FUTURE MATTERS
CENTRE OF EXCELLENCE

GFTN
Innovating Finance. For Everyone.

HOW TO DESIGN QUANTUM-SAFE SYSTEMS

A Post-Quantum Cryptography Migration Plan for Critical Infrastructure

July 2026

ABOUT

The Global Finance & Technology Network (GFTN) is a Singapore-headquartered organisation that leverages technology and innovation to create more efficient, resilient, and inclusive financial systems through global collaboration. GFTN hosts a worldwide network of forums (including its flagship event, the Singapore FinTech Festival); advises governments and companies on policies and the development of digital ecosystems and innovation within the financial sector; offers digital infrastructure solutions; and plans to invest in financial technology startups through its upcoming venture fund, with a focus on inclusion and sustainability.

For more information, visit www.gftn.co

Western Australia Web3 (WAWEB3) is an incorporated not-for-profit association registered in Australia under the legal name WAWEB3 Inc. in late 2022. WAWEB3's mission is to raise awareness about the next evolution of the internet (web3) and the integrated digital economy and facilitate collaboration between government, academia, industry and communities in the Indo-Pacific region. WAWEB3 promotes an open, human-centric, inclusive, sustainable and resilient digital economy. As a local formal partner of GFTN, WAWEB3 collaborates in bringing the Black Swan Summit to Perth.

For more information, visit https://waweb3.org/

The City of Perth is a local government area and body, within the Perth metropolitan area, which is the capital of Western Australia. The local government is commonly known as Perth City Council. The City covers the Perth city centre and surrounding suburbs. The City of Perth is an active supporter of innovation, economic development, and international collaboration.

For more information, visit https://perth.wa.gov.au/

Business Events Perth, funded by the Western Australian Government and partners, has 50 years of experience attracting conferences and incentive groups to Western Australia. Their mission is to promote WA as a destination for conventions, exhibitions, and incentive travel, both nationally and internationally. They offer expert assistance, local knowledge, and market intelligence to help event planners successfully host their events in WA. Essentially, they want to help you make your next conference a success in Western Australia.

For more information, visit https://www.businesseventsperth.com/

CONTENTS

EXECUTIVE SUMMARY

Quantum computing is advancing faster than most organisations have prepared for. In December 2024, Google's Willow quantum chip solved a benchmark problem in under five minutes that would take the world's fastest classical supercomputer ten septillion years — longer than the age of the universe by a factor of a quadrillion. What this trajectory points to is not an abstract science project. This amount of computing power can solve humanity's burning problems in health, environment and science. However, it can also break the mathematical foundations of the encryption that today protects our bank accounts, Medicare records, defence communications, payments networks, government identity systems and national intelligence infrastructure. Reserve Bank of Australia Governor Michele Bullock was direct at the 2025 Bradfield Oration: "I "If you believe what they say on the tin of quantum computing, what takes 200 years to decrypt now, to break will take a matter of minutes. So it is a big threat ... it's scary." Despite warnings of this kind from the highest levels of public leadership, a 2025 Information Systems Audit and Control Association (ISACA) global poll of more than 2,600 digital trust professionals found that 95 per cent of organisations lack a quantum computing roadmap, and only 5 per cent have a defined quantum strategy. The immediate risk is not that every encrypted system collapses on a single day. It is that nation-state adversaries are already collecting encrypted data — financial records, health records, digital assets, defence communications, intelligence assessments, identity credentials — with the intention of decrypting it when the required computing power arrives (a strategy known as Harvest Now Decrypt Later – HNDL). For organisations whose data must remain confidential for years or decades, the window to act is already narrowing.

The roundtable convened at Perth's Black Swan Summit to address a practical question: how should organisations move from post-quantum cryptography awareness to execution? The session brought together quantum researchers, cybersecurity practitioners, critical infrastructure specialists, defence and security experts, consulting professionals, and technology vendors across Australia. The answer that emerged was not a call for panic. It was a structured argument for treating Post Quantum Cryptography (PQC) migration as an enterprise risk, procurement, governance, supply-chain and operational resilience challenge — and for starting that work now, with the standards and resources already available.

This report is organised around two parts. Part I examines why the transition cannot be deferred: the nature of the quantum threat, the specific risks of HNDL, and the emerging security challenges created by agentic AI and the Model Context Protocol. Part II addresses how to respond: building cryptographic visibility without operational disruption, managing the distinctive challenges of operational technology, designing for crypto-agility, navigating the tension between cryptographic sovereignty and global interoperability, and understanding what government and industry must now do to make migration coordinated rather than chaotic.

PART I
WHY THE TRANSITION CANNOT WAIT

01
THE INFRASTRUCTURE OF TRUST

Every major digital system in use today depends on cryptography. It protects identity and authentication, banking and payments, government services, health records, defence communications, cloud platforms, software updates, machine-to-machine communications and operational technology in energy, water, ports and industrial control systems. Most of this cryptography is invisible to its users — buried inside products, protocols, certificates, firmware, chips, VPNs, APIs, databases, identity platforms and third-party services. Its invisibility is part of its problem.

Quantum computers threaten specific categories of cryptographic protection, and an average organisation may use thousands of different products with embedded cryptographic capability — all of which may eventually need to be updated. The challenge is in managing that update - identifying what and when needs to be updated in a staged process now or managing a reactive and disastrous crisis when the window has already closed.

The roundtable was also clear on what post-quantum cryptography actually is — a point that generated one of the session's critical clarifications. Post-quantum cryptography has little to do with quantum computers. It runs on standard digital hardware and software. The "quantum" in the name refers to what it defends against, not what powers it. Organisations do not need quantum computers to implement quantum-safe cryptography. The tools are available now, the standards have been finalised, and the only remaining question is when to start.

"Post-quantum cryptography is the only thing that can protect your system from the quantum threat, and you need to be implementing it now. It has moved from algebraic RSA to geometric lattice-style protection — and it works on the computers you already have."

— Roundtable Discussant

Context. National Institute of Standards and Technology (NIST) finalised its first post-quantum encryption standards in 2024: FIPS 203 / ML-KEM for key encapsulation, FIPS 204 / ML-DSA for digital signatures, and FIPS 205 / SLH-DSA as a hash-based backup standard. The shift is from algebraic structures — RSA (named after its three inventors: Ron Rivest, Adi Shamir and Leonard Adleman, who published it in 1977) and elliptic curve cryptography — to geometric lattice-based approaches believed to resist quantum attacks. The Australian Signals Directorate (ASD) now refers to ML-KEM and ML-DSA in its cryptography guidance and notes that organisations planning systems intended to operate beyond 2030 should support ASD-approved post-quantum algorithms by that date.

02
THE QUANTUM THREAT: WHAT ACTUALLY BREAKS

Quantum computers threaten specific encryption. Shor's algorithm, published in 1994 and demonstrably viable on sufficiently powerful quantum hardware, can break the public-key cryptographic systems that underpin most of the internet's security infrastructure: RSA and elliptic curve cryptography. Grover's algorithm effectively halves the security level provided by symmetric encryption, meaning that longer key lengths are an adequate response rather than a fundamental redesign. The roundtable was consistent on this point: the primary migration challenge is RSA and ECC-based public-key systems, not symmetric cryptography.

The roundtable also addressed a frequently cited misconception about timing. There is no single "Q-day" on which all encrypted data simultaneously becomes readable. Quantum computing capability will develop gradually. Early instances of Shor's algorithm at scale would likely require substantial time and computational cost to break a single key — the economics do not resemble a sudden collapse of all digital security. What this means in practice is that the risk is not a cliff edge but a rising gradient: as quantum hardware matures, the cost of breaking specific keys will fall, and the categories of data at highest risk will progressively expand. Planning should reflect this gradual escalation rather than a binary wait-and-then-react logic.

The roundtable also raised a more technically demanding observation: we cannot mathematically guarantee these PQC schemes are safe against every possible quantum algorithm, and some researchers have tried—unsuccessfully so far—to break them. Therefore, we must keep analysing them and designing systems from the beginning with the ability to substitute algorithms when better options emerge.

"There is no Q-day. There is a gradual increase in risk. The first time someone can run Shor's algorithm at scale, it will probably take a week and considerable computational cost to break a single key. But if you have the most valuable data in your sector, and a nation-state adversary with strategic patience, you should already be concerned."

— Roundtable Discussant

Context. The NIST standardisation process ran for approximately eight years. Two candidate algorithms — SIKE and Rainbow — came close to adoption but were broken using classical computers before the process was complete. Project 11, a quantum security research initiative, offers a Bitcoin bounty to experimental groups that can demonstrate quantum attacks on elliptic curve cryptographic signatures of increasing bit length, providing a structured incentive for the community to stress-test current systems. These efforts illustrate that rigorous adversarial testing of PQC standards, not only implementation, is an ongoing security necessity.

03

HARVEST NOW, DECRYPT LATER: THE IMMEDIATE RISK

For organisations that hold long-lived sensitive data, the quantum threat is not a distant security project. The HNDL means that adversaries can collect encrypted data today and store it until they have the quantum capability to decrypt it. Health records, defence communications, intelligence assessments, national identity systems, legal documents, financial records and infrastructure designs are the categories where the exposure is live.

The roundtable was precise about who is most exposed and why. The economics of HNDL do not suit organised crime. Capturing data from encrypted network connections, storing it indefinitely, and then spending the significant computational cost to decrypt each record individually does not fit a short-horizon criminal business model. What it fits is nation-state adversaries with strategic patience and large resources — actors willing to invest now against returns that may arrive years later. For governments, defence agencies, healthcare systems and critical infrastructure operators, this is the threat model that matters.

An important technical clarification emerged from the roundtable. Stored data at rest typically uses symmetric encryption, which Shor's algorithm does not break. The more significant HNDL exposure is data in transit — specifically, communications protected by Transport Layer Security (TLS - the successor to Secure Socket Layer SSL) connections, which use public-key cryptography for the key exchange phase. Each connection establishes a separate key, and these keys are the primary harvest target. The implication is that surveillance of network traffic, not access to encrypted storage systems, is the likely collection mechanism.

Submarine cables carry around 99% of international internet traffic, and critical services — utilities, communications, healthcare and financial services — are now overwhelmingly dependent on digital systems and encrypted connectivity for their core operations. Taken together, this creates a national-scale attack surface for harvest-now-decrypt-later operations against critical infrastructure. This is not merely an enterprise risk question. It is a question of national economic and security resilience, and it sits beyond the reach of any single organisation's migration plan.

"The harvest is already happening. The question is not whether sensitive data is being collected today in encrypted form. The question is how long until the computing power to decrypt it exists — and whether the data you hold today will still be sensitive by then."

— Roundtable Discussant

04

AGENTIC AI AND THE MCP SECURITY SURFACE

The roundtable addressed a newer dimension of the threat landscape: the security implications of agentic AI systems and the Model Context Protocol infrastructure through which they operate. This intersection of quantum-era risk and contemporary AI architecture is emerging quickly, and the roundtable's concern about it was clear.

The Model Context Protocol, or MCP, is a standard that allows AI systems to connect to external services, databases, payment systems and applications — enabling them to act autonomously rather than simply respond to prompts. The capability is significant: an agentic AI using MCP can retrieve information, make bookings, trigger financial transactions, check compliance records and execute sequences of actions without human intervention at each step. The roundtable observed that this architecture was designed with functionality as the primary objective, not security. The result is a system where third-party MCP servers — the bridges between AI agents and enterprise applications — have a substantially elevated rate of exposure to malicious insertion and corruption.

The roundtable discussed an AI-orchestrated attack in which an autonomous AI agent was instructed to exploit a leading AI provider's systems and then access data from that provider's largest clients. The attack was predominantly AI-executed, state-sponsored, and involved sequential steps across multiple high-security targets. The provider disclosed the incident responsibly and transparently. The roundtable recognised a signal about the architecture of future attacks: autonomous systems using exploitable infrastructure to penetrate enterprise environments at scale, at speed, and with minimal human direction.

In this context, the intersection of HNDL risk and MCP exposure means that AI-retrieved data, transmitted through machine-to-machine channels, may be subject to the same harvest-and-decrypt dynamic that applies to any TLS-protected communication. A second distinct vulnerability is side-channel attack. Even where PQC has been mathematically applied to a system, adversaries using AI-assisted electromagnetic analysis can potentially extract information from the physical operating characteristics of a chip — not by breaking the cryptographic algorithm, but by reading the physical signals it generates. PQC provides mathematical protection. It does not, by itself, eliminate hardware-level side-channel exposure.

"MCP was built for functionality, not security. It is now the interface through which agentic AI reaches into enterprise systems, payment flows, and sensitive data. As AI agents become more capable and more trusted to take autonomous action, the security of the infrastructure they operate through becomes critical — and it has not kept pace."

— Roundtable Discussant

Context. The Model Context Protocol was released by Anthropic in 2024 and has been adopted across major AI platforms as the standard for agentic tool integration. As agentic AI moves from single-response systems to multi-step autonomous agents capable of accessing data, executing transactions and triggering downstream actions, the security

architecture of MCP infrastructure becomes correspondingly more significant. PQC is part of the long-term solution for the machine-to-machine communications layer. The roundtable was also clear that prompt injection, malicious tool registration, insecure plugin design and access-control failures in MCP servers are immediate risks requiring attention independently of the quantum transition.

PART II HOW TO DESIGN QUANTUM-SAFE SYSTEMS

05 VISIBILITY BEFORE ACTION: THE CRYPTOGRAPHIC INVENTORY

The first operational challenge is visibility. Identifying cryptography in organisation's systems is not a straightforward task — cryptography can be buried in VPN gateways, API endpoints, certificate authorities, firmware and cloud services that were procured, deployed and in many cases forgotten. The roundtable's consistent advice was not to wait for a complete map before acting. Two questions do most of the practical work: where are RSA or elliptic curve algorithms in use, and what data do they protect that must remain confidential for years or decades? Start there.

A practical shortcut is to use what already exists: business continuity and disaster recovery plans already list the systems the organisation needs restored first after an outage — those systems are almost certainly where quantum-safe cryptography is most urgent. But inventory should not be left to IT teams alone. Shadow IT surfaces in every migration exercise, and the people who know which systems are actually critical sit in business units, not IT departments.

"Don't try to get the perfect inventory of everything before you start. Go and find where your RSA encryption is, where your elliptic curve encryption is, where the data is that would be of greatest value to a nation-state adversary — and begin there. If you don't have a perfect IT asset inventory, you won't have a perfect cryptographic one. Start with risk."

— Roundtable Discussant

Context. The Australian Signals Directorate's (ASD) Planning for post-quantum cryptography guidance recommends a cryptographic bill of materials — an analogue of the software bill of materials — that captures cryptographic products, libraries, algorithms, protocols, parameters and configurations. ASD's phase-out applies only to traditional asymmetric cryptography (RSA, Diffie-Hellman and elliptic curve methods), for which a quantum computer poses a fundamental threat, while symmetric encryption such as AES-256 remains approved because its quantum risk is manageable through key length. Organisations building a first-pass inventory should therefore focus on the former category: RSA certificates, elliptic curve key exchanges, public-key-based authentication systems, and TLS configurations.

06 STARTING SAFELY: PILOTS, PRIORITISATION, AND MUSCLE MEMORY

The roundtable was consistent on one operational principle: do not begin with the most critical systems. The value of starting with non-critical but meaningful environments is about building institutional knowledge, testing processes, and creating the governance and vendor engagement infrastructure that makes migration of critical systems feasible later.

A good first pilot might be an API gateway, a VPN endpoint, an internal email encryption service, or a certificate authority operating in a non-production environment. The objective of a pilot is to understand how ready the organisation is to execute a migration: whether vendor roadmaps are accessible, whether change management processes exist, whether key management systems can be updated, and whether interoperability with counterparts can be maintained through a hybrid transition. What a pilot gives you is proof of readiness: your readiness to actually implement, to manage the change, and to build the muscle memory for doing this at scale when it matters.

For organisations with a large and complex environment, the first twelve months should produce several outcomes such as:

- a prioritised list of high-risk cryptographic dependencies,
- a mapping of vulnerable public-key algorithm use,
- an understanding of vendor and supply chain readiness for priority systems,
- a completed pilot in a non-critical environment, and
- a migration roadmap for the most critical systems with defined timelines, budget estimates and procurement requirements.

An important part of the migration process is vendor management. Organisations should work with specialised, high-assurance vendors—such as those providing PQC-enabled encryptors, HSMs and key-management systems—to implement quantum-safe cryptography. These components and discovery tools should be deployed under the organisation's own security governance, with vendors supplying certified hardware, software and migration tooling. Services that require bulk access to live transactional or classified data merely to 'scan for PQC readiness' should be treated as unnecessary and potentially unsafe, and avoided in favour of in-environment scanning that exposes only cryptographic metadata.

07
OPERATIONAL TECHNOLOGY: THE MOST DIFFICULT MIGRATION

The roundtable identified operational technology as the most challenging migration domain, and arguably the one where delay carries the most severe long-term consequences for critical infrastructure.

Operational Technology systems — industrial control systems, Supervisory Control and Data Acquisition (SCADA) environments, sensors, energy grids, water infrastructure, ports, mining automation and defence-adjacent control networks — were built for reliability, longevity and operational continuity rather than for frequent cryptographic updates. Cryptography in these environments is often embedded in chips, firmware, device hardware or proprietary protocols designed to operate for ten to twenty years without replacement. Updating cryptography in this context may require hardware replacement across geographically distributed assets, under conditions where systems cannot be taken offline for maintenance.

There is a range of strategies rather than a single prescription. For systems that are genuinely critical and genuinely difficult to upgrade, isolation may be the right initial response: segment the system from broader networks, apply protective overlays such as encrypted VPN gateways at the network boundary, and accept that the underlying device cryptography cannot yet be updated. For systems where chip or hardware refresh is approaching anyway, that window is the practical opportunity to mandate PQC-capable components in procurement. The roundtable noted that chip manufacturers have already begun producing PQC-capable hardware certified to high security standards, with market availability expected to reach OT-relevant products over a four to five year horizon.

Context: Australia's Security of Critical Infrastructure Act is already improving the security posture of OT environments, through mandatory risk management plans and requirements for critical infrastructure sectors to maintain operational continuity independently of internet connectivity for defined periods. These frameworks create both the regulatory structure and the incentive for OT security investment — but the planning and procurement decisions must begin now to position organisations for migration when the hardware and regulatory conditions align.

08
CRYPTO-AGILITY: DESIGNING FOR UNCERTAINTY

The PQC migration is not a settlement for one perfect solution but a process of staying agile. The NIST process took approximately eight years. Two algorithms that came close to adoption were broken classically before they were finalised. This means the target state for PQC migration is not compliance with the current NIST standard and then stability. The target state is crypto-agility: the ability to substitute a cryptographic algorithm, key length or protocol without redesigning the surrounding system. An organisation with crypto-agile systems can respond to a future algorithmic vulnerability within days or weeks rather than years.

Context. Crypto-agility has been formally incorporated into ASD's guidance on PQC migration. The Information Security Manual notes that post-quantum algorithms are more complex than traditional ones, making implementation quality particularly important. The principle of agility also addresses a second uncertainty: different regions may adopt different standards. China has developed its own post-quantum algorithms; South Korea is developing its own. Australian organisations with international counterparties may need to support multiple standards simultaneously. Systems that can switch between algorithms provide an operational hedge against both cryptanalytic risk and standards fragmentation. NIST itself is continuing to evaluate additional candidate algorithms as potential fallbacks.

09
SOVEREIGNTY AND CORPORATE STANDARDS

The tension between national cryptographic sovereignty — the desire to control which algorithms protect national data and infrastructure — and the practical necessity of global interoperability is an important question to consider for large organisations.

The NIST process is led by a US government body, and the history of cryptographic standards includes documented cases where weaknesses were deliberately introduced into internationally adopted algorithms. An Australian government or organisation that relies entirely on US-produced standards needs to be aware that it accepts a degree of institutional trust.

A related and practically important recommendation is that major cloud and technology platforms must implement PQC as a default configuration, not an optional setting. The organisations — public and private — that will constitute most of Australia's digital

economy do not primarily run custom systems. They use Microsoft, AWS, Azure, Google and a range of other platform providers. Ensuring those platforms implement PQC as a standard configuration, rather than a premium feature or opt-in setting, is one of the highest-leverage regulatory interventions available. The use of these global services needs to come with awareness of institutional risks and trust levels.

At the same time, no single organisation, sector or country can manage this transition in isolation. At the organisational level, most cryptographic infrastructure is controlled by third parties — cloud providers, network equipment manufacturers, identity platforms, chip suppliers — and migration depends on those vendors moving on compatible timelines. Quantum-safe migration should be treated as a collaborative security challenge rather than a sovereign technology competition — with shared mathematical research to stress-test standards, shared inventory methodologies, and regulatory coordination across trusted partnerships.

10

GOVERNMENT'S ROLE: FROM GUIDANCE TO MANDATE

Australia's current regulatory posture on PQC migration is characterised by guidance. The Australian Signals Directorate has published substantial planning material and identified 2030 as a readiness horizon for Commonwealth agencies. But the roundtable drew an important distinction clearly: ASD's guidance is guidance, not a mandate. The difference matters for how organisations prioritise and resource the work.

Guidance creates awareness. Mandates create action. The gap between an organisation that knows PQC migration is necessary and an organisation that has funded it, assigned executive accountability, engaged vendors, built an inventory and run a pilot is substantial. Closing that gap at scale, across critical sectors and within the available time, requires regulatory instruments that move beyond publication and toward enforcement.

There are several mechanisms through which government could move the market more effectively:

- procurement gates requiring PQC compliance as a condition for government contracts, driving vendor development upstream through the supply chain;
- attestation and posture reporting creating evidence-based accountability rather than last-minute compliance;
- and a safe harbour model — borrowed from US practice — where organisations demonstrating good-faith migration progress face reduced liability in the event of a breach.
- Finally, greater support for domestic innovation in quantum technologies and capability building that can be deployed in Australian and international markets.

The WA government context adds a specific dimension. WA's cyber security policy is currently being updated to include post-quantum cryptography requirements, and WA government agencies will be expected to have migration plans in place and to demonstrate progress against timelines aligned with ASD guidance. WA can position itself at the leading edge of Australian state-level PQC policy — treating the requirement not as a compliance exercise but as a strategic design decision for the state's digital infrastructure.

Context. The ASD guidance roadmap calls for Commonwealth organisations to have a PQC transition plan by 2026, to begin first migrations by 2028, and to complete migration by 2030. This is more aggressive than the United States and United Kingdom, which have set a 2035 horizon. India has targeted 2028. These different national timelines create both interoperability considerations and competitive incentive effects: major cloud providers will be incentivised to prioritise PQC implementation in markets where government procurement requires it.

11

CONCLUSION: DESIGN NOW, OR REACT LATER

The roundtable's conclusion was not that a quantum security catastrophe is imminent. It was that the conditions for disruptive, expensive and potentially irreversible cryptographic failure are already here — through active HNDL collection, through emerging vulnerabilities in AI-mediated communications, through legacy and operational technology systems that cannot be rapidly updated, and through regulatory timelines that are shortening while organisational preparedness lags.

The roundtable identified a sharp practical insight about proportionality. For most organisations, the vast majority of cryptographic exposure can be addressed through routine vendor updates, standard configuration changes and normal hardware refresh cycles. A much smaller proportion — unsupported legacy systems, hardware that cannot be upgraded, OT environments that cannot be taken offline, and data of highest adversary interest — will ultimately determine whether an organisation is resilient or exposed. The temptation is to measure progress by the easy majority. The roundtable's advice was to identify this difficult slice first, understand it fully, and build the migration plan around it.

The roundtable was equally clear that the success of PQC migration, if it is achieved, will look like nothing happened. That is what good security outcomes look like. The problem is that this makes investment and urgency difficult to sustain in organisations where success is invisible.

"The success of Y2K* was that it was a non-event. It was not a hoax; it was a crisis that was prevented because people put in the work. The success of the quantum transition will look the same. When quantum computers arrive, we will not be talking about them breaking the internet. We will be talking about all the remarkable problems they are solving."

— Roundtable Discussant.

The cryptographic transition is already underway. All organisations will need to migrate eventually. The question is whether they will migrate by design, on a timeline and resources they control, with systems built to adapt further; or by reaction, under pressure and panic, with critical infrastructure and data exposed.

* Y2K (the "Year 2000 problem" or "millennium bug") was a date handling bug in older computer systems where years were stored with only two digits, so 2000 was recorded as "00" and could be misread as 1900.

This report was produced under Chatham House Rules. No statement may be attributed to any named individual or their organisation. Analytical commentary in shaded callouts draws on publicly available data and research to contextualise the roundtable discussion; it does not represent the views of any individual participant.

GLOBAL FINANCE & TECHNOLOGY NETWORK (GFTN)

6 Battery Road, #28-01, Singapore 049909
gftn.co | hello@gftn.com