://www.asic.gov.au/about-asic/corporate-publications/newsletters/market-integrity-update/miu-issue-172-october-2025/>

<sup>73</sup> <https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018>

<sup>74</sup> <https://oia.pmc.gov.au/published-impact-analyses-and-reports/critical-infrastructure-risk-management-program>

declare specific “material risks” (such as quantum computing) which then must be considered by operators of CII. It is foreseeable that the QC risk to cryptography will be declared a material risk in the future.<sup>75</sup>

## Operational readiness/ deadlines for implementation

Australia does not yet have legislated deadlines for PQC migration but rather has guidance documents and frameworks that recommend planning for PQC migration and starting cryptographic dependency inventories. For example, the ASD ISM will no longer approve the use traditional asymmetric cryptography algorithms beyond the end of 2030.<sup>76</sup>

Commonwealth entities subject to the ISM will need to exception manage non-PQC beyond this timeframe. Similar exception-based risk management can be expected of CII organisations under SOCI. When the point of quantum computing threats to traditional cryptography is actually realised, the ability to risk manage the lack of PQC will become increasingly difficult and expensive.

## Quantum in Australia: Summary

### Opportunities

- AUD 15 billion (USD 10.5bn) National Reconstruction Fund, with a minimum AUD 1bn ring-fenced for critical technologies including quantum.
- A "guidance-first, mandate-later" regulatory posture gives industry a genuine head start to prepare before compliance becomes mandatory.
- Detailed technical support already flowing from ASD/ACSC in the form of the Information Security Manual and Quantum Technology explainer series, helping organisations plan crypto-agility and PQC transition timelines.
- National Quantum Strategy's five themes (R&D, infrastructure, workforce, standards, trusted ecosystem) provide a coordinated, whole-of-government growth platform.

### Risks

- No legislated PQC migration deadline yet exists, creating a risk of under-preparation despite growing threat awareness.
- ASD's ISM will stop approving traditional asymmetric cryptography after 2030, which represents a hard technical cliff-edge for Commonwealth entities and CII operators, which could leave unprepared systems out of compliance; as Q-Day approaches, exception-managing non-PQC systems will become progressively harder and more costly.
- Sector regulators APRA and ASIC have not yet issued PQC-specific guidance, leaving financial services without clear compliance direction.
- Reliance on voluntary/guidance-based adoption risks uneven readiness across sectors and organisation sizes; for example, quantum risk is not yet formally designated a "material risk" under CIRMP, which could delay CII operator action.

---

<sup>75</sup> <https://www.cisc.gov.au/legislation-regulation-and-compliance/consultation-on-enhancements-to-cirmp-rules>

<sup>76</sup> <https://www.cyber.gov.au/business-government/secure-design/planning-for-post-quantum-cryptography>

---

## China

### Existing quantum R&D and investment

*Funding.* China has one of the most heavily funded quantum technology ecosystems globally, with public investment in quantum science and industrialisation estimated at USD 15 billion across national and provincial programs.<sup>77</sup> Advanced technologies such as quantum computing are embedded in national industrial policy frameworks including the 15<sup>th</sup> Five-Year Plan (十五五计划) (2026-2030), which designates quantum communications and quantum computing as national strategic priority technology.<sup>78</sup> Additional support has been provided through national science programmes such as the National Key Research and Development Program (国家重点研发计划) and through the creation of the National Laboratory for Quantum Information Sciences (量子信息科学国家实验室).<sup>79</sup>

*R&D/Academia.* China's quantum research ecosystem is anchored by the Chinese Academy of Sciences (CAS) Centre for Excellence in Quantum Information and Quantum Physics (中国科学院量子信息与量子科技创新研究院), which have led many of the country's quantum experiments.<sup>80</sup> It is affiliated with the University of Science and Technology of China (USTC, 中国科学技术大学), a public university founded and governed by CAS.

*Industry/Commercial.* Commercial actors are also emerging, including Origin Quantum (本源量子) and QuantumCTek (科大国盾).<sup>81</sup> Origin Quantum operates cloud accessible superconducting quantum computing systems, including the Origin Wukong (本源悟空), China's first domestically developed third-generation superconducting quantum computer, released in 2024.<sup>82</sup>

*Public-Private-Academia Partnerships.* In many instances, partnerships between the industry, public sector, and academic institutions drive R&D into quantum computing, including USTC, Shanghai Quantum Science Research Center (上海量子科学研究中心), Anhui Quantum Computing Engineering Research Center (安徽省量子计算工程研究中心), China Telecom Quantum Group (中国电信量子集团), Origin Quantum, QuantumCTek, Tsinghua University (清华大学), Peking University (北京大学).<sup>83</sup> These collaborations have enabled strong progress in quantum computer and compute capacities for the country, for example:

- Zuchongzhi 祖冲之<sup>84</sup> released in 2021 with 62 qubits, progressed to Zuchongzhi 3.2 in 2025 with 107 qubits;
- Origin Quantum's<sup>85</sup> Origin Wukong (本源悟空), China's third generation domestically developed superconducting quantum computer, equipped with a 72-qubit quantum chip, officially went online in 2024;
- Tianyan-504 (天衍-504), released in 2024, supports 504 qubits<sup>86</sup>.

---

<sup>77</sup> <https://merics.org/en/report/chinas-long-view-quantum-tech-has-us-and-eu-playing-catch>

<sup>78</sup> <https://english.cas.ac.cn/knowledge/article/china-quantum-computing-strategy/>. The previous 14<sup>th</sup> 5-year plan also highlighted quantum computing as a strategic frontier technology for the country [https://www.gov.cn/xinwen/2021-03/13/content\\_5592681.htm](https://www.gov.cn/xinwen/2021-03/13/content_5592681.htm)

<sup>79</sup> <https://www.ustc.edu.cn/info/1362/24050.htm>; <http://lqcc.ustc.edu.cn/about.html>

<sup>80</sup> <https://www.quantumcas.ac.cn/main.htm>

<sup>81</sup> <https://originqc.com.cn/>; <https://www.quantum-info.com/index.html>

<sup>82</sup> <https://www.news.cn/jiangzi/20260310/7a513191b5da47f4b3c563c7370087c1/c.html>

<sup>83</sup> <https://www.csis.org/analysis/understanding-chinas-quest-quantum-advancement>

<sup>84</sup> <https://news.ustc.edu.cn/info/1056/93566.htm>

<sup>85</sup> <https://eu.36kr.com/en/p/3474408032131719>

<sup>86</sup> <https://inspenet.com/en/news/tianyan-504-chinas-quantum-computer-surpasses-500-qubits/>

*Quantum Networks.* China's most distinctive achievement in quantum technology is the large-scale deployment of QKD infrastructure. The Beijing-Shanghai Quantum Communication Backbone (BSBN, 京沪干线), completed in 2017, created a 2000-kilometer QKD network linking Beijing and Shanghai through 32 trusted relay nodes.<sup>87</sup> This terrestrial network established a satellite-to-ground link with the Micius (墨子号) satellite, enabling the world's first integrated satellite ground quantum communication system (天地一体化广域量子通信网络).<sup>88</sup>

In February 2026, researchers from Peking University constructed Weiming Quantum Chip Network (未名量子芯网), the world's first large-scale QKD network based on integrated optical quantum chips. The network supports parallel communication among 20 chip users, achieves a single-link communication distance of 370 kilometres, and has a total parallel coverage distance of 3,700 kilometres.

Figure 6: Illustration of QKD Networks in China



Source: CAS Quantum Network Co<sup>89</sup>

## PQC regulations and requirements and roadmaps

China's cryptographic governance is led by the State Cryptography Administration (SCA, 国家密码管理局) under the State Council (国务院) and Central Military Commission (CMC, 中央军委).<sup>90</sup> The legal foundation for China's cryptography system is the Cryptography Law (密码法) which took effect 1 Jan 2020.<sup>91</sup> It established mandatory requirements for the use of approved cryptographic products in

<sup>87</sup> <https://www.cnsa.gov.cn/n6758824/n6759219/c6797164/content.html>

<sup>88</sup> <https://quantum.ustc.edu.cn/web/node/472>

<sup>89</sup> [https://docbox.etsi.org/Workshop/2023/02\\_QUANTUMSAFECRYPTOGRAPHY/TECHNICALTRACK/WORLDTOUR/CASQUANTUMNETWORK\\_QI.pdf](https://docbox.etsi.org/Workshop/2023/02_QUANTUMSAFECRYPTOGRAPHY/TECHNICALTRACK/WORLDTOUR/CASQUANTUMNETWORK_QI.pdf)

<sup>90</sup> <https://www.oscca.gov.cn/>

<sup>91</sup> [http://www.npc.gov.cn/englishnpc/c2759/c23934/202009/t20200929\\_384279.html](http://www.npc.gov.cn/englishnpc/c2759/c23934/202009/t20200929_384279.html)

government and critical infrastructure, while also providing a framework for commercial cryptography governance and international standardisation engagement.<sup>92</sup>

Other domestic regulations include:

- The **Administrative Measures for the Use of Commercial Cryptography in CII** (关键信息基础设施商用密码使用管理规定), effective August 2025, require CII operators to use approved commercial cryptographic algorithms to protect core data and key business systems. This initiative indirectly accelerates quantum-resilient adoption in China.<sup>93</sup>
- In April 2025, China implemented the **Technical Specifications for Quantum Secure Communication Application Equipment Based on Transport Layer Cryptography Protocols** (YD/T 6265-2024, 基于传输层密码协议的量子保密通信应用设备技术规范), standardising the technical requirements for gateway and terminal devices for quantum secure communication applications based on TLCP.<sup>94</sup>
- The Commercial Cryptography Standards Institute (商用密码标准研究院) launched the Next Generation Commercial Cryptography Competency Competition in February 2025. It officially released the **Requirements for Submission of Public Key Cryptography Algorithms** (公钥密码算法提交要求) in October 2025, and has begun to accept algorithm proposals.<sup>95</sup>
- In January 2025, Ministry of Industry and Information Technology (MIIT)'s **Future Industries Innovation Mission** (未来产业创新任务) designated Quantum-resistant cryptographic general-purpose chip architecture as among the targeted R&D priorities.<sup>96</sup>

Technical cryptography standards are developed by Cryptography Standardization Technical Committee (密码行业标准化技术委员会), responsible for cryptography industry standards (GM), and the National Information Security Standardization Technical Committee (**TC260**, 全国网络安全标准化技术委员会), responsible for Cybersecurity-related national standards.<sup>97</sup> The national standards includes the mandatory (**GB**, 国家标准) and voluntary (**GB/T**, 国家标准推荐) cryptographic standard series used across government and critical infrastructure systems.<sup>98</sup> A number of quantum-related standards have been released:

- GB/T 42565-2023 Quantum computing-Terminology and definition<sup>99</sup>
- GB/T 42829-2023 Basic requirements for quantum secure communication applications<sup>100</sup>
- GB/T 47177.1-2026 Quantum Computing Service Platform Part 1: Architecture and Functional Requirements<sup>101</sup>
- In April 2025, TC260 called for consultations on the draft **GB/T Cybersecurity Technology Security Requirements, Test and Evaluation Methods for Quantum Key Distribution, (网络安全技术 量子密钥分发的安全要求、测试和评估方法)**.<sup>102</sup> The draft voluntary national

<sup>92</sup> [https://www.oscca.gov.cn/sca/c100236/2019-10/28/content\\_1057345.shtml](https://www.oscca.gov.cn/sca/c100236/2019-10/28/content_1057345.shtml)

<sup>93</sup> <https://www.sca.gov.cn/sca/xgk/2025-06/27/1061270/files/4c5865c660c243349f9c133dae149209.pdf>

<sup>94</sup> <https://std.samr.gov.cn/hb/search/stdHBDetail?id=2F7B4471A788F3B1F06397BE0A0A6557>

<sup>95</sup> [https://www.niccs.org.cn/symmbzjy/tzgg/pc/content/1937422988373135360/content\\_1937422988373135360.html](https://www.niccs.org.cn/symmbzjy/tzgg/pc/content/1937422988373135360/content_1937422988373135360.html)

<sup>96</sup> [https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2025/art\\_18a01a26d22c4b65a3037bb37cd606bb.html](https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2025/art_18a01a26d22c4b65a3037bb37cd606bb.html)

<sup>97</sup> <http://www.gmbz.org.cn/main/index.html>; <https://www.tc260.org.cn/portal/>

<sup>98</sup> <https://www.gpai.org/files/upload/china/factsheets/GPQ%20Factsheet%20Standardisation%20in%20China.pdf>

<sup>99</sup> <https://www.antpedia.com/standard/en/1452798156.html>

<sup>100</sup> [https://gbstandards.org/GB\\_standard\\_english2.asp?code=GB/T%2042829-2023&id=54417](https://gbstandards.org/GB_standard_english2.asp?code=GB/T%2042829-2023&id=54417)

<sup>101</sup> <https://sesec.eu/2026/03/25/chinas-first-national-standard-for-quantum-computing-service-platform/>, <https://www.antpedia.com/standard/en/2117036513.html>

<sup>102</sup> <https://www.tc260.org.cn/portal/suggestion-detail/20250427104834>; <https://digitalpolicyalert.org/event/29400-national-information-security-standardisation-technical-committee-closes-consultation-on-cybersecurity-standard-for-quantum-key-distribution>

standard proposes a framework to evaluate QKD modules, addressing risks to traditional and quantum components of computer systems, and establishes baseline security requirements for critical assets within QKD systems.

## Critical Information Infrastructure (CII) Considerations

China's CII protection is defined under the **Cybersecurity Law** and detailed in the **Regulations on the Security Protection of CII**.<sup>103</sup> These regulations identify the CII sectors, including finance, energy, transport, water resources, telecommunications, and e-government services as CII requiring enhanced cybersecurity protection. In 2025, China released the **Regulations on the Management of Commercial Cryptography Use in CII** (关键信息基础设施商用密码使用管理规定) which impose requirements for approved commercial cryptography products in CII systems and link cryptographic governance directly to national infrastructure protection obligations.<sup>104</sup>

*Quantum-Ready Infrastructure for CII.* China is an interesting case study for state-driven quantum network development because in 2026, the country already has several existing QKD networks which have been deployed for CII use.

For example, the Beijing-Shanghai Quantum Communication Backbone (BSBN, 京沪京沪干线), the world's first long-distance quantum-secured communication route, was put into service in 2017.<sup>105</sup> The BSBN is able to provide quantum-secure communications for a subset of the country's CII operators. This national QKD space-to-ground network currently serves selected state and local banks, municipal power grids, and e-government platforms across China.

Another QKD system is the Hefei Quantum Metropolitan Area Network (合肥量子城域网部分), launched in Aug 2022.<sup>106</sup> It spans 1,147 km of fibre optic cable across 8 core and 159 access nodes, providing QKD services to approximately 500 government agencies and 380 state-owned enterprises.<sup>107</sup>

*Communications.* China Mobile (中国移动) released a commercial quantum secure application for mobile telecommunication terminals in 2022, with end-to-end encryption with quantum keys, and one-session-one-key security.<sup>108</sup>

*Quantum safe networks.* Besides the national level BSBN, China's quantum metropolitan area network has covered 25 cities as of January 2026, serving more than 6 million quantum-enabled encrypted messaging users, and has been rolled out on a large scale in multiple provinces.<sup>109</sup>

*QKD satellite.* Besides the Micius, China launched the world's first quantum micro-nano satellite, Jinan-1 (济南一号) in 2022. Weighing only about 96 kilograms, roughly one-sixth the weight of its predecessor, Micius, it successfully achieved low-cost, miniaturised, real-time QKD between satellite and ground. In 2025, Jinan-1 completed a QKD between China and South Africa for a distance of 12,900 kilometres.

---

<sup>103</sup> [https://www.cac.gov.cn/2025-12/29/c\\_1768735112911946.htm](https://www.cac.gov.cn/2025-12/29/c_1768735112911946.htm); [https://www.gov.cn/gongbao/content/2021/content\\_5636138.htm](https://www.gov.cn/gongbao/content/2021/content_5636138.htm)

<sup>104</sup> [https://www.oscca.gov.cn/sca/xxgk/2025-06/27/content\\_1061271.shtml](https://www.oscca.gov.cn/sca/xxgk/2025-06/27/content_1061271.shtml)

<sup>105</sup> <https://en.ustc.edu.cn/info/1110/3630.htm>

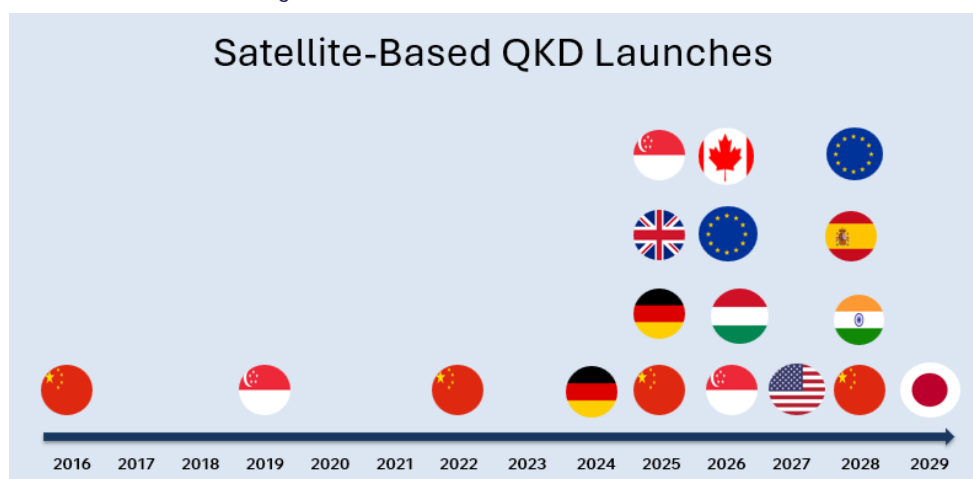
<sup>106</sup> <https://baike.baidu.com/item/China%20Telecom%20Corp%20Ltd/998727>

<sup>107</sup> [https://www.sohu.com/a/828407436\\_121106991](https://www.sohu.com/a/828407436_121106991)

<sup>108</sup> [https://docbox.etsi.org/Workshop/2023/02\\_QUANTUMSAFECRYPTOGRAPHY/TECHNICALTRACK/WORLDTOUR/CASQUANTUMNETWORK\\_QI.pdf](https://docbox.etsi.org/Workshop/2023/02_QUANTUMSAFECRYPTOGRAPHY/TECHNICALTRACK/WORLDTOUR/CASQUANTUMNETWORK_QI.pdf)

<sup>109</sup> <https://www.c114.com.cn/quantum/5285/a1303905.html>

Figure 7: Timeline of Satellite-Based QKD Launches



Source: SKY Perfect JSAT, 2026 (reconstituted from in-person presentation)

*Financial sector.* The People's Bank of China (PBOC), the central bank of China, has connected its bank clearing data centre to the quantum-secured communication BSBN QKD nodes in Beijing, Wuxi, and Shanghai termination points.<sup>110</sup>

Figure 8: Central Bank of China Clearing QKD Data Nodes



Source: CAS Quantum Network Co<sup>111</sup>

<sup>110</sup> [https://docbox.etsi.org/Workshop/2023/02\\_QUANTUMSAFECRYPTOGRAPHY/TECHNICALTRACK/WORLDTOUR/CASQUANTUMNETWORK\\_QI.pdf](https://docbox.etsi.org/Workshop/2023/02_QUANTUMSAFECRYPTOGRAPHY/TECHNICALTRACK/WORLDTOUR/CASQUANTUMNETWORK_QI.pdf)

<sup>111</sup> [https://docbox.etsi.org/Workshop/2023/02\\_QUANTUMSAFECRYPTOGRAPHY/TECHNICALTRACK/WORLDTOUR/CASQUANTUMNETWORK\\_QI.pdf](https://docbox.etsi.org/Workshop/2023/02_QUANTUMSAFECRYPTOGRAPHY/TECHNICALTRACK/WORLDTOUR/CASQUANTUMNETWORK_QI.pdf)

## Operational readiness/ deadlines for implementation

China has not yet set a specific legislative deadline for the migration to PQC. Its national strategy clearly reflects a technological path of **QKD+PQC** integration, emphasising both large-scale deployment of QKD infrastructure and continuous research and application of PQC.

At the policy level, in May 2025, China Telecom Quantum Group released the world's first distributed cryptography system integrating QKD and PQC, achieving commercial application across more than 1000 kilometres, marking the entry of integrated technology into the large-scale application stage.<sup>112</sup>

At the standards level, in March 2026, the National Technical Committee on Quantum Technology Standardization (**SAC/TC 578**, 全国量子技术标准化技术委员会) was approved for adjusted work scope, taking charge of formulation of quantum-related national standards.<sup>113</sup> However, a mandatory timetable for PQC migration has not yet been issued.

## Quantum in China: Summary

### Opportunities

- Strong QKD infrastructure already deployed at scale: the 2,000km Beijing-Shanghai Backbone, satellite links via Micius and Jinan-1, and metropolitan networks covering 25 cities and over 6 million users, coupled with strong hardware progress (Zuchongzhi 3.2 at 107 qubits, Tianyan-504 at 504 qubits)
- A dual-track "QKD+PQC" strategy, including the world's first distributed system integrating both at commercial scale (2025), positions China across two quantum-safe approaches simultaneously.
- Deep integration of quantum-secure networks into CII (banking, e-government, power grids) shows real operational deployment, not just limited to academic research.

### Risks

- No mandatory national deadline for PQC migration exists, despite extensive infrastructure investment.
- Heavy reliance on QKD (fibre/satellite) carries cost, scalability, and physical-infrastructure vulnerabilities that PQC-only approaches avoid.
- Fragmented standard-setting across multiple bodies (SCA, TC260, industry committees) could slow harmonised national rollout; in tandem, the market runs a global standards divergence risk, as China's domestic approach with its GB/T series and TC 578 differs from NIST-aligned PQC efforts pursued elsewhere in APAC and the world.
- CII cryptography rules are still commercial-cryptography-focused rather than quantum-risk-specific, leaving policy gaps.
- Rapid domestic hardware advancement increases geopolitical sensitivity and scrutiny around quantum export/technology controls.

<sup>112</sup> [https://www.chinatelecom.com.cn/ct/news/jtxw/153014.html?CT6T=8b85d0&CT6TS=1cWpWGisp\\_1NgGVL11JPL\\_nt7IZhqUNxRXdiDfsKk94SOXxi1Hc8YwXcKjUjU71](https://www.chinatelecom.com.cn/ct/news/jtxw/153014.html?CT6T=8b85d0&CT6TS=1cWpWGisp_1NgGVL11JPL_nt7IZhqUNxRXdiDfsKk94SOXxi1Hc8YwXcKjUjU71)

<sup>113</sup> <https://caifuhaobao.eastmoney.com/news/20260304113917902712220>

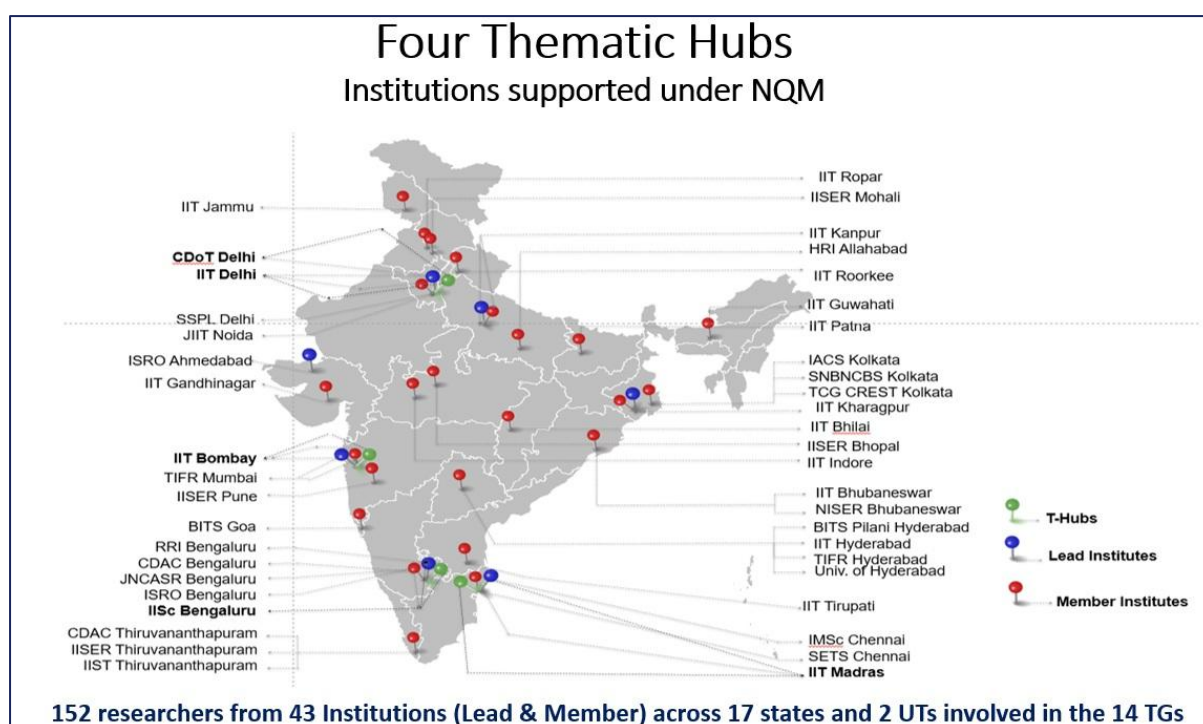
# India

## Existing quantum R&D and investment

India has made quantum technology a national strategic priority, with the National Quantum Mission (NQM)<sup>114</sup> announced in April 2023 representing a commitment of INR 6,000 crore (approximately USD 730 million) over eight years (2023-2031). Run under the Department of Science and Technology (DST), the NQM is guided by the *Implementation of Quantum Safe Ecosystem in India*<sup>115</sup> (a task force report released Feb 2026), and structured around four thematic technology “hubs” that focus on specific quantum domains:

1. **Quantum computing**, based at IISc Bangalore
2. **Quantum communication**, based at IIT Madras
3. **Quantum sensing and metrology**, based at IIT Bombay
4. **Quantum materials and devices**, based at IIT Delhi

Figure 9: India's Quantum Thematic Hubs, with Lead and Supporting Institutions



Source: <https://dst.gov.in/national-quantum-mission-nqm>

<sup>114</sup> <https://dst.gov.in/national-quantum-mission-nqm>

<sup>115</sup> [https://dst.gov.in/sites/default/files/Report\\_TaskForce\\_PQMmigration\\_4Feb26%20%28v1%29.pdf](https://dst.gov.in/sites/default/files/Report_TaskForce_PQMmigration_4Feb26%20%28v1%29.pdf)

In addition, in May 2026, the DST NQM also released the *Report on Quantum-Safe Ecosystem in India: Roadmap to Quantum Resiliency*.<sup>116</sup> It puts forth a roadmap for India's implementation of a quantum-safe ecosystem. The report describes the quantum threat, and outlines India's institutional approach under the NQM, and sets out time-bound recommendations for launching PQC and hybrid pilot projects for high-priority systems. It also establishes a National PQC Testing and Certification Program, addresses procurement requirements, as well as makes other recommendations for strategic sectors and solutions to create a national quantum secure backbone for communications, aligned with India's requirements.



In addition, the roadmap also details India's timelines and milestones for quantum migration, where CII (defence, power, telecom, and other critical sectors) must be in a preparatory stage by end of 2027, must have migrated high priority systems by 2<sup>nd</sup> 2028, and must have resiliency for all systems by end 2029. For other regular enterprises, resiliency for all systems should target end of 2033 (see next section on PQC roadmaps).

**Quantum Computing in Academia and the Private Sector.** India's quantum research ecosystem has academic roots and interests, that tie together with state initiatives to develop quantum computing, supported by private sector funding and investment.

- For example, the Indian Statistical Institute (ISI) Kolkata has a long tradition of research in cryptography and information theory with quantum implications, specifically within its Advanced Computing and Microelectronics Unit.<sup>117</sup> In Feb 2024, the Centre for Cyber-Physical Systems (C-CPS) was established between Ericsson Research and Indian Statistical Institute (ISI) to undertake interdisciplinary research in applied research, amongst which was 6G telecommunication as well as classical and quantum secure communication.<sup>118</sup>
- India's start-up ecosystem is also contributing to establishing the country's quantum capacity. QNu Labs, founded in 2016, is an Indian deeptech startup focusing on quantum security. They have developed QKD systems - such as their ARMOS QKD platform - and quantum random number generators (QRNGs) that have been deployed in initial pilots with government and financial sector clients.<sup>119</sup>
- In 2025, Bangalore-based startup QpiAI launched a 25-qubit superconducting quantum computer, the QpiAI-Indus.<sup>120</sup> This is India's first full-stack quantum computing platform.<sup>121</sup> The company continues to develop and innovate in the quantum space, including developing and launching the QpiAI Kaveri, a 64-qubit superconducting quantum processor chip, amongst other related quantum products.<sup>122</sup>
- In April 2026, local company QNu Labs - a startup nurtured by the NQM, successfully demonstrated a 1,000-kilometre quantum communication network with a secure key rate of

<sup>116</sup> <https://dst.gov.in/quantum-safe-ecosystem-in-india>

<sup>117</sup> [https://www.isical.ac.in/unit/index?unit\\_name=ACMU](https://www.isical.ac.in/unit/index?unit_name=ACMU)

<sup>118</sup> <https://www.ericsson.com/en/press-releases/2/2024/2/ericsson-research-and-indian-statistical-institute-join-hands-for-collaborative-research-in-safe-and-reliable-cyber-physical-systems>

<sup>119</sup> <https://analyticsindiamag.com/ai-news/qnu-labs-validates-its-quantum-key-distribution-performance-for-encrypted-communication>

<sup>120</sup> <https://qpi.ai/tech/products/qpi-ai-indus-quantum>

<sup>121</sup> <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2121845&reg=3&lang=2>

<sup>122</sup> <https://qpi.ai/tech/>

240 bits per second with a low error rate, under real-world conditions (i.e. not a simulated test).<sup>123</sup>

### Quantum computing in the public sector.

- The **Metro Area Quantum Access Network (MAQAN)** is India's first quantum network testbed, established in **Chennai**.<sup>124</sup> It supports a five-node topology using indigenously designed control electronics for QKD protocols.<sup>125</sup> Funded by India's Ministry of Electronics and Information Technology (MeitY),<sup>126</sup> the collaborative project brings together IIT Madras, C-DAC Bangalore, ERNET and SETS Chennai to build a last-mile quantum-secure access network. The team also plans a key relay mechanism to be demonstrated in both star and mesh topologies.<sup>127</sup>
- MeitY has also established the **Quantum Computing Applications Lab**<sup>128</sup>. This lab has been working together with other private sector partners (such as AWS) to run tests and problem statements that will demonstrate positive social impact of cloud computing technologies and prototyping.<sup>129</sup>
- Other public sector developments include state-level initiatives, such as **Andhra Pradesh's Amaravati Quantum Valley Project**.<sup>130</sup> The state established two quantum computer test beds in April 2026. The computers were built from locally developed components (and therefore part of the *Make In India* initiative) and hosted at the 1Q test bed in Medha Towers and 1S test bed at SRM University Amaravati. These quantum computers are part of an open-access approach which is being driven by the Andhra Pradesh State Quantum Mission, allowing other state governments and institutions to run tests on the quantum computers. The Tata Institute of Fundamental Research (TIFR), the Indian Institute of Science (IISc) and the Defence Research and Development Organisation (DRDO) provided technical assistance to this project.

## PQC regulations and requirements and roadmaps

India's cybersecurity regulation is handled via a multi-agency approach, rather than a singular regulatory body. The core regulatory agencies, along with their quantum-related regulations and/or guidelines are listed below.

1. In the first instance, the **Department of Science and Technology (DST)** - while not a regulator - launched a task force report in Feb 2026 that provides a framework for quantum development in India, titled *Implementation of Quantum Safe Ecosystem in India*.<sup>131</sup> This roadmap is also reiterated in the *Report on Quantum-Safe Ecosystem in India: Roadmap to Quantum Resiliency*<sup>132</sup> (see Annexure C), and sets out recommendations for India's quantum computing development, with three major milestones:

<sup>123</sup> <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2250162&reg=3&lang=1>

<sup>124</sup> <https://ieeexplore.ieee.org/document/11249862>

<sup>125</sup> <https://www.iitm.ac.in/happenings/events/metro-area-quantum-access-network-integrated-ml-ecosystem>

<sup>126</sup> <https://quantumindia.net/cdac-quantum-activities/>

<sup>127</sup> [https://www.cdac.in/index.aspx?id=project\\_details&projectId=MetroAreaQuantumAccessNetwork%28MAQAN%29](https://www.cdac.in/index.aspx?id=project_details&projectId=MetroAreaQuantumAccessNetwork%28MAQAN%29)

<sup>128</sup> <https://www.digitalindia.gov.in/initiative/the-meity-quantum-computing-applications-lab/>, <https://negd.gov.in/the-meity-quantum-computing-applications-lab/>

<sup>129</sup> <https://www.psa.gov.in/innerPage/psa-initiatives-covid/call-proposal-meity-aws-quantum-computing-applications-lab-qcal/4119>

<sup>130</sup> <https://telecom.economicstimes.indiatimes.com/news/policy/andhra-pradesh-to-launch-indias-first-open-access-quantum-computer-testbeds/130249586>

<sup>131</sup> [https://dst.gov.in/sites/default/files/Report\\_TaskForce\\_PQMigraion\\_4Feb26%20%28v1%29.pdf](https://dst.gov.in/sites/default/files/Report_TaskForce_PQMigraion_4Feb26%20%28v1%29.pdf)

<sup>132</sup> <https://dst.gov.in/quantum-safe-ecosystem-in-india> (See Annexure C).

- **Milestone 1 - Build Foundations: CII by 2027, Enterprise by 2028.** The roadmap recommends that organisations establish strong data governance foundations such as inventory of their cryptographic assets, and start working on cross-functional quantum-risk management. The report also recommends PQC readiness requirements in procurement processes and adopting hybrid PQ/T signatures for critical software and systems.
- **Milestone 2 - Migrate High Priority Systems: CII by 2028, Enterprise by 2030.** The report recommends that for this milestone, pilot projects should move into full migration to quantum programs, establishing strong supplier accountability mechanisms, as well for organisations to be upgrading their Public Key Infrastructure (PKI), Hardware Security Modules (HSM), and Key Management Systems (KMS/KSM) and libraries to PQC-ready versions. By Milestone 2, classical-only computer systems should be isolated where immediate migration is not feasible.
- **Milestone 3 - Full PQC Adoption CII by 2029, Enterprise by 2033.** This milestone is for complete enterprise-wide adoption, with organisations establishing PQC-only trust chains and quantum-secure digital signatures. The framework proposes long-term vendor oversight and accountability with audits and a process for continuous algorithm updates, as well as layered risk-management for the remaining legacy systems.

Establish a National PQC Testing and Certification Program by December 2026, utilising Tier-1 and Tier-2 labs under agencies like Telecom Engineering Centre (TEC) and Standardisation Testing and Quality Certification (STQC). The report also suggests that there is an urgent need for India's transition to quantum-safe security, which requires not only the adoption of globally recognised PQC algorithms, but also the establishment of a sovereign, measurement-driven assurance ecosystem.

Table 2: India's Milestones and Timelines for Quantum Migration

| Organisation                                           | Milestone 1 – Preparatory stage – CBOM, QRA, etc., | Milestone 2 – Migration of High Priority Systems | Milestone 3 – Resiliency for all systems |
|--------------------------------------------------------|----------------------------------------------------|--------------------------------------------------|------------------------------------------|
| CII - Defence, Power, Telecom & Other Critical Sectors | 31 Dec 2027                                        | 31 Dec 2028                                      | 31 Dec 2029                              |
| Regular Enterprises                                    | 31 Dec 2028                                        | 31 Dec 2030                                      | 31 Dec 2033                              |

Source: <https://dst.gov.in/quantum-safe-ecosystem-in-india>

The *Implementation of Quantum Safe Ecosystem in India*<sup>133</sup> framework, as well as the identified standards in the *Report on Quantum-Safe Ecosystem in India: Roadmap to Quantum Resiliency*<sup>134</sup> also provides a guiding list of international quantum standards for consideration, including NIST, ISO/IEC, ITU, ETSI, as well as local quantum standards from the India TEC (this list is non-exhaustive):

- TEC 91000:2022 Standard for Generic Requirements on Quantum Key Distribution System<sup>135</sup>

<sup>133</sup> [https://dst.gov.in/sites/default/files/Report\\_TaskForce\\_PQMigraion\\_4Feb26%20%28v1%29.pdf](https://dst.gov.in/sites/default/files/Report_TaskForce_PQMigraion_4Feb26%20%28v1%29.pdf)

<sup>134</sup> <https://dst.gov.in/quantum-safe-ecosystem-in-india>, p93, in Annexure-V of the Report of Sub-Group I on the Framework for Testing and Certification of PQC-based Quantum-Safe Products and Solutions

<sup>135</sup> [https://www.tec.gov.in/pdf/Whatsnew/QKD\\_%20Final\\_Draft\\_TEC\\_Standard\\_GR%20-%2015.07.2022.pdf](https://www.tec.gov.in/pdf/Whatsnew/QKD_%20Final_Draft_TEC_Standard_GR%20-%2015.07.2022.pdf)

- TEC 91010:2023 Standard for Generic Requirements on Quantum Safe and Classical Cryptographic Systems<sup>136</sup>
  - TEC 91020:2024 Standard for Generic Requirements on Quantum Random Number Generator<sup>137</sup>
  - TEC 91001:2023 Test Guide on Quantum Key Distribution System<sup>138</sup>
  - TEC 91021:2025 Test Guide on Quantum Random Number Generator<sup>139</sup>
2. **The Ministry of Electronics and Information Technology (MeitY)**<sup>140</sup> and its specialist agency, the **Computer Emergency Response Team India (CERT-In)**<sup>141</sup> who leads in national responses to cybersecurity incidents, and issues guidelines and emergency measures under the India IT Act 2000.<sup>142</sup> CERT-In, together with SISA, released a white paper in Jul 2025, *Transitioning to Quantum Cyber Readiness*<sup>143</sup>. The white paper offers a suggested organisational roadmap for companies - particularly in CII sectors such as banking and finance, healthcare, civil infrastructure, and defence, to transition to quantum-resilient encryption models before traditional encryption algorithms are compromised by quantum computing.

## Critical Information Infrastructure (CII) Considerations

The Critical Information Infrastructure Protection Centre (NCIIPC),<sup>144</sup> an agency under the National Technical Research Organisation (NTRO),<sup>145</sup> is responsible for protecting Indian CII across sectors including power, banking, telecom, transport, and e-governance. NCIIPC has issued guidelines for CII protection that include cybersecurity requirements through the Information Technology (Information Security Practices and Procedures for Protected System) Rules 2018,<sup>146</sup> though PQC-specific guidance has not yet been developed.

India's financial sector regulator, the Reserve Bank of India (RBI), has begun establishing strategic plans which may encompass quantum risk, such as the *Utkarsh 2029 Medium-Term Strategy Framework (2026-29)*.<sup>147</sup> Currently, the RBI's Cybersecurity Framework for Banks (2016) and subsequent Master Directions on Information Technology Governance, Risk, Controls and Assurance Practices (2023)<sup>148</sup> establish a risk-based cybersecurity framework for banks and financial institutions, but quantum risk is not explicitly addressed. However, there is institutional attention to quantum-readiness, as the RBI has set up an expert committee looking into a Quantum Secure and Adaptive Financial Ecosystem (Q-SAFE) as of May 2026, which is due to make its first report at the end of 2026.<sup>149</sup>

<sup>136</sup> [https://www.tec.gov.in/pdf/6GT/GR\\_91010\\_2023\\_for\\_Publish.pdf](https://www.tec.gov.in/pdf/6GT/GR_91010_2023_for_Publish.pdf)

<sup>137</sup> [https://www.tec.gov.in/pdf/GRs/Standard\\_GR\\_QRNG\\_TEC\\_91020\\_2024\\_Final%20\(1\).pdf](https://www.tec.gov.in/pdf/GRs/Standard_GR_QRNG_TEC_91020_2024_Final%20(1).pdf)

<sup>138</sup> [https://www.tec.gov.in/pdf/TSTP/Provisional\\_Test\\_Guide\\_QKD\\_91001\\_2023\\_Final.pdf](https://www.tec.gov.in/pdf/TSTP/Provisional_Test_Guide_QKD_91001_2023_Final.pdf)

<sup>139</sup> [https://sansad.in/getFile/oksabhaquestions/annex/185/AU689\\_WqNums.pdf?source=pqals](https://sansad.in/getFile/oksabhaquestions/annex/185/AU689_WqNums.pdf?source=pqals)

<sup>140</sup> <https://www.meit.gov.in/>

<sup>141</sup> <https://www.cert-in.org.in/>

<sup>142</sup> [https://www.meit.gov.in/static/uploads/2024/03/IT-Act-Rules\\_2000\\_0.pdf](https://www.meit.gov.in/static/uploads/2024/03/IT-Act-Rules_2000_0.pdf)

<sup>143</sup> <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/jul/doc2025714585911.pdf>

<sup>144</sup> <https://nciipc.gov.in/>

<sup>145</sup> <https://ntro.gov.in/>

<sup>146</sup> <https://www.meit.gov.in/static/uploads/2024/02/NCIIPC-Rules-notification-1.pdf>

<sup>147</sup> <https://www.varindia.com/news/RBI-aims-to-create-robust-frameworks-for-emerging-technologies-under-%E2%80%99Utkarsh-2029%E2%80%9999>

<sup>148</sup> <https://rbidocs.rbi.org.in/rdocs/content/pdfs/Utkarsh202910042026.pdf>

<sup>149</sup> [https://www.rbi.org.in/scripts/BS\\_ViewMasDirections.aspx?id=12562](https://www.rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=12562)

<sup>149</sup> [https://www.rbi.org.in/scripts/BS\\_PressReleaseDisplay.aspx?prid=62803](https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=62803)

## Operational readiness/ deadlines for implementation

There are no current deadlines for PQC implementation; there are recommendations from the DST report on *Implementation of Quantum Safe Ecosystem in India*<sup>150</sup> (see above) but these are not mandatory.

## Quantum in India: Summary

### Opportunities

- A potential quantum readiness leader, India's National Quantum Mission has committed INR 6,000 crore (~USD 730m) over 2023-2031 across four dedicated technology hubs.
- Strong digital infrastructure development and a diverse ecosystem spanning academia (IISc, IIT network), public sector (MeitY's Quantum Computing Applications Lab with AWS), and start-ups (QNu Labs, QpiAI) shows breadth of momentum in the market.
- Clear three-milestone national roadmap (2027/2028/2029 for CII; 2028/2033 for enterprise), and sector-specific guidance from CERT-In/SISA (2025) gives organisations, and CII industries like banking and healthcare an early transition roadmap, and structured planning horizon.
- Real-world application achieved, including a 1,000km quantum communication demonstration by QNu Labs (2026), show the ecosystem moving beyond lab-stage work.

### Risks

- PQC regulation is fragmented across multiple agencies (DST, MeitY, CERT-In, RBI) with no single regulatory authority.
- Current roadmap milestones are recommendations, not mandatory requirements, and implementation depends on voluntary uptake, and which may make milestone timelines (CII PQC adoption by 2029) difficult to meet given no mandatory enforcement mechanism.
- NCIIIPC's CII guidelines do not yet contain PQC-specific requirements, leaving critical sectors without recommended technical standards.
- RBI's cybersecurity frameworks for banks do not explicitly address quantum risk despite finance being a priority sector.
- Establishing a sovereign "Make In India" certification ecosystem (national PQC testing program targeted for Dec 2026) could result in fragmentation/deviation from international standards approach, and local standards development may limit growth and expansion.

---

<sup>150</sup> [https://dst.gov.in/sites/default/files/Report\\_TaskForce\\_PQMigration\\_4Feb26%20%28v1%29.pdf](https://dst.gov.in/sites/default/files/Report_TaskForce_PQMigration_4Feb26%20%28v1%29.pdf)

---

## Japan

### *Existing quantum R&D and investment*

Japan's 7<sup>th</sup> Basic Plan for Science, Technology and Innovation<sup>151</sup> designates quantum as one of six National Strategic Technology Areas, and specifically includes quantum communication and cryptography technologies within that remit. The government frames quantum both as an important source of future growth with wide cross-sector applications, while also underpinning national and economic security. Taken together, the 7<sup>th</sup> Basic Plan positions quantum technologies as foundational for next-generation industries and a determinant of Japan's geopolitical competitiveness, requiring coordinated policy, supply chain resilience, and international alignment with allies and like-minded countries.

To operationalise this, the 7<sup>th</sup> Plan outlines several support areas facilitated through a whole-of-government approach coordinated by the Council for Science, Technology and Innovation (CSTI). These include:

- Prioritised R&D investment through targeted tax incentives and long-term public funding commitments.
- strengthening human capital via expanded talent pipelines.
- international talent circulation and industry uptake of advanced researchers; and
- reinforcing public-private collaboration at leading research hubs.

These measures will be supported by forthcoming intellectual property and standardisation strategies, supply chain and technology protection measures to mitigate leakage risks, and active promotion of international partnerships to scale markets and embed Japanese technologies globally.

Between 2020 and 2023, CSTI refined Japan's national quantum strategy between three documents: the **"Quantum Technology Innovation Strategy"**<sup>152</sup> (January 2020), the **"Vision for a Quantum Future Society"**<sup>153</sup> (April 2022), and the **"Strategy for the Creation of Quantum Future Industries"**<sup>154</sup> (April 2023).<sup>155</sup> Collectively, they define three primary goals to be achieved by 2030:

1. 10 million domestic users of quantum technology;
2. JPY 50 trillion (USD 315 billion) in production generated by quantum technology;
3. Creation of Japanese quantum unicorn ventures.

Towards realising these objectives, the Quantum Technology Innovation Council released a 2024 report<sup>156</sup> emphasising the importance of international collaboration as well as the **"Promotion Measures for the Development of a Quantum Ecosystem"**<sup>157</sup> in 2025 outlining current challenges and policy recommendations.<sup>158</sup> In particular, the Council's public-private Quantum Ecosystem Promotion Working Group identified four policy areas that must be addressed:

1. Measures for creating technologies of such excellence that Japan attracts global attention, and for continuing to nurture those technologies;

---

<sup>151</sup> <https://www8.cao.go.jp/cstp/kihonkeikaku/index7.html>

<sup>152</sup> [https://www8.cao.go.jp/cstp/ryoshigijutsu/roadmap\\_220422.pdf](https://www8.cao.go.jp/cstp/ryoshigijutsu/roadmap_220422.pdf)

<sup>153</sup> [https://www8.cao.go.jp/cstp/ryoshigijutsu/ryoshimirai\\_220422.pdf](https://www8.cao.go.jp/cstp/ryoshigijutsu/ryoshimirai_220422.pdf)

<sup>154</sup> [https://www8.cao.go.jp/cstp/ryoshigijutsu/230414\\_mirai.pdf](https://www8.cao.go.jp/cstp/ryoshigijutsu/230414_mirai.pdf)

<sup>155</sup> <https://www8.cao.go.jp/cstp/ryoshigijutsu/ryoshigijutsu.html>

<sup>156</sup> [https://www8.cao.go.jp/cstp/ryoshigijutsu/240409\\_q\\_measures.pdf](https://www8.cao.go.jp/cstp/ryoshigijutsu/240409_q_measures.pdf)

<sup>157</sup> [https://www8.cao.go.jp/cstp/ryoshigijutsu/250530\\_q\\_ecosys.pdf](https://www8.cao.go.jp/cstp/ryoshigijutsu/250530_q_ecosys.pdf)

<sup>158</sup> [https://www8.cao.go.jp/cstp/ryoshigijutsu/250530\\_q\\_ecosys.pdf](https://www8.cao.go.jp/cstp/ryoshigijutsu/250530_q_ecosys.pdf)

2. Measures for ensuring that Japan joins the world’s “club members” and exercises initiative within global supply chains;
3. Measures for creating startups, venture companies, and new businesses, and for enabling their growth;
4. Institutional reforms to expand the quantum industry by supporting the overseas expansion of Japanese firms and attracting foreign firms to Japan.

*Quantum Computing in Academia and the Private Sector.* In the private sector, Japan’s quantum ecosystem is primarily led by large industrial conglomerates including NTT, NEC, Toshiba, and Fujitsu, and funding is primarily derived from domestic sources.<sup>159</sup> In addition to the Quantum Ecosystem Promotion Working Group, there are also two primary Japanese quantum industry consortia: the Quantum Forum<sup>160</sup>, which focuses on partnerships between the private sector and academic institutions, and the Quantum Strategic Industry Alliance for Revolution (Q-STAR)<sup>161</sup>, which primarily coordinates quantum R&D efforts among the conglomerates and advocates policies with the Japanese government on behalf of its members.

In academia, Japan has progressively designated research institutions as Quantum Technology Innovation Hubs (QIHs) since February 2021 to support collaboration between industry, academia, and government on quantum R&D. As of January 2026, twelve QIHs have been established with the Institute of Physical and Chemical Research (RIKEN) serving as a headquarters to support cross-hub activities.<sup>162</sup>

The institutions, and their respective focus areas, are:

1. Quantum computation pioneering (RIKEN)
2. Quantum computer applications (UTokyo & Business alliance)
3. Quantum software (Osaka University)
4. Global research and development for business by quantum-AI technology (AIST) - The AIST G-QuAT has established testbeds to foster use-case development, including the deployment of superconducting, cold-atom, and photonic quantum computers.
5. Quantum technology international collaboration (OIST)
6. Quantum security (NICT)
7. Photonic Quantum Science (Kyoto University)
8. Quantum material (NIMS)
9. Foundational quantum technology and quantum life R&D (QST)
10. Quantum sensing (Science Tokyo)
11. Quantum-based chemistry for industry development (THERS)
12. Quantum solution (Tohoku University)

Lastly, the Japan Society for the Promotion of Science, a nonprofit foundation that was part of the government until 2003, is a major funder of quantum research in Japan.<sup>163</sup> By 2023, it had funded more than twice the number of quantum information science research publications than any other individual organisation in Japan.<sup>164</sup>

<sup>159</sup> [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RRA2000/RRA2055-1/RAND\\_RRA2055-1.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2000/RRA2055-1/RAND_RRA2055-1.pdf)

<sup>160</sup> <https://qforum.org/about/org>

<sup>161</sup> <https://qstar.jp/about>

<sup>162</sup> [https://qih.riken.jp/en/images/pdf/Brochure\\_QIH\\_E.pdf](https://qih.riken.jp/en/images/pdf/Brochure_QIH_E.pdf)

<sup>163</sup> <https://www.jsps.go.jp/>

<sup>164</sup> [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RRA2000/RRA2055-1/RAND\\_RRA2055-1.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2000/RRA2055-1/RAND_RRA2055-1.pdf)

*Quantum computing in the public sector.* The Secretariat for Science, Technology and Innovation estimated that Japan’s proposed budget for FY2026 contained approximately JPY 43.4 billion in quantum-related initiatives, up from JPY 36.1 billion initially budgeted in FY2025.<sup>165</sup> They include:

- The **“Promoting the Application of Advanced Quantum Technology Platforms to Social Challenges”** initiative<sup>166</sup> under the third phase of the cross-ministerial Strategic Innovation Promotion Program (SIP), which aims to develop shared infrastructure to demonstrate concrete solutions to real-world societal and industrial problems through hybrid quantum solutions;
- The **Moonshot Research and Development Program**<sup>167</sup>, which has as one of its goals the creation of a fault-tolerant, general-purpose quantum computer by 2050;
- The **Program for Developing Important Technologies for Economic Security** (“K Program”)<sup>168</sup>, which includes exploring the use of quantum sensing technologies in non-GPS environments;
- The **Photon and Quantum Basic Research Coordinated Development Program** (“Q-LEAP”)<sup>169</sup> promoted by the Ministry of Education, Culture, Sports, Science and Technology, which includes networked research hubs carrying out projects related to quantum information processing among other fields.

Government-led quantum information security R&D is led by the National Institute of Information and Communications Technology (NICT), which frequently partners with the private sector on both PQC and QKD projects. Examples include:

- Seamless Migration to PQC for Certification Authorities, with TOPPAN Holdings and ISARA (April 2026)<sup>170</sup>
- Integration of a QKD system into a high-capacity optical transmission system, with Toshiba and NEC (July 2025)<sup>171</sup>
- Integration of quantum secure cloud and quantum computers, with RIKEN, Osaka University, and QunaSys (March 2025)<sup>172</sup>
- Tokyo QKD Network, with NEC, Mitsubishi Electric, and NTT (October 2010)<sup>173</sup>

### ***PQC regulations and requirements and roadmaps***

The Cabinet Secretariat (CAS) coordinates government-wide policies in Japan. It contains the Cabinet Intelligence and Research Office (CIRO), Japan’s national civilian intelligence agency, as well as the National Cybersecurity Office (NCO). CAS released an interim report in November 2025 and NCO released the Cybersecurity Strategy in December 2025, in which the Japanese government pledged - in principle - to complete a full transition to PQC by 2035, in part to ensure alignment with timelines already established in the US and EU.<sup>174</sup> A PQC transition roadmap will be formulated in FY 2026.

CRYPTREC<sup>175</sup> is a project that evaluates and monitors the security of cryptographic technologies used by the Japanese government. It is jointly operated by the Digital Agency, the Ministry of Internal Affairs

---

<sup>165</sup> <https://www8.cao.go.jp/cstp/ryoshigijutsu/26kai/siry04.pdf>

<sup>166</sup> <https://www.qst.go.jp/site/sip3/sip3ryousi.html>

<sup>167</sup> <https://www8.cao.go.jp/cstp/moonshot/index.html>

<sup>168</sup> [https://www8.cao.go.jp/cstp/anzen\\_anshin/kprogram.html](https://www8.cao.go.jp/cstp/anzen_anshin/kprogram.html)

<sup>169</sup> <https://www.jst.go.jp/stpp/q-leap/>

<sup>170</sup> <https://www2.nict.go.jp/qictcc/en/news/20260409.html>

<sup>171</sup> <https://www2.nict.go.jp/qictcc/en/news/20250728.html>

<sup>172</sup> <https://www2.nict.go.jp/qictcc/en/news/20250314.html>

<sup>173</sup> <https://www.nict.go.jp/en/quantum/topics/20101014-1.html>

<sup>174</sup> [https://www.cas.go.jp/jp/seisaku/pqc/pdf/report\\_202511.pdf](https://www.cas.go.jp/jp/seisaku/pqc/pdf/report_202511.pdf)

<sup>175</sup> <https://www.cryptrec.go.jp/en/about.html>

and Communications (MIC), the Ministry of Economy, Trade and Industry (METI), NICT, and the Innovation Platform Agency (IPA). In March 2025, CRYPTREC published the Cryptographic Technology Guideline - Post-Quantum Cryptography - 2024 Edition, which provides a comprehensive overview of existing approaches to PQC and includes a migration roadmap.<sup>176</sup> In addition, CRYPTREC maintains the CRYPTREC Ciphers List, which identifies cryptographic technologies that may be used in Japanese government information systems. The list was updated in March 2026 to include PQC.

Among sectoral regulators, Japan's Financial Services Agency (FSA) suggested in 2024 that financial institutions may be required to transition to PQC but has not yet issued any mandatory requirements. That notwithstanding, FSA urged financial institutions to begin the PQC migration process immediately during a dialogue meeting with the Japan Securities Dealers Association (JSDA) in June 2025.<sup>177</sup>

### **Critical Information Infrastructure (CII) Considerations**

In May 2025, Japan's National Diet adopted the Active Cyber Defence Law<sup>178</sup>, a sweeping legislation aimed at expanding the government's ability to actively manage cyber threats. Among other provisions, the law requires critical infrastructure operators identified under the Economic Security Promotion Act 2022<sup>179</sup> to report cybersecurity incidents to a newly established Cyber Council as well as to their relevant sectoral regulator.

Shortly after the Active Cyber Defence Law's passage, the Japanese government formally established the National Cybersecurity Office (NCO) to oversee its implementation while serving as the central coordinating body for Japan's cyber defence.<sup>180</sup> In the year since its establishment, the NCO has released guidelines and policies covering a variety of cybersecurity topics, including:

- Cybersecurity Talent Framework 2026<sup>181</sup>;
- Guidelines on the Roles Expected of Cyber Infrastructure Providers (March 2026)<sup>182</sup>;
- Policy for establishing a system for evaluating security measures to strengthen the supply chain (March 2026)<sup>183</sup>;
- Cybersecurity Strategy (December 2025)<sup>184</sup>.

The Cybersecurity Strategy's aim is to ensure Japan's cybersecurity, government agencies and related agencies aim for the transition to PQC by 2035, in principle. Taking into account the current use of cryptographic and other technologies at government agencies and related agencies, a roadmap will be formulated in FY2026 in collaboration with relevant ministries and agencies to promote a smooth nationwide transition.<sup>185</sup>

### **Operational readiness/ deadlines for implementation**

- Liaison Conference of Relevant Ministries and Agencies for the Use of Post-Quantum Cryptography (PQC) in Government Agencies and Related Organizations' *Interim Summary on*

<sup>176</sup> <https://www.cryptrec.go.jp/report/cryptrec-gl-2007-2024.pdf>

<sup>177</sup> [https://www.fsa.go.jp/en/press\\_releases/issues/202506/02.pdf](https://www.fsa.go.jp/en/press_releases/issues/202506/02.pdf)

<sup>178</sup> [https://www.shugiin.go.jp/internet/itdb\\_gian.nsf/html/gian/honbun/howan/g21306007.htm](https://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/howan/g21306007.htm)

<sup>179</sup> [https://www.cao.go.jp/keizai\\_anzen\\_hosho/suishinhou/suishinhou.html](https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/suishinhou.html)

<sup>180</sup> <https://japannews.yomiuri.co.jp/politics/politics-government/20250701-266862/>

<sup>181</sup> <https://www.cyber.go.jp/council/csjinzai/index.html>

<sup>182</sup> <https://www.cyber.go.jp/policy/group/kihon-2/policy.html#yakuwari>

<sup>183</sup> <https://www.cyber.go.jp/policy/group/kihon-2/policy.html#supply-chain>

<sup>184</sup> [https://www.cyber.go.jp/pdf/policy/kihon-s/cs\\_strategy2025.pdf](https://www.cyber.go.jp/pdf/policy/kihon-s/cs_strategy2025.pdf)

<sup>185</sup> [https://www.cyber.go.jp/pdf/policy/kihon-s/cs\\_strategy2025.pdf](https://www.cyber.go.jp/pdf/policy/kihon-s/cs_strategy2025.pdf)

*the Transition to Post-Quantum Cryptography (PQC)*<sup>186</sup> in Government Agencies and the NCO's Cybersecurity Strategy pledge a full, government-wide transition to PQC by 2035.<sup>187</sup>

- NCO's Cybersecurity Strategy also aims to accelerate the deployment of QKD around 2030.<sup>188</sup>
- In a 2025 dialogue, the Japan FSA urged domestic financial institutions to start transitioning to PQC immediately to counter future quantum threats expected by the mid-2030s.<sup>189</sup> They also referred to the FS-ISAC's position paper on the financial sector's global transition to PQC migration.<sup>190</sup>

## Quantum in Japan: Summary

### Opportunities

- Quantum designated one of six National Strategic Technology Areas in the 7th Basic Plan for Science, Technology and Innovation, ensuring top-level policy backing.
- Strong industrial base pairs private companies with 12 government-designated Quantum Technology Innovation Hubs.
- Rising public funding where the market's quantum budget grew from JPY 36.1bn (FY2025) to JPY 43.4bn (FY2026), signals sustained commitment.
- Active NICT-led public-private PQC/QKD pilots (e.g., certification authority migration with TOPPAN/ISARA) build practical transition experience.
- Clear, dated national commitment: full government PQC transition by 2035, aligned with US/EU timelines, supported by CRYPTREC's evolving cryptographic guidelines.

### Risks

- PQC transition roadmap is still being formulated (due FY2026), so detailed implementation guidance is not yet available, which creates business ambiguity.
- Financial regulator (FSA) PQC transition for institutions are only "suggested" and not mandated, which risks slower uptake in the financial sector.
- Newly established National Cybersecurity Office and Active Cyber Defence Law framework are still maturing implementation guidance for CII operators.

---

<sup>186</sup> [https://www.cas.go.jp/jp/seisaku/pqc/pdf/report\\_202511.pdf](https://www.cas.go.jp/jp/seisaku/pqc/pdf/report_202511.pdf)

<sup>187</sup> <https://semiwiki.com/forum/threads/2035-japan%E2%80%99s-nco-sets-the-timeline-for-quantum-security.24126/>

<sup>188</sup> [https://www.cyber.go.jp/pdf/policy/kihon-s/cs\\_strategy2025\\_abstract\\_english.pdf](https://www.cyber.go.jp/pdf/policy/kihon-s/cs_strategy2025_abstract_english.pdf) (see slide 5)

<sup>189</sup> [https://www.fsa.go.jp/en/press\\_releases/issues/202511/02.pdf](https://www.fsa.go.jp/en/press_releases/issues/202511/02.pdf)

<sup>190</sup> <https://www.fsisac.com/the-timeline-for-post-quantum-cryptographic-migration>

---

# Singapore

## Existing quantum R&D and investment

Singapore's quantum investment is driven by a combination of research institutions, proactive government R&D policy, and its financial sector and regulators.

*Government Coordination.* Singapore's research into quantum computing is heavily driven by the government and national agenda. Research and deployment of quantum computing were part of the **National Research Infrastructure (NRI)** framework (released April 2015),<sup>191</sup> and funded by the Singapore **National Research Foundation (NRF)**<sup>192</sup> under its Quantum Engineering Programme (QEP) which conducts research across quantum computing, quantum communications, and quantum-safe cryptography.<sup>193</sup>

The **National Quantum Strategy**<sup>194</sup> (launched 2024) and the National Quantum Office (NQO) currently drives Singapore's quantum approach, and the government has committed to investing close to SGD 300 million (USD 236 million) into the programme.<sup>195</sup>

*Research and Academic Institutions.* A short timeline of the various agencies and organisations which have been set up and/or involved with Singapore's quantum sector follows:

- 2007 - the **Centre for Quantum Technologies (CQT)**<sup>196</sup> was established as a Research Centre of Excellence (RCE) supported by the NRF and Ministry of Education (MOE),
- 2016 - A\*STAR established the **Quantum Technologies for Engineering (QTE)**<sup>197</sup> programme, followed by 2018 where the NRF launched the Quantum Engineering Programme,
- 2022 - **National Quantum Office (NQO)**<sup>198</sup> was formed,
- 2022 - First grant from **Agency for Science, Technology and Research (A\*STAR)** awarded for a researcher who was performing research on “quantum information technology”,
- 2024 - Launch of the **National Quantum Strategy**<sup>199</sup>.

Adjacent to the timeline, another resource which was set up was the **National Supercomputing Centre (NSCC)**,<sup>200</sup> which was established in 2015 to manage Singapore's national petascale facilities and high-performance computing (HPC) resources. As a shared resource, NSCC's technologies are used to support the research needs of the public and private sectors, including research institutes, institutes of higher learning, government agencies and companies. This “shared resource approach” undergirds Singapore's approach towards supercomputer power and access to quantum resources, with many organisations from the private, public, and research/academic sector in multilateral partnerships to explore quantum computing together.

- The **NSCC Singapore** itself has integrated quantum-classical hybrid computing capabilities. CQT researchers have made significant contributions to satellite-based QKD, having

---

<sup>191</sup> <https://www.nrf.gov.sg/programmes/nri/>

<sup>192</sup> <https://www.nrf.gov.sg/>

<sup>193</sup> <https://nqo.sg/programmes/qep/>

<sup>194</sup> <https://nqo.sg/nqs/>

<sup>195</sup> [https://www.pmo.gov.sg/newsroom/dpm-heng-swee-keat-at-the-asia-tech-x-singapore-2024-opening-ceremony/?trk=public\\_post\\_comment-text](https://www.pmo.gov.sg/newsroom/dpm-heng-swee-keat-at-the-asia-tech-x-singapore-2024-opening-ceremony/?trk=public_post_comment-text)

<sup>196</sup> <https://www.cqt.sg/>

<sup>197</sup> <https://nqo.sg/programmes/>

<sup>198</sup> <https://nqo.sg/>

<sup>199</sup> <https://nqo.sg/nqs/>

<sup>200</sup> <https://www.nscg.sg/>

demonstrated space-to-ground quantum key exchange from the SpooQySat nano satellite launched by CQT in 2019.<sup>201</sup>

- The **Singapore University of Technology and Design (SUTD)** has a quantum security research programme focused on cryptographic protocol design and quantum network security.
- A group of quantum scientists from various academic institutions established the **National Quantum Safe Network (NQSN)**,<sup>202</sup> which aims to deploy commercial quantum-safe technologies for trials with government agencies and private companies; to conduct in-depth evaluation of security systems; and to develop guidelines to support companies in adopting such technologies. The NQSN is led by the **Centre for Quantum Technologies (CQT)**, National University of Singapore (NUS) and the **School of Physical and Mathematical Sciences (SPMS)**, Nanyang Technological University (NTU), with collaboration from the **Fraunhofer Singapore Research Centre @NTU (FSR@NTU)**.<sup>203</sup> The NQSN is also supported by the NRF through its Quantum Engineering Programme, which focuses on translating quantum science into solutions for addressing real-world challenges.<sup>204</sup>
- In 2023, the **NQSN+ network**<sup>205</sup> was launched, and has been supporting network operators to deploy quantum-safe networks in Singapore and enable businesses easy access to quantum-safe solutions that safeguard their critical data. The NQSN+ is a deployment and industry-access initiative, and has on-boarded two network operators, Singtel and SPTel, together with SpeQtral. Each network operator has been tasked to build a Singapore-wide, interoperable quantum-safe network that can serve all businesses.
- In addition, the **NQSN+** will work towards integration with quantum-ready networks from like-minded countries, allowing enterprises to deploy quantum-safe solutions across global markets.
- **NQSN** is also chairing the **Quantum Communication Networks Task Force (QCNTF)**<sup>206</sup> under the IMDA's Telecommunications Standards Advisory Committee (TSAC).<sup>207</sup>

## PQC regulations and requirements and roadmaps

Singapore has been steadily releasing PQC technical and regulatory guidance for the community. The Cyber Security Agency of Singapore (CSA) first published a Quantum-Safe Security guidelines in 2021, which was then updated in 2024, culminating in the current guidance documents released in Oct 2025: the *Quantum-Safe Handbook* and *Quantum Readiness Index*.<sup>208</sup> These have been released as live documents, and the CSA continues to update them to sharpen technical guidance and key messages, with most recent updates being released on 16 July 2026.<sup>209</sup>

- **Quantum Safe Handbook.**<sup>210</sup> This provides guidance for organisations, in particular Critical Information Infrastructure (CII) owners and government agencies, in preparing for the

---

<sup>201</sup> <https://news.nus.edu.sg/singapore-nanosatellite-developed-by-cqt-goes-into-orbit/>

<sup>202</sup> <https://nqsn.sg/index.html#About-NQSN>

<sup>203</sup> <https://nqsn.sg/index.html#About-NQSN>

<sup>204</sup> <https://nqsn.sg/index.html#About-NQSN>

<sup>205</sup> <https://www.imda.gov.sg/about-imda/emerging-technologies-and-research/quantum-safe-technologies>

<sup>206</sup> <https://quantumlab.org>

<sup>207</sup> <https://nqsn.sg/index.html#About-NQSN>

<sup>208</sup> <https://www.imda.gov.sg/about-imda/emerging-technologies-and-research/quantum-safe-technologies>

<sup>209</sup> <https://www.csa.gov.sg/resources/publications/quantum-safe-handbook-and-quantum-readiness-index>

<sup>210</sup> [https://isomer-user-content.bv.gov.sg/36/11227d39-4350-4ded-9046-d62f99f561ab/Draft%20for%20Public%20Consultation%20-%20Quantum-Safe%20Handbook%20\(Oct%202025\).pdf](https://isomer-user-content.bv.gov.sg/36/11227d39-4350-4ded-9046-d62f99f561ab/Draft%20for%20Public%20Consultation%20-%20Quantum-Safe%20Handbook%20(Oct%202025).pdf)

quantum-safe transition. It explains what is at stake, highlights key areas of focus, and sets out practical considerations and resources for organisations to begin building readiness.

- **Quantum Readiness Index.**<sup>211</sup> A self-assessment questionnaire that complements the Quantum-Safe Handbook. The QRI allows organisations to understand their levels of readiness and enables system owners and security practitioners to prioritise quantum-safe migration action areas. It also facilitates conversations with senior management and decision makers about the state of readiness to address quantum threat and can be used to seek buy-in on the recommended steps to strengthen their readiness. The QRI was developed in consultation with experts from the industry.

*Standards Development.* IMDA released the RS QKDN in Jun 2023, the Reference Specification for Quantum Key Distribution Networks,<sup>212</sup> a foundational specification for QKD network deployment and interoperability. Singapore also takes part in international quantum security standards development through participation and referencing across various international standards bodies, e.g. referencing and aligning with NIST outputs<sup>213</sup>, ISO/IEC JTC 1/SC 27, ITU-T, and ETSI etc. and engaging on international standards discussions with other dialogue partners such as France, the United Kingdom, Australia, Japan, and the Netherlands.

## Critical Information Infrastructure (CII) Considerations

Singapore's Critical Information Infrastructure protection framework is established under the Cybersecurity Act 2018,<sup>214</sup> which designates eleven CII sectors: government, security and emergency, healthcare, telecommunications, banking and finance, energy, water, transportation, maritime, aviation, and media. CII owners are subject to mandatory cybersecurity audits, incident reporting requirements, and codes of practice issued by CSA. While it does not explicitly mention quantum computing/the quantum threat, the CSA released the (abovementioned) Quantum-Safe Handbook and Quantum Readiness Index to address quantum computing cybersecurity concerns.

Separately, Singapore's National AI Strategy 2.0 (2023)<sup>215</sup> explicitly identifies quantum-safe AI infrastructure as a priority.

*Financial Sector.* Specific to sectors, the financial regulator, the Monetary Authority of Singapore (MAS), is among the most proactive financial sector regulators globally on quantum risk. In February 2024, MAS published MAS/TCRS/2024/01: Advisory on Addressing the Cybersecurity Risks Associated with Quantum<sup>216</sup> which highlights the measures that financial institutions should consider as part of their quantum transition efforts.

MAS is aiming for financial institutions to achieve quantum resilience before the end of this decade,<sup>217</sup> and will next issue a set of supervisory expectations in late 2026 with clear expectations, milestones and timelines for financial institutions' migration towards quantum resilience. Progressive timelines will be set for financial institutions to establish an inventory of their cryptographic assets, develop a prioritisation of the migration of vulnerable assets to quantum-resilient solutions, and build technical capabilities and governance frameworks to support a quantum-safe migration.

<sup>211</sup> [https://isomer-user-content.by.gov.sg/36/949031c3-6734-4d33-985e-71331fa8ade4/Draft%20for%20Public%20Consultation%20-%20Quantum%20Readiness%20Index%20\(Oct%202025\).pdf](https://isomer-user-content.by.gov.sg/36/949031c3-6734-4d33-985e-71331fa8ade4/Draft%20for%20Public%20Consultation%20-%20Quantum%20Readiness%20Index%20(Oct%202025).pdf)

<sup>212</sup> <https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/telecommunication-and-security-standards/reference-standards>

<sup>213</sup> [https://isomer-user-content.by.gov.sg/36/11227d39-4350-4ded-9046-d62f99f561ab/Draft%20for%20Public%20Consultation%20-%20Quantum-Safe%20Handbook%20\(Oct%202025\).pdf](https://isomer-user-content.by.gov.sg/36/11227d39-4350-4ded-9046-d62f99f561ab/Draft%20for%20Public%20Consultation%20-%20Quantum-Safe%20Handbook%20(Oct%202025).pdf)

<sup>214</sup> <https://www.csa.gov.sg/legislation/cybersecurity-act/>

<sup>215</sup> <https://www.smartnation.gov.sg/initiatives/national-ai-strategy/>

<sup>216</sup> <https://www.mas.gov.sg/regulation/circulars/advisory-on-addressing-the-cybersecurity-risks-associated-with-quantum>

<sup>217</sup> <https://www.mas.gov.sg/news/speeches/2026/md-remarks-for-mas-ar-2025-2026>

In anticipation of the future threat posed by quantum-powered decryption, MAS has conducted trials to study the viability of quantum-safe solutions for adoption in financial services.

- In November 2024, MAS and Banque de France announced the successful completion of a joint experiment using PQC to secure international electronic communications. A technical report which details the results and takeaways from the experiment was published in November 2024.<sup>218</sup>
- In July 2025, MAS announced the successful completion of a QKD sandbox, conducted in collaboration with several banks and technology partners. This sandbox trialled QKD for securing sensitive financial communications. A technical report detailing the results and takeaways was published in September 2025.<sup>219</sup>

To support quantum innovation in financial services, MAS has established a Quantum Computing Programme<sup>220</sup> to build ecosystem capabilities and explore how financial institutions can leverage the technology for meaningful use cases. In addition, MAS has committed up to SGD 100 million (USD 79 million) to support quantum and AI capabilities in the financial sector<sup>221</sup>, through the FSTI Quantum Track grant scheme (FTSI 3.0).<sup>222</sup>

*Transport and Logistics.* Singapore's port infrastructure is one of the world's busiest ports and has been working together with private operators to trial quantum computing in traffic optimisation tests.<sup>223</sup> The initial tests started in 2022, and looked into three areas:

- Berth scheduling - assigning vessels to available berths in a way that minimises overall delays while maximising utilisation.
- Yard crane scheduling - reducing “dead time” in crane operations by optimising task sequences.
- Container reshuffling - minimising unnecessary container relocations while enabling faster access to outbound freight.

## Operational readiness/ deadlines for implementation

Singapore released formal guidance on migration dates for Critical Information Infrastructure in the Quantum-Safe Handbook (July 2026). This sets out three milestones, to submit migration plans by 31 March 2027, incorporate quantum-safe considerations into new CII procurements from 1 January 2028, and complete quantum-safe migration for CIIs by 31 December 2031.<sup>224</sup>

## Quantum in Singapore: Summary

### Opportunities

- Long, coordinated institutional build-out since 2007 (CQT, A\*STAR QTE, National Quantum Office, National Quantum Strategy 2024) shows sustained strategic commitment.
- SGD 200m (~USD 150m) Quantum Engineering Programme funds an integrated quantum research agenda together, binding computing, communications, and quantum-safe cryptography research.

<sup>218</sup> <https://www.mas.gov.sg/news/media-releases/2024/bdf-and-mas-conduct-groundbreaking-post-quantum-cryptography-experiment>

<sup>219</sup> <https://www.mas.gov.sg/news/media-releases/2025/mas-and-industry-partners-publish-technical-report-on-proof-of-concept-sandbox>

<sup>220</sup> <https://www.mas.gov.sg/schemes-and-initiatives/quantum-computing-programme>

<sup>221</sup> [https://www.mas.gov.sg/news/media-releases/2024/mas-commits-up-to-s\\$100-million-to-support-quantum-and-artificial-intelligence-capabilities](https://www.mas.gov.sg/news/media-releases/2024/mas-commits-up-to-s$100-million-to-support-quantum-and-artificial-intelligence-capabilities)

<sup>222</sup> <https://www.mas.gov.sg/schemes-and-initiatives/fsti-quantum-track>

<sup>223</sup> <https://www.quantumlogistics.com/articles/2022/7/02172022>

<sup>224</sup> <https://www.csa.gov.sg/resources/publications/quantum-safe-handbook-and-quantum-readiness-index/>

- The NQSN+ initiative is actively building commercial nationwide quantum-safe networks with operators.
- MAS is among the most proactive financial regulators globally on quantum risk, backed by a dedicated Quantum Computing Programme and up to SGD 100m (~USD 79m) in funding.
- Practical CII trials already underway, including banking sector QKD proof-of-concept with Singapore banks, and port-logistics quantum optimisation.
- Strong international standards engagement (NIST, ISO/IEC, ITU-T, ETSI) plus bilateral cooperation with the UK, France, Australia, Japan, and Netherlands.

## Risks

- No mandatory PQC migration deadline exists yet - the government has explicitly described a "risk-oriented," non-mandated approach.
- Readiness varies by sector - finance is advanced, but broader enterprise adoption outside CII sectors is less clear.
- Success of the NQSN+ rollout depends on continued collaboration among a small number of network operators, concentrating execution risk.

## South Korea

### Existing quantum R&D and investment

*Government quantum coordination.* South Korea has committed to expanding its position in global quantum technology development through national research and innovation programmes coordinated by the Ministry of Science and ICT (MSIT). The government announced a long-term **National Quantum Strategy** to support research in quantum technologies in 2023,<sup>225</sup> which was then updated in January 2026 with the **First Comprehensive Plan for Promotion of Quantum Science and Technology and Quantum Industry**.<sup>226</sup>

Figure 10: South Korea's 2026 First Comprehensive Plan for Promotion of Quantum Science and Technology and Quantum Industry



Source: <https://www.msit.go.kr/bbs/view.do?sCode=user&mId=307&mPid=208&bbsSeqNo=94&nttSeqNo=3186815>

The 2026 plan<sup>227</sup> highlights the government's plans to focus on five key sectors for the quantum industry, and create regional industrial clusters for the following sectors: (1) quantum computing, (2) communications, (3) sensors, (4) materials, parts, and equipment, and (5) algorithms. These clusters would create a self-sustaining quantum industry ecosystem, and would converge the industry, academia, and research institutes.

<sup>225</sup> [https://quantuminkorea.org/wp-content/uploads/2024/06/Koreas-National-Quantum-Strategy-2023\\_c.pdf](https://quantuminkorea.org/wp-content/uploads/2024/06/Koreas-National-Quantum-Strategy-2023_c.pdf), <https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&nttSeqNo=828&searchOpt=ALL&bbsSeqNo=42&mId=4&mPid=2>, [https://quantuminkorea.org/wp-content/uploads/2024/06/Koreas-National-Quantum-Strategy-2023\\_c.pdf](https://quantuminkorea.org/wp-content/uploads/2024/06/Koreas-National-Quantum-Strategy-2023_c.pdf), <https://www.msit.go.kr/bbs/view.do?sCode=user&mId=84&mPid=83&bbsSeqNo=65&nttSeqNo=3017410>

<sup>226</sup> <https://www.msit.go.kr/bbs/view.do?sCode=user&mId=307&mPid=208&bbsSeqNo=94&nttSeqNo=3186815>

<sup>227</sup> <https://nsp.nanet.go.kr/plan/main/detail.do?nationalPlanControlNo=PLAN0000059917>

The 2026 plan updates the 2023 strategy, which aimed to grow South Korea's global quantum market share from 1.8% to 10% and to develop a domestically built 1,000-qubit quantum computer, underpinned by the **Quantum Technology Promotion Act 2024**, which provides a statutory mandate for funding programs, R&D investment, and international cooperation.<sup>228</sup> The strategy targeted combined public-private investment of KRW 3 trillion (USD 2.3 billion) by 2035, with the government contributing 80% of that total.<sup>229</sup>

In 2025, South Korea also established the **Quantum Strategy Committee**,<sup>230</sup> chaired by the Prime Minister's Office, the same year that the country's budget allocated KRW 198 billion (USD 134 million) to computing, communication, and sensing, with support from the Korea Research Institute of Standards and Science (KRISS) and other institutions.<sup>231</sup>

Local provincial governments are also establishing initiatives to support quantum computing development. For example, the Seoul Metropolitan Government (SMG) has plans to establish a *Seoul Quantum Technology Industry Mid- to Long-Term Development Strategy (Five-Year Plan)* under the *Seoul Metropolitan Government Ordinance on the Promotion of the Quantum Industry 2025* to create a more systematic foundation for the industry.<sup>232</sup> The SMG has also established the **Seoul Quantum Hub** (tentative name) at Yangjae, which will work with the **Seoul AI Hub** to develop quantum and AI-integrated application services and fostering quantum technology-based emerging industries.

*Academic and Technical Quantum Computing Research.* South Korea's quantum research ecosystem is vested in its universities and related labs, who have strong histories of conducting R&D on quantum communications and developing QKD technologies, such as:<sup>233</sup>

- Korea Advanced Institute of Science & Technology (KAIST) Graduate School of Quantum Science and Technology,<sup>234</sup>
- Seoul National University's Quantum Information and Quantum Computing Lab,<sup>235</sup>
- Electronics and Telecommunications Research Institute (ETRI) Quantum Technology Research Division,<sup>236</sup>
- Yonsei University Institute of Quantum Information Technology.<sup>237</sup>

*Private Sector Participation.* In addition to the academic and technical sectors, South Korea's private sector also has significant experience and history in developing quantum technology and research programmes.

- Yonsei University built Korea's first physical quantum computer with a 127-Qubit Eagle Processor (IBM's System One) in 2024,<sup>238</sup> and Chungbuk National University (CBNU) installed the first IBM quantum system on 13 May 2025.<sup>239</sup>

<sup>228</sup> <https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&bbsSeqNo=42&nttSeqNo=1053&searchOpt=ALL>

<sup>229</sup> [https://quantuminkorea.org/wp-content/uploads/2024/06/Koreas-National-Quantum-Strategy-2023\\_c.pdf](https://quantuminkorea.org/wp-content/uploads/2024/06/Koreas-National-Quantum-Strategy-2023_c.pdf)

<sup>230</sup> <https://thequantuminsider.com/2025/01/09/south-korea-to-form-quantum-strategy-committee/>

<sup>231</sup> [https://koreapoint.org/articles/article\\_detail.php?topic\\_idx=176&idx=442&start=](https://koreapoint.org/articles/article_detail.php?topic_idx=176&idx=442&start=)

<sup>232</sup> <https://english.seoul.go.kr/seoul-to-foster-quantum-technology-in-conjunction-with-ai-bio-and-finance/>

<sup>233</sup> <https://postquantum.com/quantum-computing/quantum-south-korea/>

<sup>234</sup> <https://quantum.kaist.ac.kr/>

<sup>235</sup> <https://quicql.snu.ac.kr/>

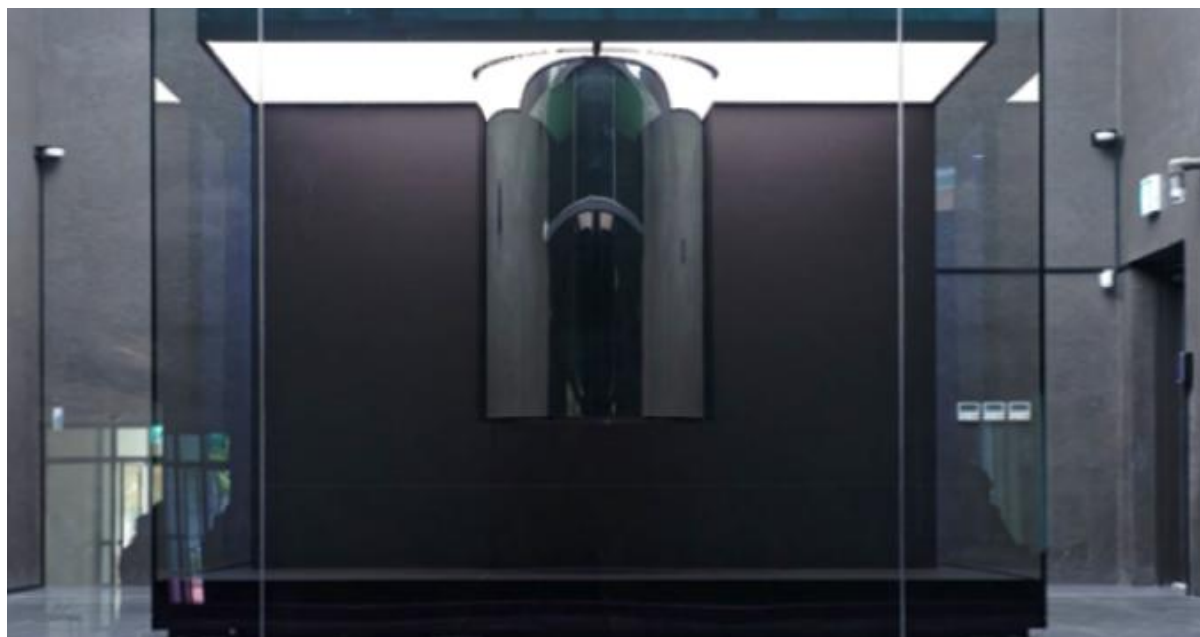
<sup>236</sup> [https://www.etri.re.kr/eng/sub6/sub6\\_01020101.etri;jsessionid=376521345F9E5D1A75115C5D18D09C6C?departCode=172&departInfoCode=327](https://www.etri.re.kr/eng/sub6/sub6_01020101.etri;jsessionid=376521345F9E5D1A75115C5D18D09C6C?departCode=172&departInfoCode=327)

<sup>237</sup> [https://devcms.yonsei.ac.kr/iqit\\_e/index.do](https://devcms.yonsei.ac.kr/iqit_e/index.do)

<sup>238</sup> <https://qinitiative.yonsei.ac.kr/en/infrastructure?ckattempt=1>

<sup>239</sup> <https://meetqim.com/press-releases/qims-first-quantum-computer-in-asia-pacific-goes-online-set-to-open-office-in-seoul/>

Figure 11: Yonsei University's 127-Qubit Quantum Computer on campus



Source: <https://qinitiative.yonsei.ac.kr/en/infrastructure?ckattempt=1>

- Samsung Electronics and Samsung Semiconductors have worked on quantum computing and security, as well as on bringing quantum-safe mobile security technologies to consumers, such as the company's Samsung Knox Matrix, which provides Post-Quantum Enhanced Data Protection (EDP) with post-quantum cryptography that follows cryptographic standards established by the Korea National Institute of Standards.<sup>240</sup> Samsung has also released the Samsung Galaxy Quantum 6 smartphone,<sup>241</sup> which they highlight as the latest generation quantum-secure mobile device.
- Telco SK Telecom (SKT) established Quantum Random Number Generator (QRNG) with Thales<sup>242</sup> for subscriber authentication in 2019,<sup>243</sup> and in 2023 started offering Quantum-Safe-as-a-Service (QaaS) subscription for secure networking.<sup>244</sup> SKT has also partnered with ID Quantique to deploy quantum secure communications infrastructure in Korea and internationally.<sup>245</sup>
- LG Uplus also maintains a robust quantum technology research programme, contributing technical proposals for (1) a PQC-based software defined network (SDN) interface and (2) SOLMAE, an NTRU<sup>246</sup> lattice-based digital signature scheme, both of which have been officially adopted as domestic standards by the Telecommunications Technology Association (TTA).<sup>247</sup>

<sup>240</sup> <https://news.samsung.com/sg/the-first-step-towards-a-quantum-safe-future-with-samsung-knox>, <https://news.samsung.com/global/the-first-step-to-a-quantum-safe-future-with-samsung-knox>

<sup>241</sup> <https://www.idquantique.com/random-number-generation/qrng-use-cases/samsung-qrng-use-case/>

<sup>242</sup> <https://www.thalesgroup.com/en/search/enterprise/mobile-communications/thales-and-sk-telecom-unveil-innovative-post-quantum>

<sup>243</sup> [https://www.sktelecom.com/en/press/press\\_detail.do?idx=1385](https://www.sktelecom.com/en/press/press_detail.do?idx=1385)

<sup>244</sup> <https://www.idquantique.com/sk-telecom-launches-a-brand-new-subscription-based-quantum-safe-as-a-service-offering/>

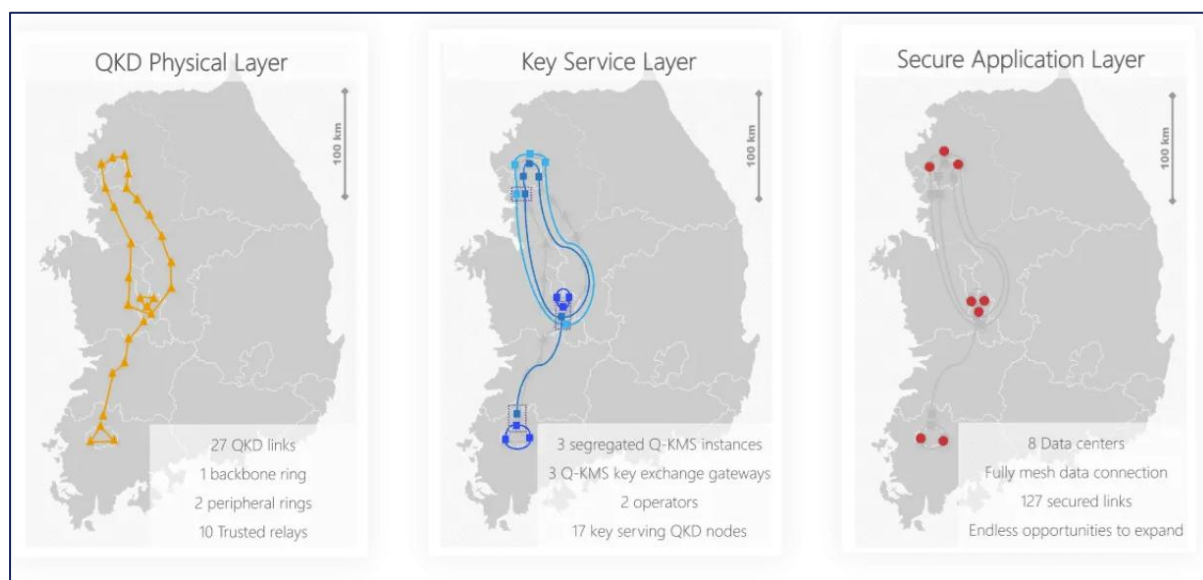
<sup>245</sup> <https://www.idquantique.com/idq-and-sk-telecom-celebrate-5-years-of-collaboration/>

<sup>246</sup> <https://www.ntru.org/it/hps98.pdf>

<sup>247</sup> <https://www.businesskorea.co.kr/news/articleView.html?idxno=259872> ; <https://www.tta.or.kr/eng>

On the QKD side, the **National QKD Network** was developed by ID Quantique and SK Broadband and completed in 2022.<sup>248</sup> It connects 48 government departments across an 800 km optical fibre backbone, making it one of the largest quantum-encrypted government networks outside China.<sup>249</sup>

Figure 12: South Korea's National QKD Network's Data Centres with 16 Encryption Points Establishing up to 127 Secure Links



Source: <https://www.idquantique.com/quantum-safe-security/nation-wide-quantum-safe-key-distribution-network-in-south-korea/>

## PQC regulations and requirements and roadmaps

South Korea is known for having Korea-specific technical requirements such as its HWP/HWPX word processing document format,<sup>250</sup> and its cryptographic certification programme is no different. Its primary government cryptographic certification framework is the **Korea Cryptographic Module Validation Program (KCMVP)**, operated by the National Intelligence Service (NIS) with technical support from the National Security Research Institute (NSR).<sup>251</sup>

The KCMVP or 한국형 암호모듈 검증제도 (Hanguk-hyeong Amho Module Geomjeung Jedo) can also be directly translated as “Korean Cryptographic Module Validation Program”, and sometimes is also known as the 암호모듈 검증제도 (Amho Module Geomjeung Jedo) or “Cryptographic Module Validation Program”.<sup>252</sup> Designed to test and affirm how critical components comply with security and implementation suitability, the KCMVP functions similarly to the US FIPS 140 program by validating cryptographic modules used in government systems and critical infrastructure. The framework is being updated to accommodate PQC standards and future algorithm validation requirements.

In parallel, the NIS and NSR established the Korean Post-Quantum Cryptography (KpqC) research group, which started running the Korean PQC competition (KpqC) in 2021.<sup>253</sup> Seven Key Encapsulation Mechanism (KEM) candidates and nine digital signature candidates were selected in

<sup>248</sup> <https://www.idquantique.com/quantum-safe-security/nation-wide-quantum-safe-key-distribution-network-in-south-korea/>

<sup>249</sup> <https://www.idquantique.com/quantum-safe-security/nation-wide-quantum-safe-key-distribution-network-in-south-korea/>

<sup>250</sup> <https://www.saemangeum.go.kr/sda/en/content.do?key=2309260362001>

<sup>251</sup> <https://www.lawwin.co.kr/mokpo/knowledgedetail?index=7281>

<sup>252</sup> <https://www.lawwin.co.kr/incheon/knowledgedetail?index=7281>

<sup>253</sup> <https://pqshield.com/south-korea-announces-winners-of-kpqc-competition/>

the first round in November 2022,<sup>254</sup> and in December 2023, four KEM algorithms and four digital signature algorithms advanced to the second round.<sup>255</sup> The final winners of the KpqC competition were announced in January 2025: digital signatures **HAETAE** and **AIMer**; PKE/KEMs **SMAUG-T** and **NTRU+**.<sup>256</sup>

### Digital Signatures

- **HAETAE** (Lattice-based Signature) is a close variant of the ML-DSA (Module-Lattice-Based Digital Signature Algorithm) from NIST's FIPS 204<sup>257</sup> that uses a different rejection sampling technique. Analysts have identified it as being more efficient as it is more complex and more efficient, and results in more compact signatures.
- Industry observers highlight that the **AIMer** digital signature algorithm (Symmetric-based Signature) has a larger signature size than NIST-standardised ML-DSA, but while it runs slower than lattice-based schemes, its performance is comparable with SLH-DSA (Stateless Hash-Based Digital Signature Algorithm) from NIST's FIPS 205.<sup>258</sup>
- Both HAETAE and AIMer were selected in July 2023 for the first round of NIST's Post-Quantum Cryptography: Additional Digital Signature Schemes,<sup>259</sup> although neither advanced to the Oct 2024 second round.<sup>260</sup>

### PKE/KEMs

- **SMAUG-T**. This KEM is similar to ML-KEM (Kyber) from NIST FIPS 203<sup>261</sup>, using similar technical assumptions, and observers have noted it performs similarly.<sup>262</sup>
- **NTRU+**. Observers have noted that *NTRU was originally a NIST finalist, but was not selected as a KEM, being surpassed by ML-KEM (Kyber) during the standardisation project. NTRU+ can be similarly efficient but can also mean more complicated implementations.*<sup>263</sup>

Cybersecurity guidance and implementation support are provided by the Korea Internet and Security Agency (KISA) under MSIT.<sup>264</sup> South Korea's National Cybersecurity Strategy 2023 also identifies quantum computing as a significant future security challenge and calls for the development of national capabilities to address emerging cryptographic risks.<sup>265</sup>

## Critical Information Infrastructure (CII) Considerations

In Korea, CII responsibility is divided between the NIS supporting the public sector and MSIT overseeing the private sector,<sup>266</sup> with KISA operating the Korean National Computer Emergency Response Team (KNCERT) and conducting mandatory annual vulnerability assessments across designated CII operators.<sup>267</sup>

South Korea's digital economy is highly integrated and concentrated among several large conglomerates including Samsung Group, SK Group, LG Group, and Hyundai Motor Group.<sup>268</sup> This

<sup>254</sup> <https://kpgc.or.kr/competition.html>

<sup>255</sup> [https://kpgc.or.kr/competition\\_02.html](https://kpgc.or.kr/competition_02.html)

<sup>256</sup> <https://pqshield.com/south-korea-announces-winners-of-kpgc-competition>

<sup>257</sup> <https://csrc.nist.gov/pubs/fips/204/final>

<sup>258</sup> <https://csrc.nist.gov/pubs/fips/205/final>

<sup>259</sup> <https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures>

<sup>260</sup> <https://csrc.nist.gov/pubs/ir/8528/final>

<sup>261</sup> <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.203.pdf>

<sup>262</sup> <https://pqshield.com/south-korea-announces-winners-of-kpgc-competition>

<sup>263</sup> <https://pqshield.com/south-korea-announces-winners-of-kpgc-competition>

<sup>264</sup> <https://www.kisa.or.kr/EN>

<sup>265</sup> [https://ccdcoc.org/uploads/2018/10/South-Korea\\_English-National-Cybersecurity-Strategy-03-April-2019\\_English-1.pdf](https://ccdcoc.org/uploads/2018/10/South-Korea_English-National-Cybersecurity-Strategy-03-April-2019_English-1.pdf)

<sup>266</sup> <https://ccdcoc.org/uploads/2022/12/ROK-Country-report.pdf>

<sup>267</sup> <https://www.first.org/members/teams/kn-cert>

<sup>268</sup> <https://www.koreatimes.co.kr/business/banking-finance/20241009/south-koreas-major-conglomerates-dominate-40-percent-of-gdp-in-2023>

interdependent structure of domestic firms means that cryptographic transitions implemented by a small number of firms can influence a large share of national economic activity.

For example, in South Korea's telco sector, there is high 5G penetration, which therefore represents simultaneous opportunity and challenge, as 5G specifications often depend on ECC-based security standards that would require migration to a PQC system. KT, SK Telecom, and LG Uplus are all evaluating PQC migration pathways for their core network security systems, and any one - or all private companies - deciding to move into a PQC-ready network could possibly spark off a positive domino effect, resulting in a PQC-ready telco sector for South Korea.<sup>269</sup>

- KT announced in Feb 2026 that it has developed Korea's fastest quantum key distribution system, capable of generating 300,000 encryption keys per second.<sup>270</sup> These keys cannot be duplicated, effectively blocking eavesdropping attempts on physical communication lines.

In the financial sector, there are several agencies performing regulatory and operational functions. Regulations are led by the Financial Services Commission (FSC)<sup>271</sup> with the South Korea Financial Supervisory Service (FSS)<sup>272</sup> performing inspections/audit and oversight functions. The Korea Financial Telecommunications and Clearings Institute (KFTC) operates core interbank settlement and payment systems,<sup>273</sup> while the Korea Securities Depository (KSD)<sup>274</sup> manages the custody and settlement of Korean securities. None of these organisations appear to address quantum initiatives as yet.

## Operational readiness/ deadlines for implementation

South Korea's master plan for migration to PQC was announced by MSIT and NIS on 12 Jul 2023 (see figure below), with the following deadlines:<sup>275</sup>

- 2024 - sector-specific PQC migration action plan will be established
- 2026 to 2035 - an integrated migration support centre will be established
- 2029 - PQC cryptography standards will be selected
- 2028 to 2032 - public infrastructure will start migration to PQC

Central to this roadmap is the Korea PQC competition (see KpqC above) to develop sovereign PQC standard algorithms. Subsequent phases will cover further work on identifying and selecting PQC standardisation, cryptographic transformation technologies, and pilot implementations in critical sectors including finance, healthcare, and government services, ahead of the 2035 transition deadline.<sup>276</sup>

In addition, in Feb 2025, the MSIT's Information Security Planning Division released a note that the first phase of the country's quantum-resistant cryptography pilot transition support had completed, in "Taking the First Step Toward a Major Transformation of the National Cryptosystem to Prepare for Quantum Era Threats".<sup>277</sup> The news release noted that the government was in the middle of plans to **transition domestic cryptographic systems to quantum-resistant cryptography by 2035**, prioritising healthcare, national defence, and finance sectors from 2025 to 2028.

<sup>269</sup> <https://postquantum.com/quantum-computing/quantum-south-korea/>

<sup>270</sup> <https://www.koreaherald.com/article/10668527>

<sup>271</sup> <https://www.fsc.go.kr/index>

<sup>272</sup> <https://www.fss.or.kr/>

<sup>273</sup> <https://eng.kftc.or.kr/home/main>

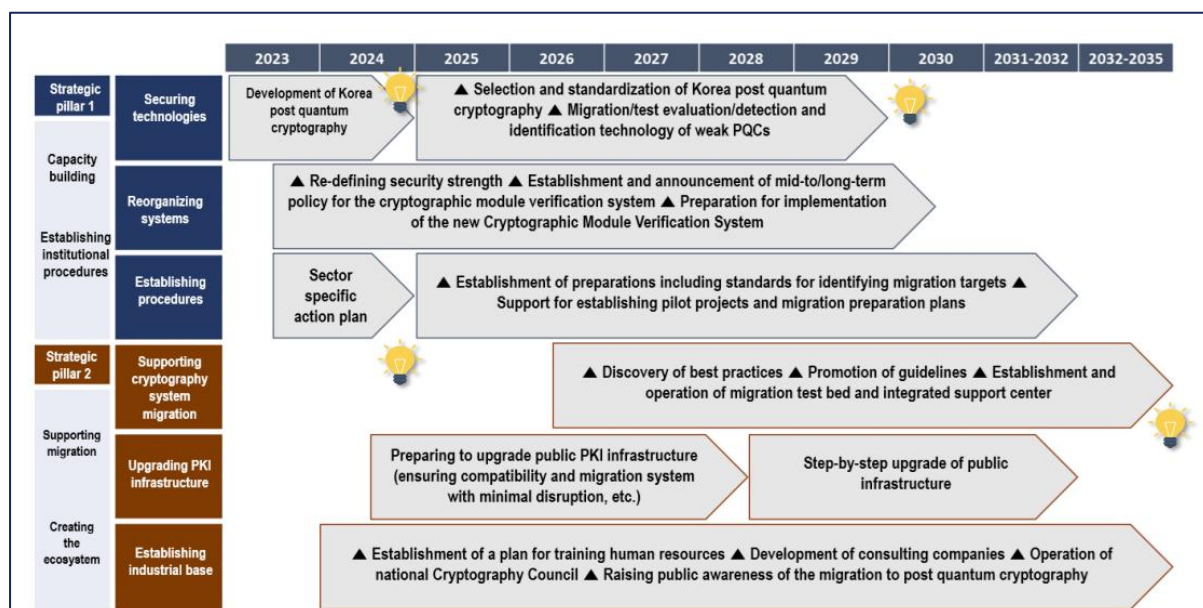
<sup>274</sup> <https://www.ksd.or.kr/en/>

<sup>275</sup> [https://www.itu.int/en/ITU-T/academia/kaleidoscope/2024/Documents/1st\\_author\\_corner/ITU%20Kaleidoscope%202024%20-%20keynote%20-%20f.pdf](https://www.itu.int/en/ITU-T/academia/kaleidoscope/2024/Documents/1st_author_corner/ITU%20Kaleidoscope%202024%20-%20keynote%20-%20f.pdf)

<sup>276</sup> <https://d216w31g89z0j.cloudfront.net/site/2025s/abs/0183-FEOTP.pdf>

<sup>277</sup> <https://www.msit.go.kr/bbs/view.do?sCode=user&mId=307&mPid=208&pageIndex=&bbsSeqNo=94&nttSeqNo=3185512&searchOpt=ALL&searchTxt=>

Figure 13: South Korea Master Plan for PQC Migration



Source: [https://www.itu.int/en/ITU-T/academia/kaleidoscope/2024/Documents/1st\\_author\\_corner/ITU%20Kaleidoscope%202024%20-%20keynote%20-%20f.pdf](https://www.itu.int/en/ITU-T/academia/kaleidoscope/2024/Documents/1st_author_corner/ITU%20Kaleidoscope%202024%20-%20keynote%20-%20f.pdf)

## Quantum in South Korea: Summary

### Opportunities

- The National Quantum Strategy (2023) targets growing global market share from 1.8% to 10%, backed by the statutory Quantum Technology Promotion Act 2024. This is coupled with a substantial funding commitment - KRW 3 trillion (~USD 2.3bn) by 2035, 80% government-funded - with a dedicated Quantum Strategy Committee chaired by the PM's Office.
- Deep private-sector engagement suggest commercial maturity being pursued alongside research capabilities.
- Established 800km National QKD Network already connects 48 government departments - one of the largest such networks outside China.
- Clear, dated national migration roadmap (2024 sector plans, 2029 standards selection, 2028-2032 infrastructure migration, 2035 full transition) gives strong planning certainty.

### Risks

- Heavy economic concentration among a few conglomerates (Samsung, SK, LG, Hyundai) could mean crypto-transition delays have outsized national impact.
- Focus on local development of standards raises interoperability questions with global systems.
- 5G networks' dependence on ECC-based security creates a large, complex migration surface for telecoms.
- Key financial infrastructure bodies (KFTC, KSD) do not yet appear to have quantum-specific initiatives underway.

---

### Case Study: Taiwan Market Profile - Quantum-Safe Developments

Taiwan has been proactively preparing for the security implications of quantum computing, driven by its strategic position in global semiconductor supply chains and its close alignment with like-minded partners on cybersecurity and resilience. Its approach combines centralised public sector planning, strong academic cryptography capabilities, and early ecosystem efforts with international technology providers.

**At the policy level, Taiwan has established national quantum computing R&D coordination structures, including the Taiwan Quantum Program Office (TQPO) under the National Science and Technology Council (NSTC).**<sup>278</sup> The Ministry of Digital Affairs (MODA), through its Administration for Digital Industries (ADI), has also supported the development of Taiwan's PQC ecosystem and industry collaboration.<sup>279</sup> These efforts are increasingly being completed by practical migration guidance for regulated sectors and government systems.<sup>280</sup>

These national strategies frame quantum computing and quantum-safe capabilities as important elements of cybersecurity, digital resilience, supply chain security, and trusted data flows. Taiwan's policy direction increasingly recognises that PQC migration should be treated as a medium- to long-term programme involving governance, risk management, procurement, technical modernisation, and ecosystem development, rather than a purely technical upgrade.<sup>281</sup>

**On the technical side,** Taiwan's academic community, particularly the cryptography group at Academia Sinica's Institute of Information Science (IIS), has actively participated in international PQC standardisation efforts. Taiwan also hosted the PQCrypto 2025 international workshop in Taipei in April 2025.<sup>282</sup> This positions Taiwan as an economy with both theoretical PQC expertise and with the capacity to contribute to emerging global standards.<sup>283</sup>

**Market-wise,** Taiwan is taking steps to move from research to implementation. The Post-Quantum Cybersecurity Industry Alliance (PQC-CIA), established with support from the ADI, connects chip vendors, security firms, IP providers, and service companies around PQC-ready solutions. The alliance aims to foster collaboration among government, academia, and industry, and accelerate the development of relevant domestic technologies.<sup>284</sup>

Sector-specific implementation efforts are underway across multiple industries. In the semiconductor and supply chain sector, the Taiwan Quantum Security Industry Association (TQSA) and PQC-CIA signed an MOU with French embedded security firm Secure-IC in August 2024 to accelerate PQC adoption in semiconductor IP chip design.<sup>285</sup>

In the cloud and network sector, Chelpis and Gorilla Technology announced in May 2026 a collaboration to deploy quantum-safe SD-WAN solutions targeting government, finance, and AI infrastructure.<sup>286</sup>

In the financial sector, the Financial Supervisory Commission (FSC) released its Post-Quantum Cryptography Migration Reference Guide for the Financial Industry on 18 Jun 2026.<sup>287</sup> The Guide is intended to help financial institutions strengthen preparedness for quantum-related cryptographic risks through a risk-based and phased migration approach. The FSC proposes a phased migration approach. During 2026–2027, financial institutions are encouraged to establish governance arrangements, cryptographic inventory methodologies, cryptographic asset inventories, and

foundational crypto-agility capabilities. During 2027–2029, the focus shifts to pilot validation, infrastructure upgrades, and joint testing mechanisms. Through 2035, financial institutions are expected to prioritize the migration of high-risk and critical systems and progressively expand migration scenarios.

For the public sector, the Administration for Cyber Security (ACS) under MODA has stated that it plans to publish a Government Agency Post-Quantum Cryptography Migration Policy by the end of 2026.<sup>288</sup> The policy is intended to guide the overall migration timetable for government agencies and align Taiwan’s approach with relevant international practices, including those of the United States and the European Union.

**Going forward**, key priorities for Taiwan’s PQC readiness are likely to include:

- Implementing the FSC’s financial-sector PQC migration guidance, including governance, cryptographic inventories, crypto-agility, supplier readiness assessments, pilot testing, and ecosystem-level coordination;
- Publishing and operationalizing the planned Government Agency Post-Quantum Cryptography Migration Policy and accompanying practical reference handbook for public-sector entities by the end of 2026;
- Embedding PQC readiness, cryptographic agility, and relevant risk-management requirements into procurement, outsourcing, technical specifications, and supply-chain governance;
- Prioritizing high-risk and critical systems, particularly those that process sensitive data, depend on long-lived confidentiality, or support critical infrastructure and cross-organization interoperability; and
- Expanding pilot deployments and testing of hybrid cryptographic approaches, while maintaining interoperability with evolving international standards and trusted international partners.

<sup>278</sup> <https://qpf.org/taiwan-quantum-program-office/>

<sup>279</sup> <https://moda.gov.tw/en/ADI/news/latest-news/20440>

<sup>280</sup> <https://www.regulationasia.com/articles/taiwan-issues-landmark-post-quantum-cryptography-migration-guide>

<sup>281</sup> <https://amcham.com.tw/2025/06/2025-technology-position-paper/>

<sup>282</sup> <https://www.taiwannews.com.tw/news/5917785>

<sup>283</sup> <https://www.iis.sinica.edu.tw/en/page/ResearchOverview/KeyProjects/Post-QuantumCryptography.html>

<sup>284</sup> <https://moda.gov.tw/en/ADI/news/latest-news/17604>

<sup>285</sup> <https://www.secure-ic.com/news-and-events/news/secure-ic-signs-international-collaboration-with-taiwan-quantum-safe-association-and-pqc-cja/>

<sup>286</sup> <https://investors.gorilla-technology.com/gorilla-technology-and-chelpis-accelerate-quantum-safe-sd-wan-to-global-market-deployment-securing-sovereign-infrastructure-for-the-post-quantum-era/>

<sup>287</sup> [https://www.fsc.gov.tw/en/home.jsp?id=54&parentpath=0.2&mcustomize=multimessage\\_view.jsp&dataserno=202606300001&dtable=News](https://www.fsc.gov.tw/en/home.jsp?id=54&parentpath=0.2&mcustomize=multimessage_view.jsp&dataserno=202606300001&dtable=News)

<sup>288</sup> <https://moda.gov.tw/ACS/press/report/20430>

## Quantum Readiness in APAC – Comparative Summary Chart

| Category                        | Australia                                                                                                                                                                                                                                           | China                                                                                                                                                                                                  | India                                                                                                                                                                                                 | Japan                                                                                                                                                                                                                                                                                                                      | Singapore                                                                                                                                                          | South Korea                                                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>National Quantum Policy</b>  | National Quantum Strategy (3 May 2023)                                                                                                                                                                                                              | No single named strategy, but quantum is designated a national strategic technology under the 15th Five-Year Plan (2026-2030).<br><br>Cryptography governed by the Cryptography Law (eff. 1 Jan 2020). | National Quantum Mission (NQM), announced April 2023.                                                                                                                                                 | Quantum Technology Innovation Strategy (2020), Vision for a Quantum Future Society (2022), Strategy for the Creation of Quantum Future Industries (2023).<br>Quantum also named one of six areas in the 7th Basic Plan for Science, Technology and Innovation.                                                             | National Quantum Strategy (2024), built on the National Research Infrastructure framework (2015).                                                                  | National Quantum Strategy (2023), updated as the First Comprehensive Plan for Promotion of Quantum Science and Technology and Quantum Industry (Jan 2026).<br>Statutory basis: Quantum Technology Promotion Act 2024.                                       |
| <b>Timeline/Deadline</b>        | No legislated PQC deadline. ASD's Information Security Manual (ISM) will stop approving traditional asymmetric cryptography after 2030. Approved PQC algorithms to be supported in newly procured cryptographic equipment and software by agencies. | No mandatory national PQC deadline. Dual-track "QKD+PQC" approach; SAC/TC 578 (national quantum standards body) approved March 2026.                                                                   | 3-milestone DST roadmap (Implementation of Quantum Safe Ecosystem in India, Feb 2026): CII by 2027/2028/2029; Enterprise by 2028/2030/2033. PQC Testing & Certification Program targeted by Dec 2026. | Full government-wide PQC transition pledged by 2035 (NCO Cybersecurity Strategy, Dec 2025). QKD deployment acceleration targeted ~2030; detailed roadmap due FY2026. CRYPTREC's "Guidelines" regarding PQC were drafted in fiscal year 2024, but they are scheduled to be revised during fiscal year 2026 (by March 2027). | Formal quantum safe migration guidance, including key migration milestones, was issued to CII Operatos in June 2026.                                               | MSIT/NIS Master Plan for PQC Migration (12 Jul 2023): 2024 sector plans → 2026–2035 migration support centre → 2029 standards selection → 2028–2032 infrastructure migration → full transition by 2035. Healthcare, defence, finance prioritised 2025–2028. |
| <b>Budget (Local &amp; USD)</b> | AUD 15bn (USD 10.5bn) National Reconstruction Fund, min. AUD 1bn (USD 0.75bn) ring-fenced for critical tech incl. quantum.                                                                                                                          | ~USD 15bn public investment across national/provincial programs.                                                                                                                                       | INR 6,000 crore (~USD 730 million) over 2023–2031.                                                                                                                                                    | JPY 43.4bn quantum budget FY2026 (up from JPY 36.1bn FY2025). Strategic goal: JPY 50 trillion (USD 315bn) in                                                                                                                                                                                                               | Close to SGD 300 million (USD 236 million) investment under the National Quantum Strategy. + up to SGD 100m (USD 79m) MAS FSTI Quantum Track for financial sector. | KRW 3 trillion (USD 2.3bn) combined public-private target by 2035 (80% govt-funded). KRW 198bn (USD 134m) allocated in 2025 for                                                                                                                             |

| Category                                | Australia                                                                                                                                                                                                                                                                                                                                            | China                                                                                                                                                                                                                                                       | India                                                                                                                                                                                                                                  | Japan                                                                                                                                                                                                                                                                                                 | Singapore                                                                                                                                                                                                                                                                                           | South Korea                                                                                                                                                                                                                     |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                         | + ~AUD 1bn (USD 0.75bn)<br>Commonwealth/Queensland<br>co-investment in<br>PsiQuantum (2023–2028).                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                        | quantum-driven<br>production by 2030.                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                     | computing/ communication/<br>sensing.                                                                                                                                                                                           |
| <b>CII &amp;<br/>Quantum</b>            | Governed by SOCI Act 2018<br>(11 CII sectors) + Critical<br>Infrastructure Risk<br>Management Program<br>(CIRMP, Feb 2023).<br>No PQC-specific CII<br>requirements yet; proposed<br>CIRMP amendments would<br>let quantum be declared a<br>"material risk."<br><br>Government agencies to<br>manage PQC readiness<br>under the PSPF<br>requirements. | Cybersecurity Law +<br>Regulations on Security<br>Protection of CII.<br>2025 Regulations on<br>Commercial Cryptography<br>Use in CII mandate<br>approved crypto for CII<br>operators.<br>QKD (BSBN) already serves<br>banks, power grids, e-<br>government. | NCIIPC (under<br>NTRO) oversees CII<br>(power, banking,<br>telecom, transport,<br>e-governance).<br>No PQC-specific<br>NCIIPC guidance<br>yet; CERT-In/SISA<br>white paper (Jul<br>2025) recommends<br>PQC roadmap for<br>CII sectors. | Active Cyber Defence Law<br>(May 2025) + Economic<br>Security Promotion Act<br>2022 define CII operators.<br>NCO Cybersecurity<br>Strategy (Dec 2025)<br>commits to PQC transition<br>support for CII.<br>FSA has only "suggested"<br>(not mandated) PQC<br>transition for financial<br>institutions. | Cybersecurity Act 2018 (11 CII<br>sectors).<br>CSA's Quantum-Safe<br>Handbook (July 2026) outlines<br>specific quantum safe<br>migration guidance issued to<br>CII Operators.<br>MAS Technology Risk<br>Management Guidelines<br>require quantum risk<br>assessments for financial<br>institutions. | CII split between NIS (public<br>sector) and MSIT (private<br>sector).<br>KISA/KNCERT conduct<br>mandatory annual<br>vulnerability assessments.<br>No explicit PQC-specific CII<br>mandate yet beyond sector<br>prioritisation. |
| <b>Focal<br/>Industrial<br/>Sectors</b> | Communications, data<br>storage/processing,<br>defence,<br>education/research, energy,<br>financial services, food &<br>grocery, health, space,<br>transport, water & sewerage<br>(SOCI's 11 sectors).                                                                                                                                               | Finance, energy, transport,<br>water resources,<br>telecommunications, e-<br>government services<br>(designated CII sectors).                                                                                                                               | Quantum<br>computing,<br>quantum<br>communication,<br>quantum<br>sensing/metrology,<br>quantum<br>materials/devices (4<br>NQM hubs).<br>CII priority sectors:<br>banking/finance,<br>healthcare, civil<br>infrastructure,<br>defence.  | Cross-sector national<br>strategic technology; 12<br>Quantum Technology<br>Innovation Hubs<br>(computing, sensing,<br>materials, chemistry,<br>software, security).                                                                                                                                   | Finance (MAS-led),<br>telecommunications/networks<br>(NQSN+ under IMDA), port &<br>logistics/transport.                                                                                                                                                                                             | Quantum computing,<br>communications, sensors,<br>materials/ parts/ equipment,<br>algorithms (5 regional<br>clusters).<br>Priority migration sectors:<br>healthcare, defence, finance,<br>telecom (5G).                         |

| Category                               | Australia                                                                                                                                      | China                                                                                                                                                                                                                                        | India                                                                                                                                                                                              | Japan                                                                                                                                                                               | Singapore                                                                                                                                                                       | South Korea                                                                                                                                                                          |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Named PQC Algorithms/ Standards</b> | No indigenous algorithms named.<br>ISM reviews/approves PQC algorithms for government use (implicitly NIST-aligned: ML-KEM/ML-DSA family).     | No specific winning algorithms named yet — domestic submission process underway ("Requirements for Submission of Public Key Cryptography Algorithms," Oct 2025).<br>Existing standards: GB/T 42565-2023, GB/T 42829-2023, GB/T 47177.1-2026. | No indigenous PQC algorithms named; roadmap points to internationally recognised algorithms (NIST, ISO/IEC, ITU, ETSI).<br>Own QKD/QRNG standards: TEC 91000:2022, TEC 91010:2023, TEC 91020:2024. | CRYPTREC Ciphers List updated March 2026 to include FIPS 203 (ML-KEM); remaining NIST PQC algorithms (ML-DSA, SLH-DSA) scheduled for FY2026.<br>No indigenous algorithms developed. | No indigenous algorithms named; Quantum-Safe Handbook references NIST algorithms.<br>Own network standard: IMDA's RS QKDN (Reference Specification for QKD Networks, Jun 2023). | KpqC competition winners (Jan 2025): digital signatures HAETAE and AIMer; KEMs SMAUG-T and NTRU+ — indigenous sovereign PQC algorithm set, run by NIS/NSR via KCMVP.                 |
| <b>Key Sector Regulators</b>           | Department of Home Affairs (DHA)<br>Australian Signals Directorate (ASD)/ACSC<br>APRA (banking prudential)<br>ASIC (markets/financial conduct) | State Cryptography Administration (SCA)<br>Central Military Commission (CMC)<br>MIIT<br>TC260 (National Info Security Standardisation Committee)<br>People's Bank of China (financial infrastructure)                                        | Department of Science and Technology (DST)<br>MeitY/CERT-In<br>NCIIPC<br>Reserve Bank of India (RBI)<br>Telecom Engineering Centre (TEC)/STQC (testing & certification)                            | Cabinet Secretariat (CAS)<br>National Cybersecurity Office (NCO)<br>CRYPTREC (joint government project)<br>Financial Services Agency (FSA)                                          | Cyber Security Agency (CSA)<br>Infocomm Media Development Authority (IMDA)<br>Monetary Authority of Singapore (MAS)                                                             | National Intelligence Service (NIS)<br>MSIT/KISA<br>Financial Services Commission (FSC)/Financial Supervisory Service (FSS)<br>KFTC (interbank clearing)/KSD (securities depository) |



# 04

---

## **Chapter 4 – Recommendations for the Enterprise**

For many private and public sector organisations, 2026 marks the beginning of the migration window to ensure Q-Day readiness. To maintain digital trust and operational resilience, businesses should consider shifting from passive monitoring to active implementation. CCAPAC offers the following recommendations.

## **Elevate Quantum Risk to the Executive Level, in recognition that it is a Systemic Challenge**

# **E1.**

Public and private sector organisations should consider quantum risk as an issue of national and economic security, digital resilience, and operational continuity, rather than a narrow cryptographic or technical concern. Quantum risk must be elevated with executive education, to the same level of board and executive attention as climate risk, geopolitical risk, and systemic cybersecurity risk.

In practical terms, this means:

- **C-suite alignment:** The CISO, CRO, CFO, and COO must develop a shared understanding of quantum risk and a common framework for prioritising migration investments within organisational resource constraints.
- **Dedicated budget:** Cryptographic lifecycle management - including PQC migration - should have dedicated budget line items rather than competing with operational priorities in general IT or cybersecurity budgets. The CISO should be resourced and empowered to develop a quantum readiness programme with this dedicated budget, staff, and executive sponsorship.
- **Board education:** Quantum risk should be presented to the board through dedicated briefings, at least annually, covering the threat timeline, the organisation's current exposure, migration progress, and the business impact of both inadequate and delayed migration.
- **Performance metrics and reporting:** Board reporting on quantum risk should include quantitative metrics: percentage of cryptographic inventory completed, percentage of high-priority systems migrated, vendor PQC readiness scores, and regulatory compliance status. Similarly, quantum risk disclosures should be incorporated into annual reports and regulatory filings where applicable, consistent with emerging requirements from financial regulators.

## **Organisations Should Conduct a Quantum Risk Assessment and Perform a Cryptographic Inventory**

# **E2.**

Immediately map all internal and external-facing systems to identify where vulnerable public-key cryptography (RSA/ECC etc) is being used. Undertake a risk assessment of already compromised encrypted data that may soon be vulnerable.

Organisations cannot manage what they cannot see. The foundational step in any PQC migration programme is a comprehensive cryptographic inventory - a systematic mapping of all systems, applications, data flows, and integrations that use public-key cryptography. This inventory must cover

the full technology estate: on-premises infrastructure, cloud environments, SaaS applications, third-party integrations, operational technology, and IoT systems.

A recommended approach would be that the cryptographic inventory should capture the following information for each cryptographic dependency:

- Algorithm type and key size (RSA-2048, ECDSA-256, AES-256, etc.)
- Usage context (key exchange, digital signature, certificate authentication, data encryption at rest, etc.)
- System or application name, owner, and environment (production/test/development)
- Sensitivity and longevity of data protected (high-value data requiring 10+ year confidentiality is HNDL priority)
- Protocol version and cryptographic library used (OpenSSL, BouncyCastle, etc.)
- Hardware embedding (is the algorithm in a TPM, HSM, smart card, or software-only etc?)
- Vendor dependency (is migration dependent on a third-party vendor's PQC roadmap?)
- Regulatory requirement (is this system subject to specific cryptographic standards mandated by regulation?)
- Undertake a risk assessment of already compromised encrypted data that may soon be vulnerable.

Automated cryptographic discovery tools are available from vendors including open-source projects such as cbomkit,<sup>289</sup> which generates a Cryptography Bill of Materials (CBOM) for software projects. (CBOM is being standardised by ECMA International.<sup>290</sup>)

Following the inventory, organisations should conduct a risk assessment that prioritises cryptographic dependencies by the combination of data sensitivity, data longevity, system criticality, and migration complexity.

Not all data requires the same urgency of PQC protection. High-priority targets - those protecting long-lived, high-sensitivity data on hard-to-migrate systems - should receive immediate attention and accelerated migration timelines. Organisations should triage their PQC migration efforts by the longevity and sensitivity of the data they are protecting, focusing first on data that must remain confidential for the longest periods and that carries the highest value to adversaries.

- **Immediate priority (begin PQC protection now):** Data that must remain confidential for 10+ years, including trade secrets, R&D data, clinical trial data, diplomatic communications, national security data, and genomic databases.
- **Near-term priority (migrate within 2 years):** Long-term financial records, customer personal data, intellectual property, and proprietary algorithmic models.
- **Medium-term priority (migrate within 5 years):** Operational data, authentication credentials (which can be rotated but benefit from PQC protection), and transactional data.
- **Long-term priority (migrate on hardware refresh cycles):** Symmetric encryption for data at rest (AES-256 retains adequate quantum security), non-sensitive operational data, and ephemeral session data.

This prioritisation framework allows organisations to allocate their limited PQC migration resources where they will have the greatest impact on reducing quantum risk exposure, rather than attempting to migrate everything simultaneously - an approach that typically leads to either paralysis or superficial compliance across the board.

---

<sup>289</sup> <https://github.com/cbomkit/cbomkit>

<sup>290</sup> <https://ecma-international.org/publications-and-standards/standards/ecma-424/>

## E3. Consider PQC Readiness Requirements at the Organisational Level

Evaluate the introduction of PQC readiness expectations, or mandates for the organisation to ensure a consistent uplift in quantum preparedness across the market/economy.

Organisations should evaluate the degree to which their critical operational systems are dependent on cryptographic security that may become quantum vulnerable. This evaluation should be integrated into the organisation's existing operational resilience and business continuity planning frameworks, treating cryptographic obsolescence as a scenario requiring contingency planning.

Specific areas deserving close attention include:

- **Long-term data confidentiality:** Data that must remain confidential for 10+ years is at immediate HNDL risk. This category typically includes trade secrets, R&D data, M&A plans, government correspondence, and personal health and financial data.
- **Digital signature integrity:** Systems where the authenticity of historical records, software, or communications must be verifiable in the long term - financial audit trails, legal documents, regulatory filings - are at risk from future signature forgery.
- **Cross-border data flows:** Encrypted data crossing international borders is particularly exposed to HNDL risk, as it may transit or be stored in jurisdictions with sophisticated collection programs.
- **Supply chain cryptographic dependencies:** Third-party systems and supply chain integrations that the organisation cannot directly control may create quantum vulnerabilities that bypass the organisation's own PQC migration.

## E4. Adopt and Implement Existing PQC Implementation Pathways

Develop a documented Cryptographic Transition Plan and follow established migration frameworks and vetted tools

Awareness and assessment must translate into concrete migration plans with defined milestones, budgets, and accountability. Organisations should develop a Cryptographic Transition Plan (CTP) that covers the full scope of PQC migration across the organisation's technology estate. The CTP should include:

- A prioritised list of cryptographic systems to be migrated, ordered by risk assessment outcomes
- Technical migration approach for each system (algorithm replacement, hybrid implementation, hardware replacement, vendor engagement)
- Timeline for each migration phase, with clear milestones
- Resource requirements (budget, staffing, external expertise)
- Dependencies and blockers (vendor PQC roadmaps, regulatory timelines, hardware refresh cycles)

- Testing and validation approach for each migrated system
- Rollback and contingency plans for migration failures

Implementing PQC correctly requires following established implementation pathways rather than developing bespoke approaches. Examples of implementation pathways include NIST's PQC migration guides and US CISA's PQC Roadmap.

Organisations should leverage the ecosystem of reference architectures, algorithm transition frameworks, and implementation guides developed by NIST <sup>291</sup>, CISA <sup>292</sup>, ENISA <sup>293</sup>, and the international cryptographic research community. Key implementation principles include:

- **Use vetted, open-source PQC libraries:** The Open Quantum Safe project's liboqs library<sup>294</sup> and the PQCclean<sup>295</sup> reference implementation provides well-reviewed starting points.
- **Follow established hybrid schemes:** For TLS and other protocols, implement hybrid key exchange and signature schemes as specified in IETF drafts, using both classical and PQC algorithms in combination during the transition period.
- **Update certificate management infrastructure:** Migrate certificate authorities and PKI systems to support PQC certificates. This includes updating certificate enrolment, renewal, and revocation processes.
- **Test in staging environments:** Before deploying PQC in production, test thoroughly in staging environments that mirror production traffic patterns and performance requirements. Pay particular attention to performance impacts on latency-sensitive applications.
- **Plan for certificate size increases:** Update load balancer, proxy, and application configurations to handle larger PQC certificate and handshake sizes without connection failures or timeouts.

## E5. Adopt a Hybrid-First Strategy

Deploy hybrid cryptographic schemes today to protect against HNDL attacks while maintaining backward compatibility with legacy clients and partners.

The recommended immediate tactical approach for most organisations is to adopt a hybrid-first cryptographic strategy: deploy hybrid cryptographic schemes that combine classical (RSA/ECC) and PQC algorithms, providing security against both classical and quantum attacks while maintaining backward compatibility with clients and partners that have not yet migrated.

A hybrid scheme, properly implemented, provides the best of both worlds: if the PQC component is later found to have a vulnerability (an important hedge given that the algorithms are newer and less battle-tested than RSA), the classical component still provides security; and if quantum computers emerge and break the classical component, the PQC component still provides security. The additional performance overhead of hybrid schemes is modest and well within the tolerance of most applications on modern infrastructure.

<sup>291</sup> <https://csrc.nist.gov/pubs/ir/8547/ipd>

<sup>292</sup> <https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography>

<sup>293</sup> <https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation>

<sup>294</sup> <https://openquantumsafe.org/liboqs/>

<sup>295</sup> <https://github.com/pqclean/PQClean>

## **E6.** **Mandate Organisational PQC-Ready Procurement**

Update vendor contracts to require “Quantum-Safe” or “Crypto-Agile” certifications for all new hardware and software acquisitions.

One of the most powerful levers available to organisations is the procurement process. Organisations should update their vendor contracts, technology procurement requirements, and supplier assessment frameworks to require demonstrated PQC readiness as a condition of new purchases and renewals. For example, the US Department of War’s Cybersecurity Maturity Model Certification (CMMC)<sup>296</sup> programme is beginning to incorporate PQC requirements for defence contractors. Specific procurement requirements to implement:

- Establish tools, policies and procurement requirements to identify and mitigate cryptographic vulnerabilities, including appropriate transparency from vendors regarding the cryptographic algorithms supported by software and hardware products and their migration status.
- Include “quantum-safe” or “crypto-agile” requirements in RFPs for all cryptographic hardware (HSMs, TPMs, smart cards, network security appliances) and software (TLS libraries, identity management, PKI systems).
- Require vendors to provide a PQC migration roadmap with committed timelines for PQC support in their products.
- For cloud service providers, require documentation of PQC migration plans for key management services, certificate management, and API security.
- Include contractual provisions requiring vendors to notify the organisation of any cryptographic vulnerabilities in their products and to provide migration support within defined timelines.

---

<sup>296</sup> <https://dodcio.defense.gov/CMMC/>



# 05

---

## **Chapter 5 – Considerations for Government Legislators and Policy Makers**

Legislators and policy makers in Asia Pacific face a dual challenge in the quantum security transition: managing PQC migration while also providing the regulatory, institutional, and market conditions that enable their economies to make this transition safely and efficiently. This chapter provides strategic recommendations for governments in their capacity as legislators and policy makers across both dimensions.

# G1.

## Treat Quantum Risk as a Systemic National Challenge

Provide government leadership through policy alignment and embed PQC readiness in strategies

Strong government leadership is needed to drive sector-wide engagement, build internal capability, and accelerate adoption through procurement policy, regulatory alignment, and public-private partnerships. This may necessitate including PQC readiness in key government policy documents and strategies.

# G2.

## Align With International PQC Standards, Develop Collaboration for Certification and Interoperability

Conduct crosswalks for national PQC roadmaps with international standards (NIST, ISO/IEC etc) to avoid digital fragmentation and ensure cross-border interoperability

A risk in the quantum security transition is cryptographic fragmentation, where different jurisdictions, sectors, and technology ecosystems adopt incompatible quantum-safe standards that prevent secure interoperability. Fragmented testing and validation requirements could also increase costs for governments, delay the adoption of secure technologies and undermine cross-border interoperability. Recognising equivalent testing conducted under other governments' assurance schemes or against international standards can help avoid these risks. Preventing this fragmentation will require active government-to-government collaboration on PQC standard alignment, mutual recognition of certification programs, and interoperability testing. Some suggested actions could include:

- **Conduct crosswalks between national PQC requirements and NIST standards:** Each jurisdiction's domestic cryptographic requirements should be aligned with NIST's ML-KEM, ML-DSA, and SLH-DSA standards, with documented crosswalk matrices that allow multinational organisations to demonstrate compliance across jurisdictions simultaneously.
- **Establish systems that allow recognition of global standards, and/or mutual recognition agreements for PQC certifications based on internationally recognised standards:** Countries with equivalent PQC certification frameworks should develop mutual recognition agreements that allow products certified under one framework to be accepted in partner markets without full re-evaluation. This would enhance cross-border trust, increase the practical value of certification, and reduce duplicative testing time and costs for industry.

- **Coordinate Asia Pacific participation in global standards development organisations:** Governments should coordinate their expert nominations to ISO/IEC JTC 1/SC 27, ITU-T SG17, IETF, and ETSI to ensure that Asia Pacific perspectives are represented in the development of global quantum security standards.
- **Develop a regional PQC interoperability testing framework:** A regional body - potentially hosted by APEC or ASEAN - should develop a common interoperability testing framework for PQC implementations, allowing vendors to demonstrate that their products work correctly with implementations from other jurisdictions.

APEC's Digital Economy Steering Group (DESG, the former Electronic Commerce Steering Group/ECSG)<sup>297</sup> and the ASEAN Consultative Committee for Standards and Quality (ACCSQ)<sup>298</sup>, and the ASEAN Digital Economy Framework Agreement (DEFA)<sup>299</sup> are potential institutional homes for regional PQC coordination.

G3.

## Establish National “Quantum-Safe” Pilot Programmes

Fund sandboxes and testbeds for government agencies and CII sectors (such as telcos, finance, logistics etc) to identify performance bottlenecks.

Government-funded pilot programmes that test PQC and QKD implementations in real critical infrastructure environments could be a key contribution from governments to pave the way through quantum migration and transition. Pilot programmes serve multiple functions:

- they generate practical knowledge about implementation challenges, performance impacts, and interoperability issues before those challenges become crises;
- they demonstrate government commitment and technical leadership;
- they create replicable reference architectures for the private sector; and
- they develop the operational expertise needed to support broader deployment.

Successful models from within Asia Pacific that other governments should emulate include:

- **Singapore's NQSN+:**<sup>300</sup> A government-funded operational QKD network connecting ministries and critical infrastructure, supported by detailed technical evaluation and published results. The NQSN+ provides a model for how a government can establish quantum-secure communications for its most sensitive operations while generating exportable knowledge about implementation.
- **Japan's Tokyo QKD network:**<sup>301</sup> A decade-long operational quantum network involving government, academic, and industry partners, generating sustained technical expertise and a domestic commercial QKD ecosystem.

<sup>297</sup> <https://www.apec.org/what-we-do/committee-on-trade-and-investment/digital-economy-steering-group/overview--digital-economy-steering-group>

<sup>298</sup> <https://asean.org/our-communities/economic-community/standards-technical-regulations-and-conformity-assessment-procedures/>

<sup>299</sup> <https://asean.org/asean-defa-study-projects-digital-economy-leap-to-us2tn-by-2030/>

<sup>300</sup> <https://nqsn.sg/>

<sup>301</sup> <http://www.uqcc.org/QKDnetwork/>, <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2023/0724/Documents/Kenyoshi.pdf>, <https://www.nict.go.jp/en/quantum/topics/20101014-1.html>

- **India's QCI testbed:**<sup>302</sup> A research institution-focused quantum communication network that strengthens technical capacity in quantum networking and PQC while fostering global collaboration, interoperability, and shared innovation.

Governments that have not yet established quantum-safe pilot programmes should consider prioritise doing so. Pilot results should be published (to the extent compatible with national security requirements) to maximise knowledge sharing with the private sector.

## G4.

### Establish Transparency in Government and Critical Infrastructure

Require operators of government, CII and essential services to report on their PQC migration status and provide clear timelines for reaching quantum-readiness.

Effective quantum risk management across the economy requires that governments have visibility into the quantum readiness status of critical infrastructure operators, and that these operators have a clear and transparent accountability mechanism established for their PQC migration progress. Governments should establish these transparency and accountability mechanisms specifically for quantum readiness, building on existing critical infrastructure regulatory frameworks, such as:

- **Establishing quantum risk assessments for CII operators:** Require operators of government and designated critical infrastructure organisations to conduct and submit annual quantum risk assessments, including cryptographic inventories, HNDL risk assessments, and migration plans while also considering the adoption of a globally aligned assessment framework for Cryptographic Bills of Materials (CBOMs).
- **Establishing PQC migration timelines:** Establish regulatory timelines by which government agencies and CII operators must achieve defined milestones - for example, completing cryptographic inventories by 2026, deploying hybrid PQC for high-priority systems by 2028, and completing full migration by 2033-2035.
- **Regulatory audit and assurance:** Cybersecurity regulatory agencies should have the authority and capacity to audit PQC migration plans and their implementation, and to impose penalties for non-compliance or material misrepresentation.

<sup>302</sup> <https://telecom.economictimes.indiatimes.com/news/policy/andhra-pradesh-to-launch-indias-first-open-access-quantum-computer-testbeds/130249586>

# G5.

## **PQC ready procurement.**

Governments policy makers should require procurements across government organisations and critical infrastructure operators to be PQC ready.

Procurement is one of the strongest levers governments have to shape market behaviour, but it only works if “PQC-ready” is defined consistently and backed by credible assurance pathways. Governments should require all agencies and CI entities to update procurement policies and contracts to require PQC-ready / crypto-agile capabilities for new hardware and software acquisitions.

# G6.

## **Accelerate Practical Engagement and Planning and Provide Clear Implementation Pathways.**

Governments should actively promote guidance, roadmaps, and tailored materials for key stakeholders.

Set clear expectations for organisations to develop migration plans and begin transition preparations as soon as practicable, with priority given to high value and high risk systems. Support adoption through detailed reference architectures, algorithm transition frameworks, and practical adoption models. Particular attention should be given to the challenges of operating at scale and modernising legacy systems.

Government policy makers should drive awareness and support organisations to translate this into concrete migration plans with defined milestones, budgets, and accountability. Government agencies can ensure that PQC is implemented correctly by establishing and/or promoting implementation pathways. Examples of implementation pathways include NIST’s PQC migration guides and US CISA's PQC Roadmap.

# G7.

## **Incentivise SME Adoption and PQC Migration.**

Provide tax credits or technical subsidies for SMEs to upgrade their digital security, preventing them from becoming weak entry points into the supply chain.

SMEs could be the largest security gap for Asia Pacific’s PQC migration, as they typically lack the internal cybersecurity expertise to assess quantum risk, the financial resources to fund comprehensive PQC migrations, and the procurement leverage to demand PQC-ready products from suppliers. While exact figures vary, SMEs form 90-99% of all businesses in Asia and form an integral component of the regional and global supply chains. SMEs’ quantum vulnerability could be considered a serious systemic risk, and effective government interventions may be needed to accelerate SME quantum readiness. Some approaches include:

- **Tax credits and subsidies for PQC migration costs:** Targeted tax incentives for SME investment in quantum-safe technology upgrades - similar to existing incentives for energy efficiency or digital transformation - can significantly reduce the financial barrier to adoption.
- **Government-funded SME assessment services:** Cybersecurity agencies could operate SME cybersecurity support programmes that can be extended to include PQC risk assessment services.
- **Procurement requirements that create market signals:** When governments and large regulated entities (banks, utilities, defence contractors) require PQC-ready supply chain partners, it creates a powerful market signal that drives SME investment in quantum readiness.
- **Simple, actionable PQC guidance for SMEs:** Most SMEs do not need to understand lattice cryptography - they need simple, practical guidance on which specific software updates to apply, which hardware to replace, and which questions to ask their IT vendors. Government cybersecurity agencies should develop and widely distribute such guidance.

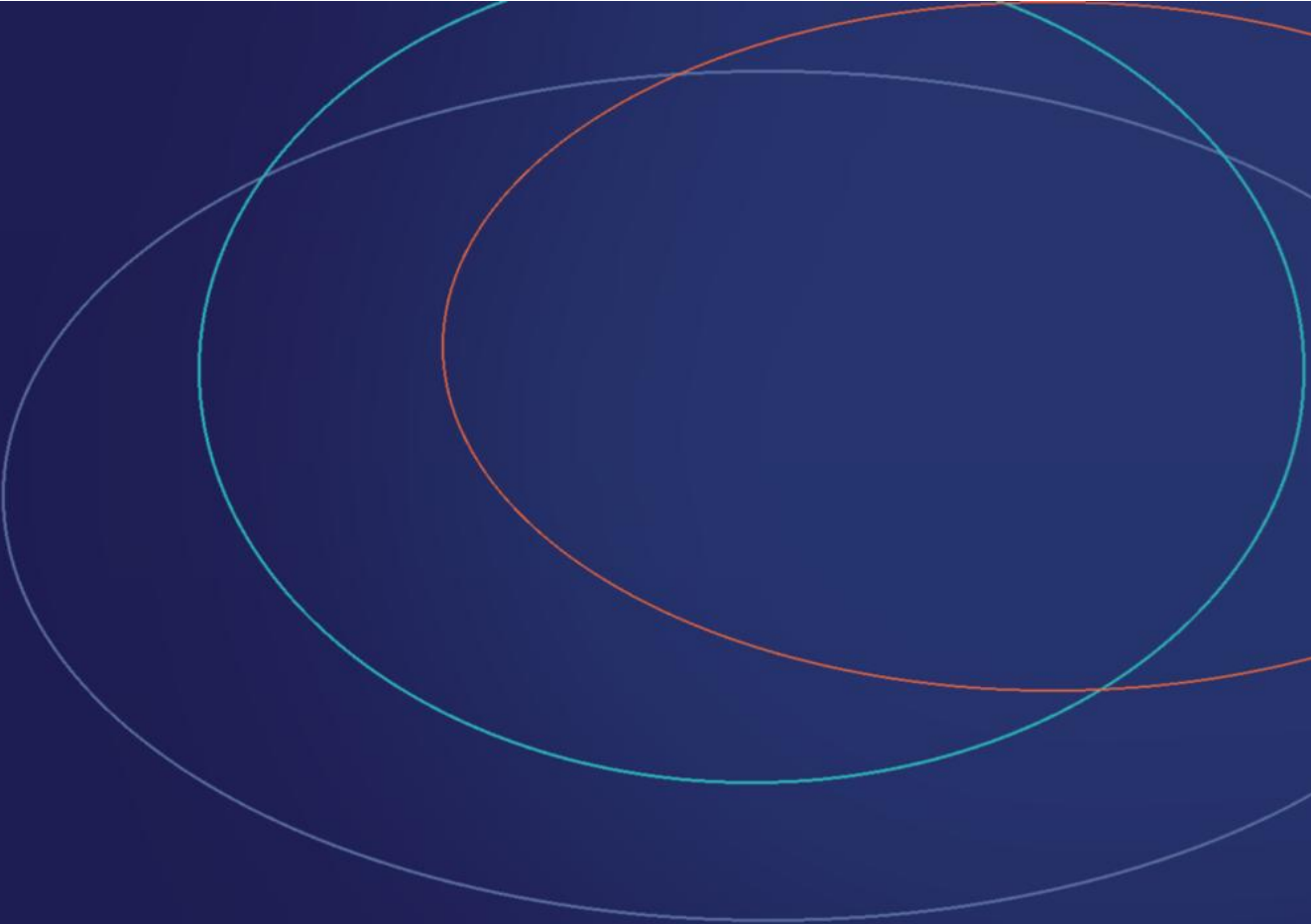
## G8.

### Foster a Quantum-Ready Workforce.

Fund regional university programmes and professional certifications focused on post-quantum mathematics and secure implementation

The quantum security transition will require a significantly expanded pool of professionals with expertise in post-quantum cryptography, quantum-safe system design, and cryptographic implementation. Building this workforce is a long-term investment, given the training pipelines required to develop competent cryptographers and security engineers. Key workforce development initiatives governments could fund and support:

- **University curriculum development:** Fund the development and deployment of PQC curriculum at undergraduate and graduate levels across computer science, mathematics, and cybersecurity programs.
- **Professional certification programs:** Develop regional professional certification programmes for PQC practitioners that validate implementation competence and create career incentives for specialisation.
- **Government-industry secondment programs:** Establish programmes that allow government cybersecurity specialists to spend time in industry (and vice versa), building cross-sector PQC expertise and relationships.
- **Regional researcher mobility:** Fund grants and fellowships that enable Asia Pacific PQC researchers to spend time at leading international institutions and to bring expertise back to the region.
- **Industry training subsidies:** Provide subsidies for employees of SMEs and critical infrastructure operators to undertake PQC training and certification, reducing the cost barrier to workforce development in smaller organisations.



---

## **Conclusion – The Imperative of Quantum Readiness in Asia Pacific**

The quantum security transition represents a technological challenge for Asia Pacific's next leap into the digital age. The finalisation of NIST's post-quantum cryptographic standards in 2024 marked the end of the "what algorithms should we use?" debate and the beginning of the "how do we implement this at scale?" era. The region's response to that question - and the speed and effectiveness with which it can mobilise governments, enterprises, infrastructure operators, and citizens toward quantum-safe digital systems - will determine whether Asia Pacific's digital future is built on a foundation of enduring security or chronic vulnerability.

**The picture that emerges from this comprehensive assessment is one of steady but uneven progress, significant potential, and urgent need for acceleration.** Singapore and Japan have made significant progress in the region in quantum security readiness, combining strong research foundations with proactive regulatory engagement and operational quantum security deployments. South Korea is advancing rapidly, driven by government mandates and the formidable technical capabilities of its domestic technology industry. Australia has the strategic orientation and international partnerships required for leadership but must urgently translate these strengths into concrete regulatory mandates and enterprise-level action. India faces the greatest scale challenge in the region, with a digital economy of 1.4 billion people in rapid transformation and quantum readiness infrastructure still in early development.

Across all six markets, common themes emerge.

- The "Harvest Now, Decrypt Later" and "Trust Now, Forge Later" threats are real, active, and not adequately appreciated at the organisational level.
- Cryptographic inventories are incomplete or non-existent in the majority of organisations.
- Regulatory mandates with specific timelines alone are insufficient to drive the pace of migration required.
- SMEs - the connective tissue of Asia Pacific's supply chains - are largely unaware of quantum risk and unequipped to address it. And the talent required to execute PQC migrations correctly and securely is in severe short supply.

These challenges are formidable but not insurmountable. We observe that the tools are available: NIST-standardised algorithms, open-source implementations, proven migration frameworks, and a growing ecosystem of commercial quantum security products and services. The institutional capacity also exists to design and execute effective PQC programs within government cybersecurity agencies, financial regulators, standards bodies, and leading enterprises across the region. What has been lacking is urgency, coordination, and a shared recognition that the quantum threat is not a future problem but a present one.

**CCAPAC offers this report as a contribution to building that urgency and coordination.** The recommendations contained in Chapters 4 and 5 are practical, actionable, and calibrated to the specific context of Asia Pacific's diverse economies and regulatory environments. They are not exhaustive - the quantum security landscape is evolving rapidly, and specific technical and regulatory recommendations will require continuous updating as standards evolve and implementation experience accumulates. But the strategic direction is clear, and the quantum age is arriving. Asia Pacific's digital economy, critical infrastructure, and national security depend on meeting it prepared.



The Coalition for Cybersecurity in Asia-Pacific or CCAPAC is a group of dedicated industry stakeholders who are working to positively shape the cybersecurity environment in Asia through policy analysis, engagement, and capacity building.

Join us! Find out more at  
[ccapac.asia](https://ccapac.asia)