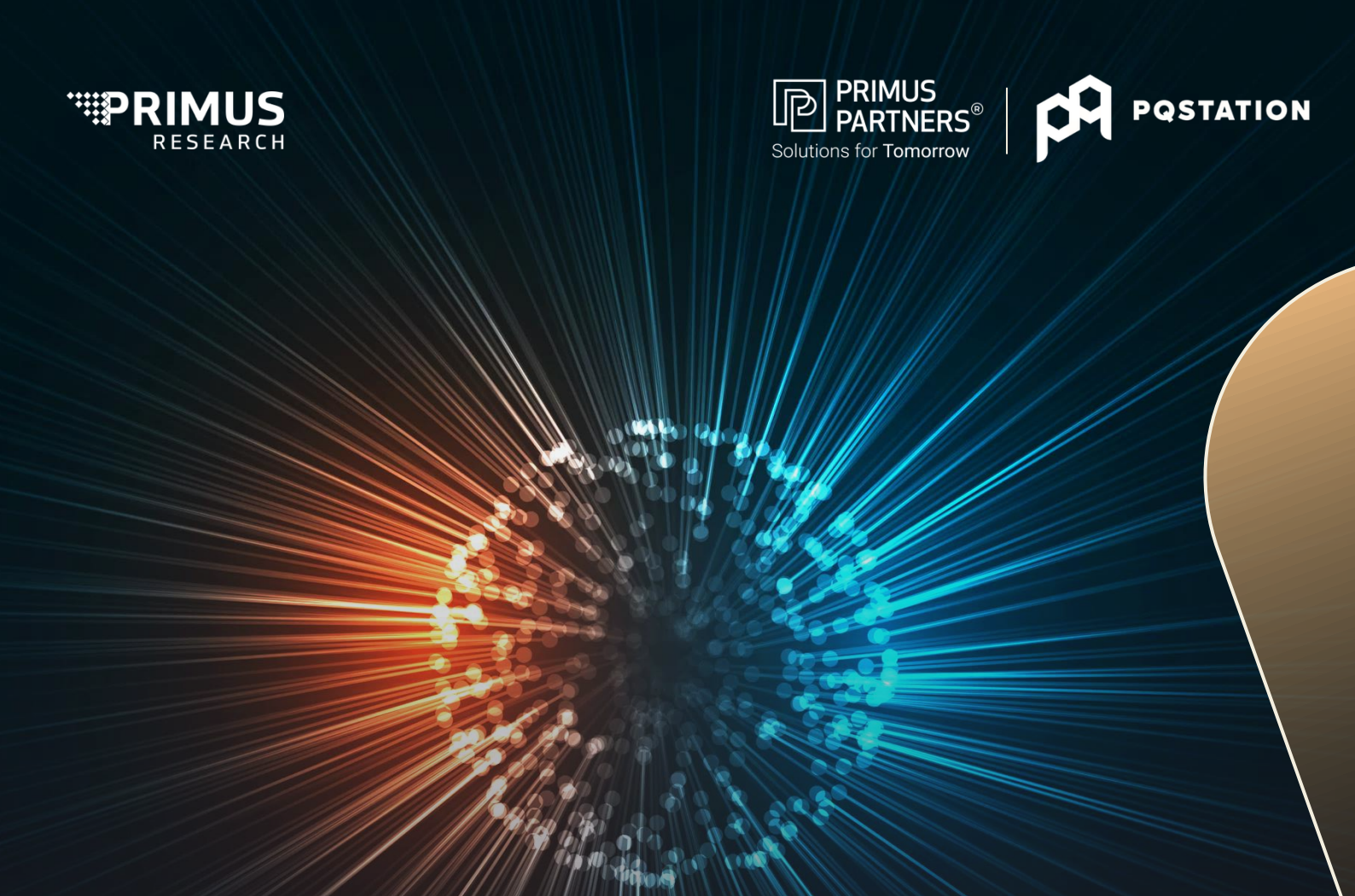
PRIMUS RESEARCH

PRIMUS PARTNERS®
Solutions for Tomorrow

PQSTATION



A Practical Guide To Quantum-Safe Migration for Indian Enterprises

APRIL 2026

Foreword

We come to this document from different directions: one of us from the world of policy and enterprise governance, the other from the laboratory where post-quantum cryptographic standards were forged. What brought us together was a shared frustration: the gap between the urgency of the quantum threat and the pace at which Indian enterprises are responding to it.

This gap is not born of complacency, but rather a framing problem. Quantum-safe migration has often been presented as a challenge of the future, that is something to monitor, to plan, to revisit later. That framing is inaccurate and creates a complex challenge. The data which is being encrypted by Indian organizations today, be it - loan agreements, identity records, regulatory filings, clinical trial data, and more, will continue to be sensitive in 2030, in 2035, and beyond. Sophisticated adversaries may be collecting some data, in its encrypted form, with an intention of decrypting it once advanced quantum capability arrives. However, the attack has already begun. It is simply a case of deferred decryption. This reality has drove us to write this guidebook together.

This is the reality that drove us to write this guide together.

India is in a genuinely strong position. The National Quantum Mission has committed ₹6,003 crore to building indigenous quantum capability. The Department of Science and Technology have published a national quantum-safe cryptography roadmap. NIST has finalised the world's first post-quantum cryptographic standards: ML-KEM, ML-DSA, and SLH-DSA — the product of an eight-year global effort. The direction of travel, for regulators in Washington, Brussels, and New Delhi alike, is the same: classical encryption must be replaced, on a defined timeline, and the organisations that act now will choose the terms of their own transition.

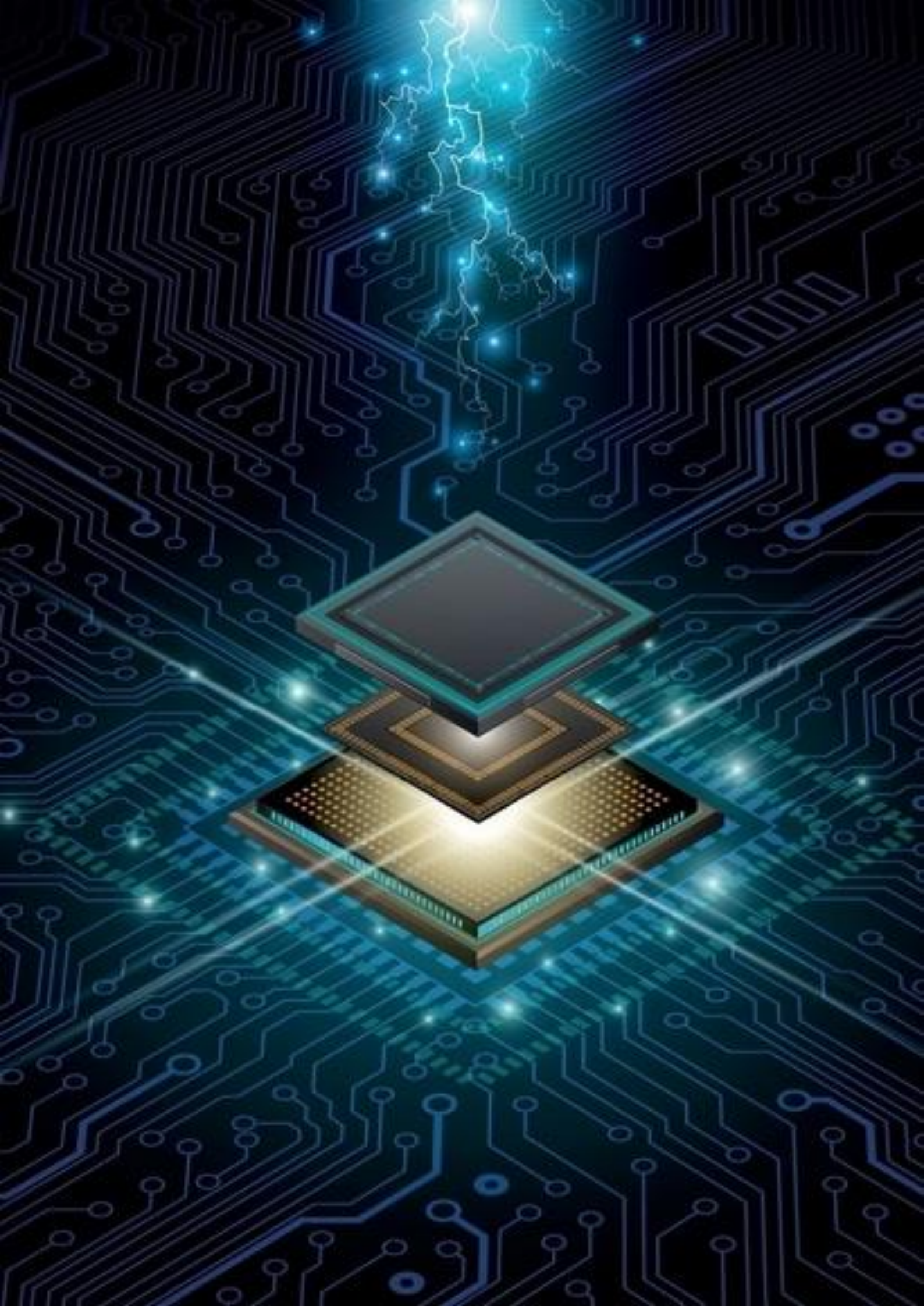
What is missing is not policy intent, rather – a concrete action by organizations. From the consulting lens, we have seen that cryptographic risk falls through the governance gap for it being - too technical for the risk team, or too strategic for the IT team, or even in a long-horizon for a Board agenda which is crowded with short-term pressures. This can lead to an organisational posture which is neither managed nor justifiable: cryptography deployed by third party contractors years ago, was not inventoried or governed, and quietly accumulated into a liability which will likely come to forefront in an unpleasant way.

From the technology perspective, we have seen a major failure - point solutions which are sold as migrations. This includes multiple partial augmentations: a vendor integration, a protocol upgrade, a PQC layer bolted onto infrastructure that was never designed to carry it. These are not migration programmes. They give an impression of action without much substance in it. The real cryptographic agility is the true ability to comprehend what you have, govern it responsibly, and update it systematically whenever standards require, and not to be agreeable with off the shelf solutions. It has to be built into the DNA of the organisation.

The answer we offer in this guide is - Ownership. Not panic. Not compliance theatre. This entails a well-thought-out decision by CISOs, CIOs, CTOs, Chief Risk Officers, and Boards to understand the cryptographic infrastructure which their enterprises depend on. This is to be coupled with active governance, and systematic migrations within the adequate transition window being open. India's enterprises did not build the internet. They inherited it, along with its vulnerabilities. But the organisations that act with clarity and deliberateness now, that treat cryptographic agility not as a technical project but as a governance capability will be the ones that define the new standard of digital trust in India's next decade of growth. What we need is not a point solution, but a process that needs to be put in place, to govern, own and manage cryptography in enterprises. We hope this guide is a practical first step in that direction.

DEVROOP DHAR
Co-founder & CEO,
Primus Partners

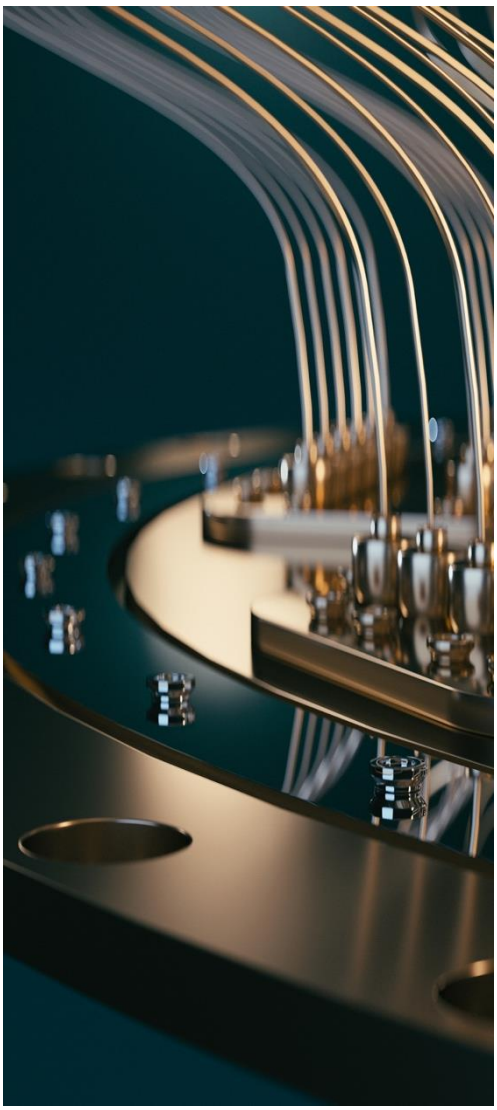
PRASANNA RAVI
CEO and Founder,
PQ Station



Executive Summary

The Quantum Security problem is Urgent. Global efforts target quantum machine readiness by 2029. Currently, critical information may be vulnerable in a "harvest now, decrypt later" state. Organizations must commence with a 90-day quantum risk assessment, followed by controlled Post Quantum Cryptography implementation solution. Begin Now.

Cybersecurity threats are evolving faster than most organisations can respond. Ransomware, supply chain attacks, identity fraud, and AI-enabled intrusions dominate today's risk registers. But regulators, intelligence agencies, and the world's largest technology companies are now drawing attention to a different category of threat, one that operates on a longer horizon and carries consequences that cannot be undone after the fact.



The World Economic Forum, Gartner, and the US Cybersecurity and Infrastructure Security Agency have all identified quantum computing as one of the defining cybersecurity risks of the coming decade. Unlike most cyber threats, it does not arrive suddenly. It approaches gradually and organisations that wait until it arrives will find that the window to protect themselves has already closed.

The reason is straightforward. The security of every digital transaction i.e. every banking payment, every government communication, every identity verification, every signed contract rests on a mathematical foundation called Public Key Infrastructure (PKI).

PKI works because certain mathematical problems are extraordinarily difficult for today's computers to solve. Quantum computers are being engineered to solve precisely those problems. When they do, the encryption protecting decades of sensitive data will no longer hold.

India has built one of the world's most ambitious digital public infrastructure (DPI) programmes backed by: UPI, Aadhaar, DigiLocker, GSTN are all resting on this same cryptographic foundation. The data flowing through these systems today such as financial records, identity data, healthcare information, regulatory filings will remain sensitive for years, in many cases decades. Sophisticated adversaries may have initiated archiving encrypted data, with the intention of decrypting it once quantum capability arrives. This is not a future risk. The data collection is happening now.

The regulatory signal is unambiguous. The National Institute of Standards and Technology (NIST), USA published the world's first post-quantum cryptography (PQC) standards in August 2024. In the case of India, in February 2026, the Department of Science and Technology (DST) released a landmark report covering the quantum-safe cryptography roadmap. The direction of travel is set. The organisations which navigate this transition successfully will not be those with the fastest technical response when the threat materialises. They will be those which have already taken a pro-active ownership of their cryptographic infrastructure, have established governance over it, and are migrating it systematically.

This whitepaper is a practical guide to taking that ownership. It is written for CISOs, CTOs, Chief Risk Officers, and the boards and executive committees to whom they report. It requires no technical background. It explains what is at stake, maps the Indian regulatory landscape, introduces the distinction between organisations that manage their security posture actively and those that do not, and offers a structured approach to building a quantum-safe migration programme that is proportionate, prioritised, and sustainable.

The message is not one of alarm. It is one of clarity: the organisations that act with deliberate ownership today will be safe. Those that defer will face a significantly harder problem and a shrinking window in which to solve it.

No panic. Just ownership.

Table of Contents

INTRODUCTION

The digital systems that underpin modern economies, right from financial transactions and identity verification to healthcare records and government services rest on a foundation that most organisations have never had reason to examine. That foundation is cryptography: the mathematical layer that makes data confidential, signatures verifiable, and communications trustworthy. For decades, it has worked invisibly and reliably. The quantum era is about to change that.

What is Quantum?

Quantum mechanics is the branch of physics that describes how matter and energy behave at the subatomic scale. Unlike classical computers, which process information as binary bits that are either a definitive zero and one simultaneously, which is a property called - Superposition. Coupled with entanglement, the ability of qubits to be correlated in unique ways which do not have classical analogue and interference, amplifies the correct computational paths while cancelling the incorrect ones. This means that Quantum processors can evaluate vast solution spaces, which classical architectures cannot. This makes them uniquely powerful in solving certain subset(s) of computationally hard problems in a exponentially faster time than the classical computers.

This is not an incremental improvement on existing computing power. **It is a different computational paradigm.** For most business applications it is inventory optimisation, simulation, machine learning at scale, drug discovery, quantum computing promises accelerated performance that classical hardware cannot match.

For cryptography, the implications are more urgent: the mathematical problems on which today's encryption depends are precisely the class of problems that quantum algorithms are engineered to solve efficiently.

What Are the Objectives of Adopting Quantum?

Quantum technology is being pursued simultaneously on two fronts. The first is **offensive capability:** the development of quantum computers powerful enough to perform computations that no classical system can execute within a practical timeframe, with applications spanning materials science, pharmaceutical research, financial modelling, logistics, and artificial intelligence. The second, and for the purposes of this paper, the more pressing is **defensive readiness**: the transition of cryptographic infrastructure away from algorithms that quantum computers will eventually be able to defeat, towards standards designed to remain secure against both classical and quantum attack.

For Governments and national competitiveness agencies, quantum technologies help with: advances in navigation, medical imaging, environmental monitoring, etc. Further, quantum communication infrastructure offers a deeper possibility of secure data transmission; In addition, quantum computing leadership is increasingly seen as a strategic priority which is comparable to semi-conductor capability or even, access to space. The countries which will focus on developing robust quantum expertise will shape the economic opportunity as well as the security landscape of the next generation.

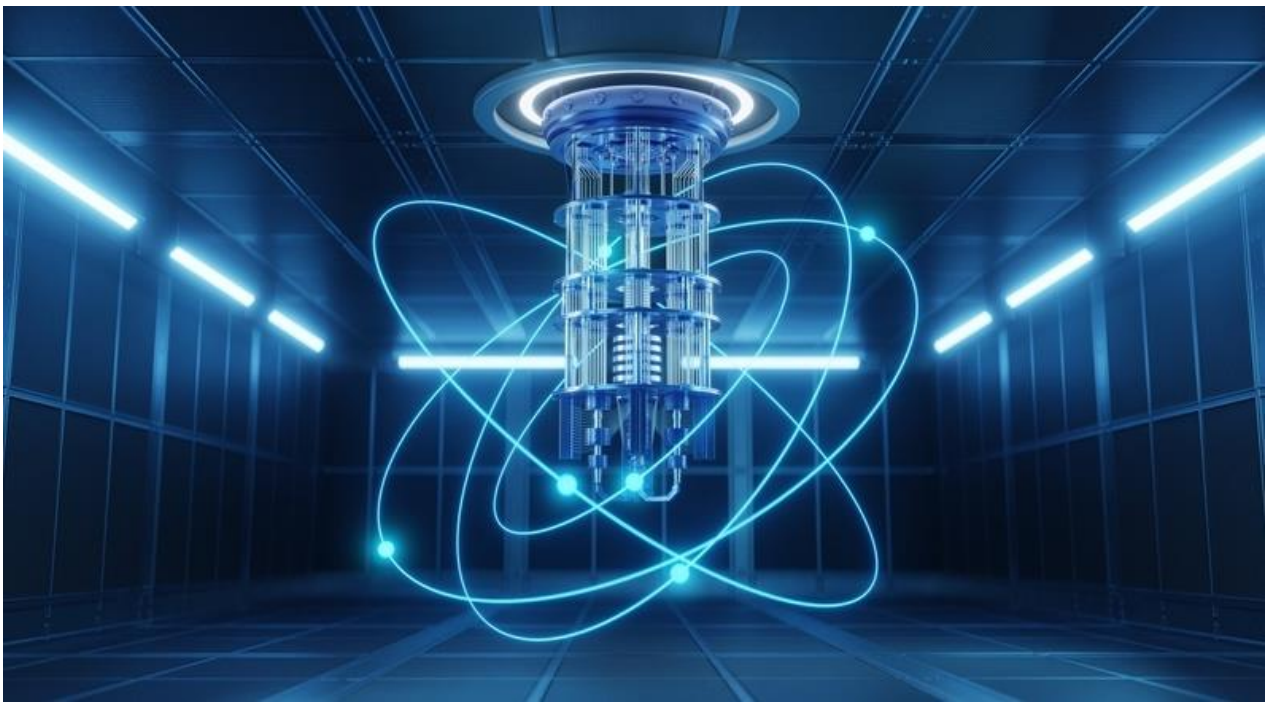
What are the Benefits?

The benefits of quantum technology are spread across two durations.

First, in the medium to longer term scenario, quantum computing is anticipated to accelerate drug discovery by simulating molecular interactions at a level which classical computers cannot achieve, augment the accuracy of climate and financial risk models, optimise supply chains and energy grids; and also, advance machine learning by training models at speeds and scales not otherwise possible. Second, in the short-term priorities, Quantum sensing is already delivering precision measurement capabilities in a range of sectors i.e. medical imaging defence, geospatial, etc.

In the **nearer term,** and for the enterprise organisations that this paper addresses, the most tangible benefit of engaging with quantum now is a defensive one: quantum-safe migration. **Organisations that complete the transition to post-quantum cryptographic standards will have eliminated one of the most consequential long-horizon security risks facing digital infrastructure today. This will have eliminated the possibility of quantum attacks against the data they hold and the infrastructure that they manage to provide services to their customers.**

They will hold an auditable, governed cryptographic posture that regulators are increasingly requiring and that counterparties and customers are beginning to ask about. And they will have built the organisational capability i.e. cryptographic agility, to respond to future cryptographic transitions without the cost and disruption of having to start from the beginning again.



What is happening Globally in this Space?

The global quantum landscape is moving with an urgency that few anticipated even five years ago.

The **United States** has invested substantially through its National Quantum Initiative, with dedicated programmes across NIST, DARPA, and the Department of Energy**. In August 2024, NIST published the first finalised post-quantum cryptographic standards: ML-KEM, ML-DSA, and SLH-DSA and it is the product of an eight-year international standardisation effort.** US federal agencies have been directed to begin migration planning on the basis of these standards, and the intelligence community has set internal timelines that the enterprise sector is expected to follow.

The **European Union** has channelled significant funding through its Quantum Flagship programme, covering hardware, software, communication, and standardisation workstreams. The European Union Agency for Cybersecurity (ENISA) has issued detailed post-quantum migration guidance for critical infrastructure operators, and several EU member states have established national quantum strategies with defined milestones..

The **United Kingdom's** National Quantum Strategy commits to making the country a leading quantum-enabled economy, with specific workstreams on quantum-safe communications. China has reportedly invested substantially in both quantum computing hardware and quantum communication infrastructure, including an operational quantum-secured communication network spanning thousands of kilometres.

In the **private sector**, the acceleration is equally visible. Recently, **Google announced that it was pulling forward its internal deadline for completing a quantum-safe cryptographic transition to 2029, citing the pace of hardware advancement.** IBM, Microsoft, and many specialist quantum firms, including those focused on post-quantum security tooling are investing at a rate that reflects a shared conviction: the transition from laboratory to commercial-scale capability is no longer a matter of if, but when. Research published in early 2026 suggested that qubit requirements to break widely deployed encryption standards could be substantially lower than previously estimated, compressing the timeline

What efforts has India undertaken in this space?

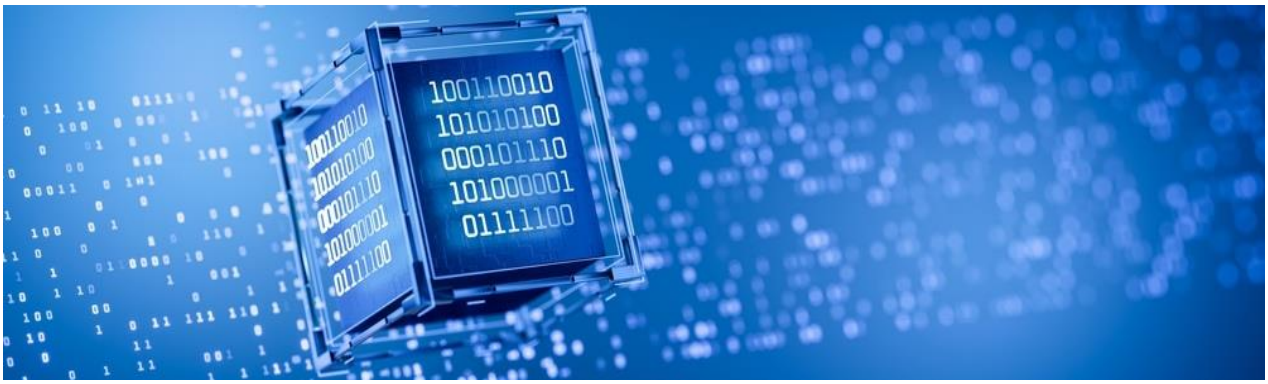
India's commitment to quantum is substantial and well-structured. The National Quantum Mission was approved by the Union Cabinet in 2023 with an allocation of INR 6,003.65 crore over eight years, highlighting a significant public investment in recent times in Emerging Technology in India.

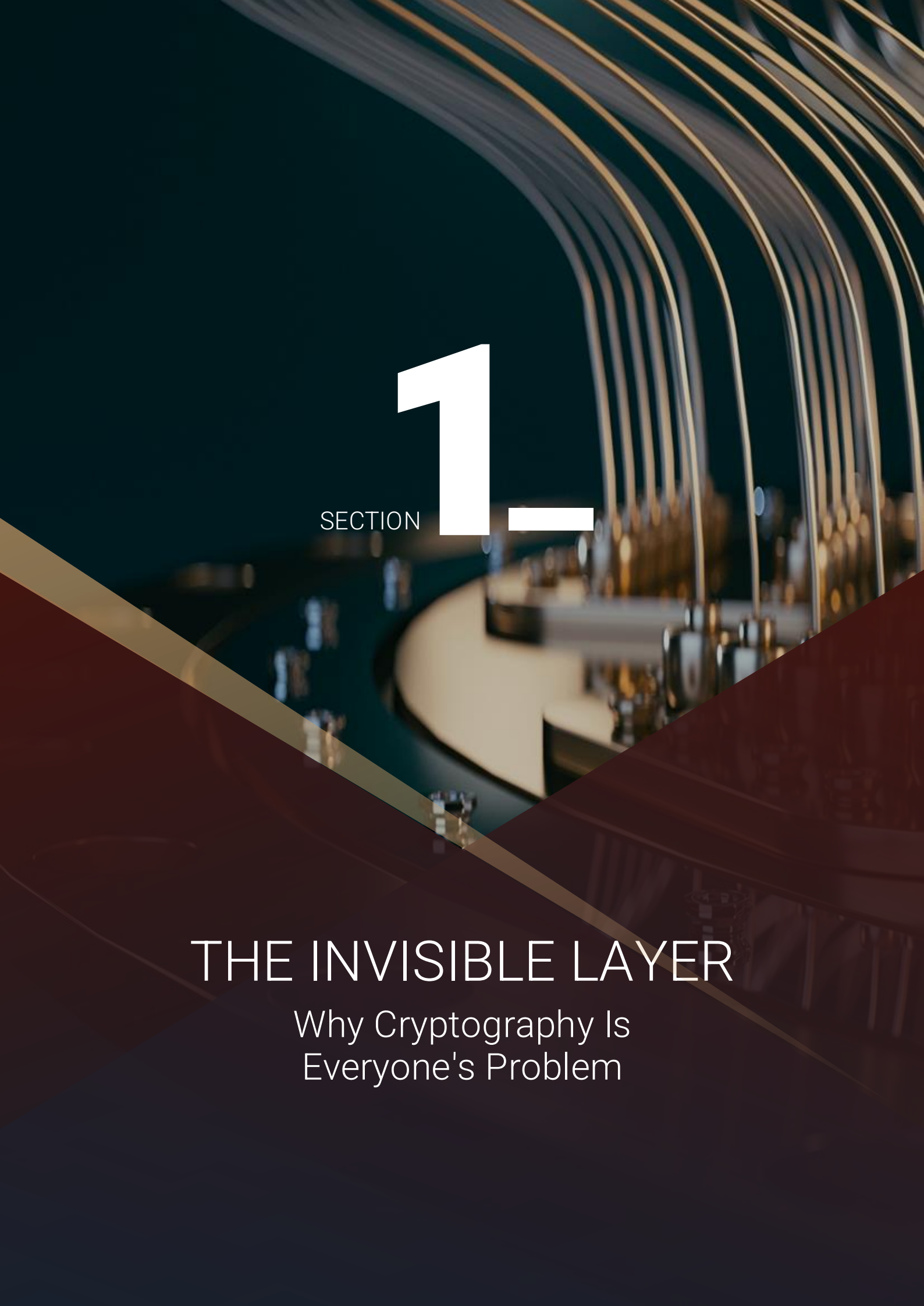
This Mission is backed by four strong technological pillars i.e. quantum computing; quantum communication; quantum sensing and metrology; and quantum materials and devices. Each of these pillars has defined milestones, and the programme is charted to develop indigenous, in-house capability rather than relying on technology transfer

On the cryptographic front, the DST quantum-safe cryptography roadmap from February 2026 aligns the country's migration expectations with the USA's NIST post-quantum standards from August 2024. Further, CERT-In has initiated embedding post-quantum readiness in its guidance for critical information infrastructure operators. The RBI's Technology Vision documents have also signalled quantum computing as an emerging risk to financial infrastructure, highlighting that sector-specific regulatory guidance is a near-term expectation rather than a distant consideration.

India's academic and research institutions have been active contributors to this effort. The Indian Institutes of Technology and the Indian Institute of Science have established dedicated quantum research groups, and the Technology Innovation Hubs established under the National Quantum Mission are designed to bridge the gap between fundamental research and applied deployment. In the private sector, a nascent but growing ecosystem of quantum-focused companies which are spanning hardware, software, and security, is beginning to emerge, supported by both domestic and international capital.

The policy architecture is in place. The regulatory signal is becoming progressively clearer. What the National Quantum Mission has established at the level of national strategy, this guide addresses at the level of enterprise action: how the organisations that make up India's digital economy should understand their quantum exposure, govern their cryptographic infrastructure, and build the migration programmes that the coming decade will require of them.





SECTION 1_

THE INVISIBLE LAYER

Why Cryptography Is Everyone's Problem

1.1

The Invisible Layer of Trust

Every digital transaction, every payment, login, and signed document, is protected by an invisible mathematical lock called PKI. Quantum computers are being built to break that lock.

Each time a customer opens their banking app to check their balance, something intangible happens. Before any amount features on the screen, a handshake occurs between the customer's device and the bank's server, which performs a cryptographic communication with the aim to create a secure, authenticated, private channel. Nothing is visible to the customer. Possibly, the bank's front-end developers do not lay much emphasis on this. However, without this negotiation, the transaction is at risk: readable by any stakeholder with access to the network; or forgeable by someone who chooses to fabricate it.

This invisible layer of trust is Public Key Infrastructure (PKI). It is the cryptographic system that underlies not just banking apps, but every secure website, every digital signature on a contract, every authentication token, every VPN tunnel, every API call between enterprise systems. It is the reason a patient's medical records can travel securely between a hospital and an insurer. It is the reason a property transaction can be registered digitally with the confidence that the signature on the document is genuine. It is the reason Aadhaar-linked e-KYC works.

PKI is invisible not because it is unimportant, but because it works It has worked reliably for decades, secured by mathematical problems that classical computers cannot solve in any practical timeframe. That reliability has bred a kind of institutional invisibility. Cryptography became infrastructure: assumed, not managed; present, not audited; foundational, not reviewed. So, organizations kept accumulating what we refer to as “cryptographic debt” which is largely invisible in most organizations as of today. The quantum era is about to make the invisible very visible indeed.

1.2

The Quantum Threat

Quantum computers solve the math which protects today’s encryption. Adversaries may already be collecting encrypted data today to decrypt it later. The quantum threat is not hypothetical, the collection has already commenced.

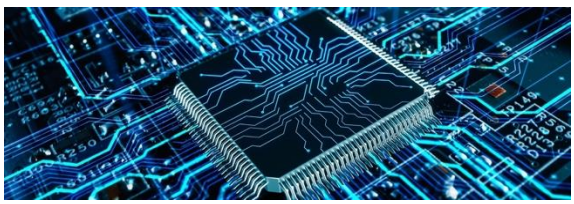
The mathematical problems that make PKI secure today is factoring large numbers, solving discrete logarithms, etc. are not universally hard. They are hard for classical computers. However, a quantum computer, exploiting the principles of superposition and entanglement, approaches these problems in a fundamentally different way. Where a classical computer must try solutions sequentially, a sufficiently powerful quantum computer can evaluate vast numbers of possibilities simultaneously. The algorithms that have protected the world's digital infrastructure for over thirty years dissolve against this capability. This is not theoretical physics speculation, but something we know can be realized provided a sufficiently large quantum computer.

Realising this threat, standardization bodies and government agencies around the world have been trying to standardize cryptographic algorithms that can resist quantum attacks.

This is not theoretical physics speculation. In August 2024, the US National Institute of Standards and Technology published the first three finalised post-quantum cryptographic standards, the product of an eight-year global competition to find algorithms that quantum computers cannot break. The standards exist because the threat is real, the timeline is credible, and the migration window is finite.

The most urgent dimension of the threat is one that does not require a quantum computer to exist today. Sophisticated adversaries such as nation-state intelligence agencies, in particular may be looking at intercepting and archiving encrypted network traffic, with the intention of decrypting it once quantum capability arrives. Security researchers call this **Harvest Now, Decrypt Later (HNDL).** For Indian enterprises processing long-lived financial contracts, identity records, and regulatory filings, the data being encrypted today is precisely the data most at risk. The attack on it has already begun. The decryption event is simply deferred.

The question facing every enterprise is therefore not "when will quantum computers arrive?" It is "how long will our data remain sensitive, and is that longer than our migration will take?" For most organisations handling financial, health, or identity data, the honest answer demands action now.



1.3

Why the Clock Is Already Running

India's most critical digital systems backed by UPI, Aadhaar, DigiLocker, GSTN — rest on the same cryptographic foundation that quantum computers will eventually break. The data flowing through them today will still be sensitive long after that capability arrives.

The systems underpinning India's digital economy rest on this same cryptographic foundation:

- **UPI:** 18+ billion monthly transactions authenticated and secured by classical cryptographic protocols
- **Aadhaar:** 1.4 billion biometric identity records, linked to financial, healthcare, and government services through PKI-secured authentication
- **DigiLocker:** 270+ million users storing and sharing digitally signed documents whose validity rests on the unforgeability of classical digital signatures
- **GSTN:** The tax infrastructure of a $3.7 trillion economy, secured by the same RSA and ECC algorithms that quantum computers will eventually be able to break

None of these systems are currently vulnerable. The threat is not today's. But the data flowing through these systems today that is, loan agreements, biometric records, tax filings, property registrations, etc., will still exist and still matter in 2030, 2035, and beyond. And the adversaries which may be looking at opportunities for intercepting and archiving that data today are counting on that.

1.4

The Ownership Imperative

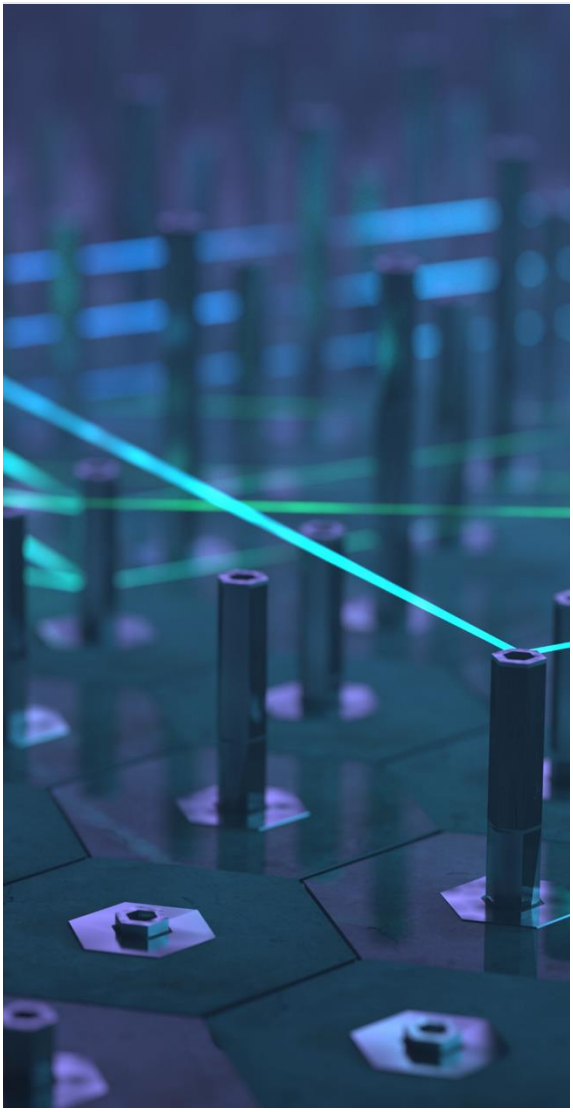
Every global regulator has reached the same conclusion: migration from classical encryption to quantum-resistant standards is not optional. The only question left is how fast, and in what order. Organisations that act now choose the terms of that transition. Those that wait will not.

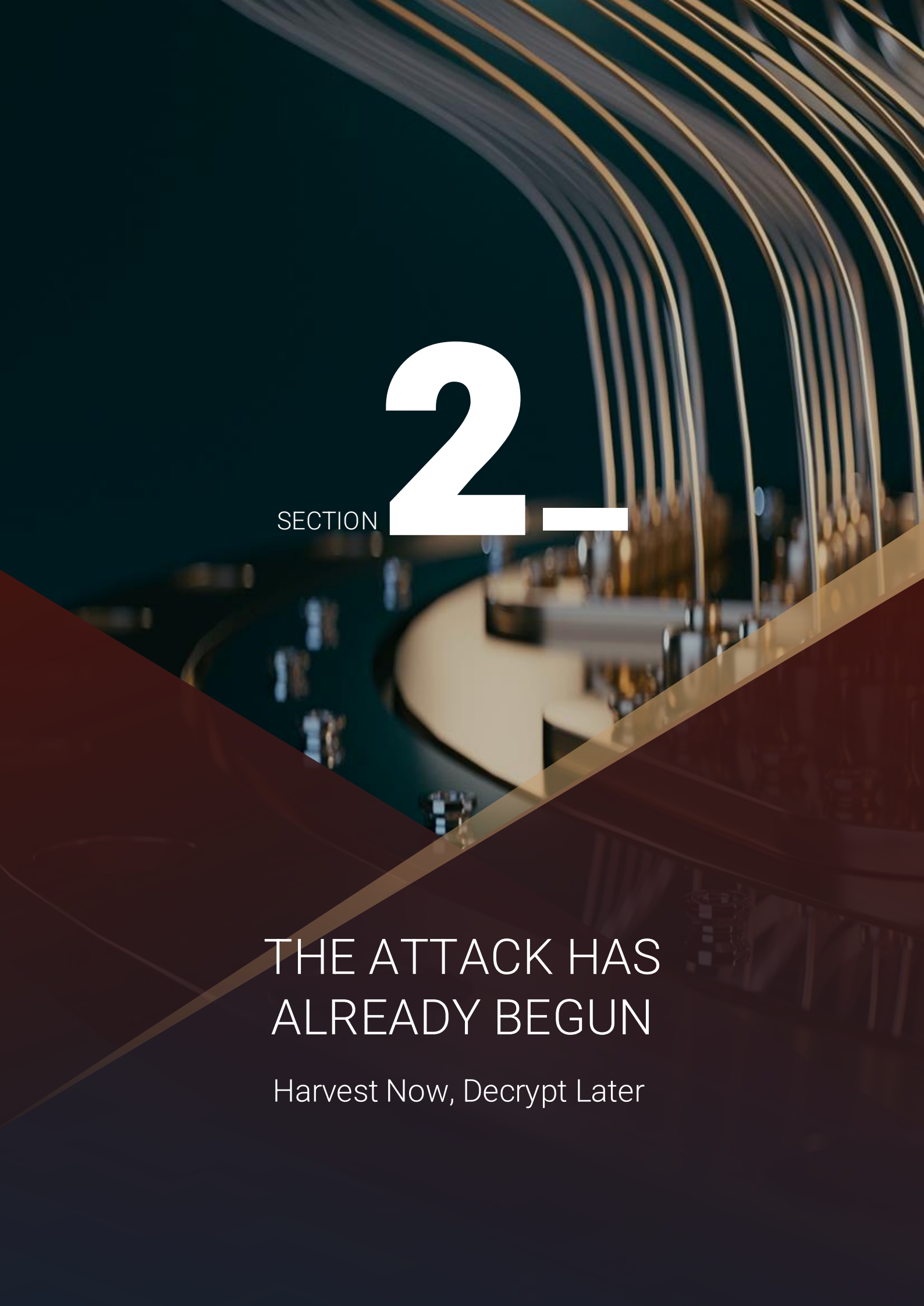
The most important reframe for any organisation approaching quantum-safe migration is this: the question is not whether to migrate, but when, how, and in what order.

Every credible regulatory body such as the NIST in the United States, European Union Agency for Cybersecurity (ENISA) in Europe; and DST, MeitY and CERT-In in India has arrived at the same conclusion. Classical public-key cryptography must be replaced with quantum-resistant algorithms on a defined timeline. The standards exist. The regulatory signals are clear. The only remaining variable is organisational ownership.

Whoever takes ownership of their cryptography faster, who knows what they have, governs it deliberately, and migrates it systematically will be ready. Others will not.

The question is not whether quantum computers will eventually break today's encryption. They will. The question is whether your organisation will be ready when they do.





SECTION 2_

THE ATTACK HAS ALREADY BEGUN

Harvest Now, Decrypt Later

2.1

A Threat That Does Not Wait for Tomorrow

Attackers don't need a quantum computer today. They are intercepting and storing encrypted data right now, ready to decrypt it the moment quantum capability arrives. The attack is already underway, only the decryption is deferred.

The most dangerous aspect of the quantum threat to cryptography is a widely misunderstood one: an adversary does not need a working quantum computer today to begin exploiting it.

The strategy is straightforward, and it is almost certainly already underway. A sophisticated attacker i.e. a nation-state intelligence agency, a well-resourced criminal syndicate, or a hostile foreign power — intercepts and archives encrypted network traffic today. The data is unreadable now. It does not matter. Once a sufficiently powerful quantum computer becomes available, the archived ciphertext can be decrypted retroactively. The attacker harvests now and decrypts later.

Security professionals call this strategy: Harvest Now, Decrypt Later (HNDL) and its signature-focused variant, Trust Now, Forge Later (TNFL). The first variant compromises confidentiality, while the second variant compromises integrity. This means an attacker who captures a digitally signed document today can, forge a valid-looking signature retrospectively using a future quantum computer. This is also applicable in the case of a legal contract - a land registry record, a pharma approval, or a financial settlement instruction, where the the consequences are critical and irreversible.

KUNJ TANDON

CEO, I-Hub Quantum Technologies Foundation

The Digital Personal Data Protection Act, 2023 makes Indian enterprises accountable for the safety of a range of digital data. However, data encrypted with current protocols becomes vulnerable to Quantum enabled attacks. Quantum safe encryption becomes critical for Indian enterprises to keep data safe from harvest-now-decrypt-later scenarios for enterprises. Migrating to quantum safe data storage and quantum safe data exchange is a business priority right now.

2.2

Why This Changes the Migration Timeline Completely

The right question is not "when will quantum computers exist?" It is "how long will our data stay sensitive?" If the answer is more than eight years, the migration window is already open and closing.

The HNDL/ TNFL dynamic fundamentally reframes when the migration problem becomes urgent. **The relevant question is not: "When can a quantum computer break our encryption?" The relevant question is: "How long will our current data remain sensitive?"**

In the case of a retail bank, a loan agreement which is being executed today may carry legal and financial significance for 20, 30 years or even longer. In a pharmaceutical company, clinical trial data results may be referenced for decades. For a Government department, a policy drafted today may remain sensitive. It is likely all these examples may be well beyond a clear quantum computing timeline. Any data which is being encrypted right now is most at risk, because this data is highly likely to be relevant when quantum decryption becomes possible.

This creates what security researchers call the problem of data longevity i.e. the enterprises with the longest data lifecycles face deadline for migration for sooner, irrespective of when quantum computers actually arrive.

2.3

The Shrinking Timeline

The engineering gap between today's quantum hardware and cryptography-breaking capability is shrinking much faster than expected. Google has already moved its internal deadline to 2029. The timeline is no longer theoretical.

Until recently, the standard estimate for breaking RSA-2048 required nearly 20 million physical qubits on a fault-tolerant quantum computer. This figure has been updated. In February 2026, Iceberg Quantum published a research paper demonstrating an architectural approach that could factor RSA-2048 with fewer than 100,000 physical qubits, a reduction of over 99% from the 2019 consensus. While this is a research result and not yet a deployed system, the trajectory is clear: the engineering distance between today's quantum hardware and a cryptographically relevant quantum computer is closing faster than anticipated.

Industry is responding accordingly. Google has moved its internal deadline for completing its quantum-safe cryptography transition to 2029, a full six years ahead of earlier estimates — citing the accelerating pace of quantum hardware development as the reason for the pull-forward. When the company that arguably leads the world in both quantum computing research and large-scale cryptographic infrastructure sets a 2029 internal target, it is a signal the enterprise world cannot afford to ignore.

The year commonly cited for "quantum relevance" has moved from "beyond 2035" to somewhere in the 2030–2034 window in mainstream expert consensus. Given that a serious enterprise quantum-safe migration programme takes three to five years to complete, the window to begin is not the arrival of quantum relevance. The window to begin is now. As we speak, the migration window is becoming smaller, as it is unclear how fast the research in quantum computing as well as the quantum computing industry is advancing. So, these are certainly uncertain times from a cryptographic standpoint for entire economies.

2.4

What this means for Indian Enterprises

India's digital scale: 18 billion monthly UPI transactions, 1.4 billion Aadhaar records — makes it a high-value harvesting target. The longevity of that data makes the exposure uniquely severe.

India presents a particularly acute version of the HNDL problem for three reasons.

First, **scale of interception exposure**. India processes over 18 billion UPI transactions monthly, all secured by classical cryptographic infrastructure. The volume of encrypted financial traffic passing through Indian networks makes it a high-value harvesting target for any actor with sufficient network access and storage capacity.

Second, **longevity of identity and financial data**. Aadhaar biometric records, income tax data, property registrations, insurance policies, and long-tenure bank loans are among the most long-lived data assets in any economy. These records, once compromised through a future HNDL decryption event, cannot be recalled or reissued in the way a compromised password can be reset.

Third, **the Trust Now, Forge Later risk to digital governance**. India's digital public infrastructure backed by Aadhaar-linked eKYC, DigiLocker document verification, digital signatures on government approvals, rests on the unforgeable nature of today's cryptographic signatures. A future quantum capability to forge those signatures would not merely compromise individual transactions; it would undermine the integrity of the entire digital trust infrastructure that India's digital economy has been built upon

2.5

The Attacker's Calculus

Nation-states with advanced intelligence capabilities are not waiting. They are systematically collecting encrypted data from high-value sectors today. For organisations in defence, finance, pharma, or government, this is a present-day risk and it is definitely not a future one.

Several Nation-state intelligence agencies possess the technical infrastructure to intercept large volumes of encrypted traffic at scale, and they have well-documented long-term data collection programmes. These agencies have every incentive to archive encrypted data from sectors where today's secrets will have value a decade from now: defense procurement, pharmaceutical intellectual property, financial system architecture, strategic infrastructure blueprints, and diplomatic communications.

For organizations operating in any of aforementioned sectors, or processing data on behalf of government agencies, the HNDL threat is not in theory. It is a real time data collection risk with a future risk of decryption which cannot be remediated beyond a reasonable time.

SECTION 3_

INDIA'S REGULATORY LANDSCAPE

The Signals Are Clear

3.1

India's National Quantum Mission

India has committed ₹6,000 crore to the National Quantum Mission: one of Asia's largest quantum investments. The Government is treating quantum-safe security as national infrastructure, not just a technology trend.

India committed **₹6,000 crore** (approximately USD 720 million) to the National Quantum Mission in 2023, making it one of the largest national quantum investments in Asia. The Mission encompasses quantum computing hardware, quantum communication, quantum sensing, and quantum-safe cryptography — recognising that the transition to post-quantum security is as much a national infrastructure priority as it is an enterprise risk management question.

Within the Mission's cryptography mandate, DST published India's quantum-safe cryptography roadmap in February 2026. The roadmap aligns with NIST's finalised the Post-Quantum Cryptography (PQC) standards and establishes a phased migration expectation for critical information infrastructure operators, financial institutions, and government agencies. **The roadmap does not yet carry the force of binding regulation in most sectors, but it is the clearest signal yet that India's regulatory posture on quantum-safe migration has moved from awareness to action.**

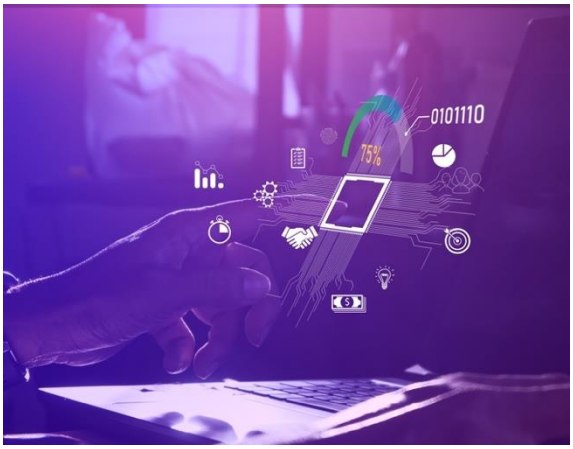
3.2

Financial Sector Guidance

RBI, SEBI, and MAS Singapore have all flagged quantum computing as an emerging financial risk. Binding compliance guidance is expected within three to five years — the same time a migration programme takes to complete. Early movers will be ready; late movers will not.

The RBI has not yet issued sector-specific post-quantum cryptography guidance, but the direction of travel is visible. RBI's Innovation Hub position paper on quantum security explicitly identifies quantum computing as an emerging risk to the security of financial infrastructure and has outlined practical steps for protection against quantum threats.

SEBI has similarly flagged quantum threats in its risk framework discussions. Market infrastructure institutions — stock exchanges, depositories, and clearing corporations — handle settlement data with multi-year legal significance, placing them squarely in the HNDL risk category.



3.3

India's position on quantum-safe migration: A Government-Led, Mission-Driven Response

The DST Task Force has created a clear, time-bound national roadmap – from cryptographic inventory to a complete post-quantum adoption placing India among the few major economies with a structured, and mandated organizational migration roadmap in effect.

In February 2026, DST published the Report of the Task Force on the Implementation of Quantum Safe Ecosystem in India: one of the most comprehensive national quantum migration blueprints released by any major economy to date. Constituted under the National Quantum Mission (NQM) and chaired by Dr. Rajkumar Upadhyay (CEO, C-DOT), the Task Force draws on academia, R&D labs, government ministries, and industry, with a concrete mandate to move India from awareness to action. The Task Force is explicit about the Harvest Now, Decrypt Later (HNDL) threat. For a country processing over 18 billion UPI transactions monthly and holding 1.4 billion Aadhaar biometric records, the scale of exposure is uniquely severe. Inaction, the report warns, risks becoming the weakest defence.

The quantum-safe roadmap is organised around three milestones across two adoption tracks. Critical Information Infrastructure (CII) that comprises of defence (DRDO), power, telecom, banking, government, space (ISRO), and oil & gas (ONGC) operates on an accelerated timeline.

Regular enterprises follow a standard track. Organisations are classified into three personas: Urgent Adopters (CII and high-risk), Regular Adopters (moderate-risk enterprises), and Technology Providers (vendors of libraries, HSMs, PKI, and cloud services). Where an organisation spans multiple personas, the highest-risk designation governs.

Testing, Certification, and Sovereign Assurance

Alongside migration, the Task Force has defined a national framework for testing and certifying quantum-safe products, a critical step given India's ambition to prefer domestically developed solutions. Four assurance levels (L1–L4) cover the full spectrum of deployment contexts, starting from L1: Basic Conformance, L2: Secure Software & Hardware, L3: Enterprise Infrastructure and L4: Critical & Sovereign Infrastructure.

A tiered national laboratory structure supports this: Tier-1 (TEC/BIS labs) for L1, Tier-2 (STQC, CERT-In empanelled labs) for L2, and Tier-3 (to be established) for L3/L4. The full framework is expected to be operational within 12–18 months, with existing TEC approval mechanisms bridging the interim. Notably, the roadmap calls for India to develop its own national list of cryptography-dependent product categories, referencing CISA's January 2026 list.

The roadmap carries operational implications for organizational leaders in India with immediate effect. The deadlines are set by the Government with milestones clearly defined, which are as below:

- **Cryptographic asset inventories now:** CII operators must complete CBOMs and launch pilots by December 2027. Regular enterprises by December 2028.
- **CBOM mandates in procurement:** From FY 2027–28, all vendors supplying to Indian government and CII entities must submit Cryptographic Bills of Materials.
- **No new classical-only systems:** From 2028 for CII and 2030 for enterprises, all new systems procured or built must be PQC-capable.
- **Cryptographic agility as default architecture:** The ability to swap algorithms, protocols, keys, etc. without impacting operations is not an optional feature but mandatory design principle
- **Preference for indigenous solutions:** PQC, QKD, and QRNG technologies developed in India are to be prioritised, subject to performance and interoperability requirements, aligning with AtmaNirbhar Bharat.

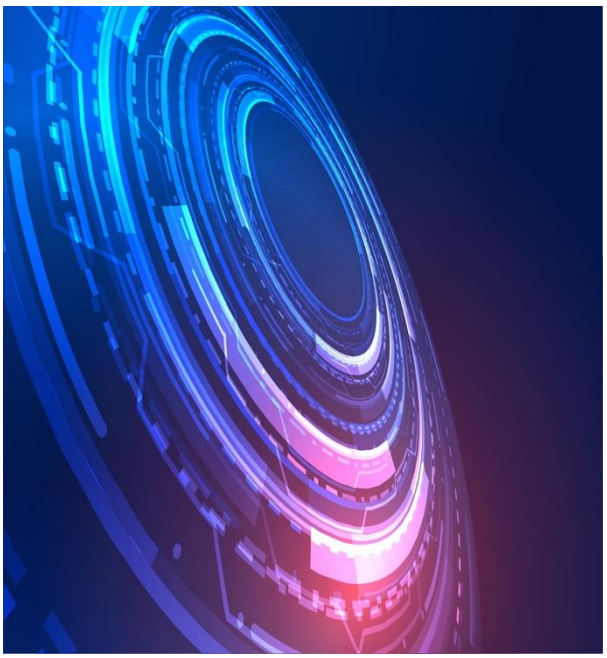
India's roadmap places it alongside the United States (full federal migration by 2035), the European Union (critical systems by 2030), and the United Kingdom (full transition by 2035), but with a distinctly sovereignty-conscious posture that privileges indigenous capability, domestic certification infrastructure, and the NQM's inter-city QKD backbone as long-term national strategic infrastructure. The policy architecture is in place. The milestones are set. For Indian enterprises, the question is no longer whether to migrate, it is whether to lead or to be compelled.[11]

3.4

The NIST Standards: The Global Foundation

The compliance requirements and associated migration timelines are in collision. Both - in three to five years timeline. Organisations which ate yet to commence, have no margin left.

The combined effect of India's National Quantum Mission, DST's February 2026 roadmap, and the USA' s NIST finalized standards creates a compliance window which is finite and measurable. Organisations operating in the space of banking and financial services, healthcare and pharmaceuticals, telecommunications, etc. should assume that compliance requirements will be coming in very soon, and the time required to undertake a serious enterprise migration is in the next three to five years. The arithmetic is clear.

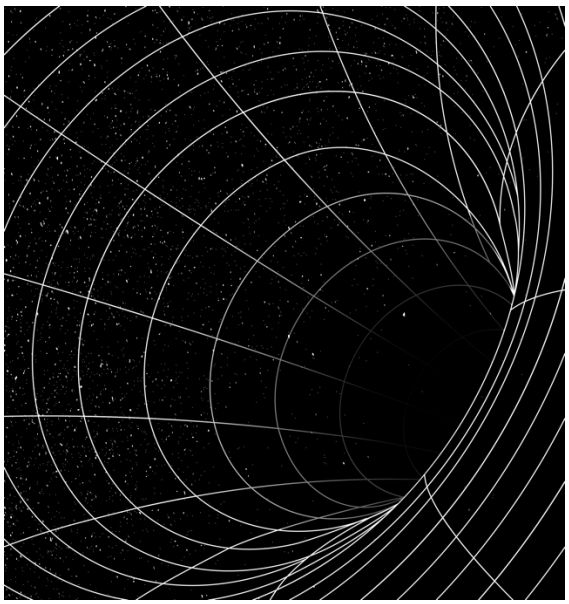


3.5

The Compliance Window Is Narrowing

Compliance requirements and migration timelines are on a collision course. Both are measured in three to five years. Organisations that have not started have no margin left.

The combined effect of India's National Quantum Mission, DST's February 2026 roadmap, and the NIST standard finalisation creates a compliance window that is measurable and finite. Organisations in financial services, healthcare, government contracting, and critical information infrastructure should assume that binding compliance expectations will arrive very soon and the time required to complete a serious enterprise migration programme is in the next three to five years. The arithmetic is stark.



3.6

Sector-Specific Priorities

The quantum threat looks different across different industries - banking, government, healthcare, and telecom, however, none is exempt. Each sector faces its own challenges of regulatory pressure, data longevity, and cryptographic dependency which must be deciphered on its own terms.

The urgency and character of the migration challenge varies by sector. The following assessments reflect the specific data longevity, regulatory exposure, and cryptographic dependency profiles of India's most exposed industries.

Banking and Financial Services

The banking and finance industry faces one of the most critical combinations of data longevity risk and regulatory scrutiny. Long term financial instruments such as mortgages, bonds, insurance policies, provident fund records, etc. create data sensitivity windows across decades. The HNDL threat is directly applicable for them. For example, a mortgage originating today will be legally binding in 20, 30 or even 40 years, which is long after quantum computers could decrypt the cryptographic protections applied at origination in a retroactive manner.

Specific first-priority migration targets for Indian banks and NBFCs:

- Transport Layer Security (TLS) infrastructure securing customer-facing applications and API gateways
- Digital signature infrastructure for loan documentation, regulatory filings, and interbank communications
- HSM (Hardware Security Module) firmware: Many HSMs require vendor-side upgrades to support PQC algorithms
- SWIFT and correspondent banking integrations, which involve third-party cryptographic dependencies
- Core banking system interfaces, where cryptographic dependencies are often deeply embedded and poorly documented

RBI's IT examination framework already assesses cryptographic hygiene. Institutions that have completed a CBOM and can demonstrate a migration roadmap will be in a materially stronger position in regulatory reviews.

Government and Public Sector

For government agencies, the **Trust Now, Forge Later** (TNFL) variant of the quantum threat carries particularly severe implications. Property registries, court records, regulatory approvals, and policy documents derive their legal validity from the unforgeable nature of the digital signatures applied at the time of creation. A future quantum capability to forge those signatures would retrospectively compromise the integrity of the entire documentary record.

Central and state government agencies involved in digital governance such as land records, company registrations, tax filings, import/ export documentation — should treat digital signature infrastructure as a first-priority migration target.

Healthcare and Pharmaceuticals

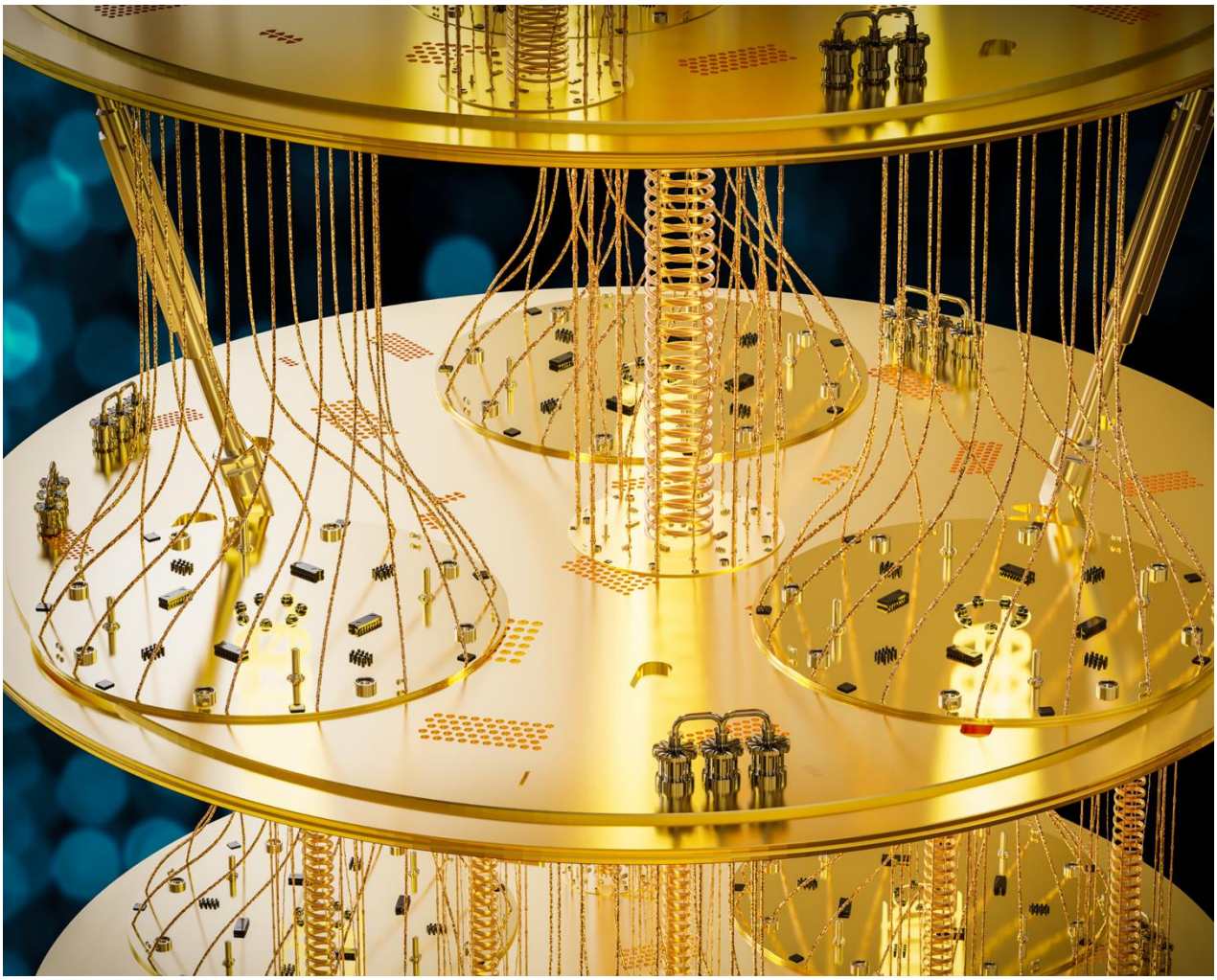
Healthcare data is among the most long-lived sensitive data in any economy. A few examples of this include: a patient's electronic health record may be of relevance both clinically and legally for their lifetime. Once genomic data is compromised, it cannot be changed. Additionally, clinical trial data which is shared with regulatory authorities also carries scientific and legal significance for a long period.

For Indian pharmaceutical companies, particularly for those operating in regulated export markets (US FDA, EMA), the quantum-safe posture of clinical data management systems will increasingly become a compliance expectation in international regulatory submissions.

Telecommunications

Telcos occupy a unique position in the quantum-safe migration landscape: they are both a target for HNDL attacks as operators of the network infrastructure through which sensitive data flows, and a critical infrastructure provider whose own cryptographic security is foundational to every enterprise that uses their networks.

5G network slice security, core network authentication, and subscriber identity management all rely on classical cryptographic primitives. Indian telcos participating in international roaming, IMS, and interconnect agreements face additional complexity from multi-party cryptographic dependencies that require coordinated migration across multiple operators.



SECTION 4_

QUANTUM-SAFE MIGRATION PROBLEM

Is Really A Cryptography Management Problem

4.1

The Problem With How Organisations Think About Cryptography Today

Most organisations don't manage their cryptography, it was embedded by vendors years ago and left untouched. This "set and forget" approach is the root of the problem. Bolting on a fix later only makes things worse. So, cryptography rarely has any ownership, management or governance in organizations today. While it might be available in a siloed manner, there has never been a central approach towards managing cryptography.

Most enterprises do not manage their cryptography. They have it.

Cryptography was embedded into their systems by vendors, by developers, by IT teams following best practices at the time of deployment. It lives inside TLS configurations, VPN tunnels, database encryption modules, and API signing certificates. It is everywhere — and in most organisations, nobody has a complete picture of where.

This is the condition of **cryptographic rigidity:** infrastructure that is fixed, invisible, and unmanaged. Algorithms are deployed once and left in place until something breaks. There is no inventory, no governing policy, no coordinated process for updates. It is not a failure of security consciousness, it is simply how cryptography has historically been treated: a solved problem, baked into standards, and never revisited.

The quantum era has ended that assumption permanently.

The instinctive response from many organisations — and from a growing number of vendors, is to treat post-quantum cryptography as an add-on. A separate appliance. A plugin.

An additional layer bolted onto existing infrastructure. This approach is not a solution. It is an acceleration of the underlying problem.

Organisations already carry enormous cryptographic debt i.e. a sprawling, undocumented accumulation of legacy algorithms, expired certificates, deprecated protocols, and inconsistent implementations built up over years of deployment without governance. Adding a PQC layer on top of this does not reduce the debt. It increases it, creating new dependencies, new inconsistencies, and new surface area that will need to be managed, or will quietly be forgotten — for years to come.

There is a further reason why the "add-on" model fails: quantum-safe migration is not a one-time event. Cryptographic standards can be weakened with time. New vulnerabilities keep emerging. Algorithms which are considered secure today, may be eliminated or be redundant - tomorrow as RSA and ECC themselves demonstrate. The long-term mandate is not to migrate only once. It is to ensure that the organisational builds capability to update and upgrade cryptographic implementations whenever necessary, in a periodic and structured manner. This capability which we refer to as cryptographic agility cannot be bolted on. It must be built into the organization's DNA.

4.2

What Cryptographic Agility Actually Means

Cryptographic agility means knowing exactly what encryption you have, governing it deliberately, and being able to update it across your entire organisation, quickly and without disruption — whenever standards change.

Cryptographic agility is the organisational capability to discover, govern, and update cryptographic implementations across an enterprise's entire infrastructure — systematically, continuously, and without disrupting operations.

An organisation with cryptographic agility can:

- **Know:** Maintain a complete, accurate, and continuously updated inventory of every cryptographic implementation across every system, including third-party and vendor-supplied components
- **Decide:** Establish and enforce a consistent organisational policy on which algorithms are approved, which are deprecated, and what the migration timeline is for each
- **Act:** Execute cryptographic updates across the full infrastructure in a coordinated, auditable, and operationally safe way
- **Adapt:** Repeat this process as standards evolve, as new vulnerabilities emerge, and as new systems are onboarded

An organisation with cryptographic agility is not immune to future cryptographic threats. But it can respond to them within months rather than years.

4.3

Migration as an Opportunity, Not Just an Obligation

Quantum-safe migration is not just a compliance exercise. It is the first time most organisations will truly own and govern their cryptographic infrastructure, and a capability that will serve them well beyond the quantum transition.

Quantum-safe migration is often framed as a technical remediation exercise. It is better understood as a governance transformation.

For most organisations, the process of preparing for quantum-safe migration will be the first time cryptography is treated as an organisational asset to be actively managed, rather than an infrastructure component to be silently inherited. That shift in posture is itself valuable, independent of the quantum timeline.

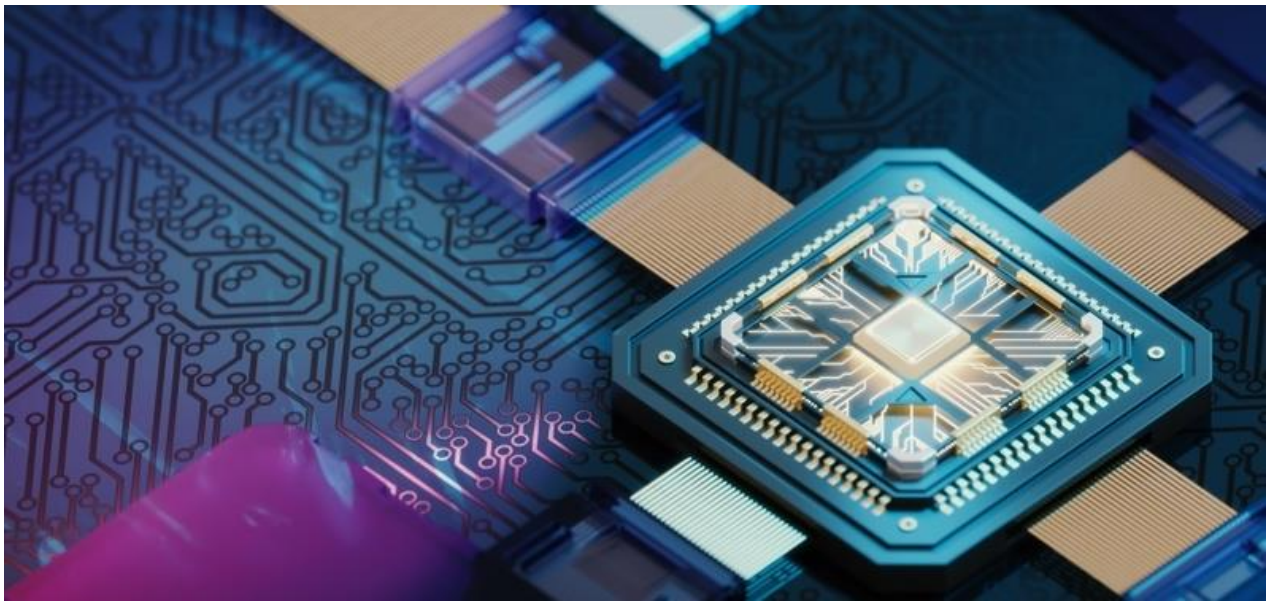
Quantum safe migration cannot be owned by a team or a unit. This is not an IT project with a completion date. This requires cryptographic synergies with IT infrastructure, security, application development, procurement, legal, and sign off by the Board. All third part contractors must be assessed. Policies must be documented and then, enforced. This concept is a standing organisational capability, which must be exercised again as standards/ policies/ systems evolve; new vulnerabilities emerge; and the enterprise's technology landscape changes.

Prof (Dr.) Anupam Chattaopdhyay
Associate Professor,
Nanyang Technological University, Singapore

In last few months, there is an accelerated growth in the capability of Quantum computers supported by - quantum device technologies, quantum error correction codes and circuit-level optimization - resulting in orders of magnitude reduction in estimated time to break standardized public-key cryptography. Migrating to quantum-safe systems, which is a massive undertaking for every organization, cannot wait anymore.

The organisations that approach migration this way by building the governance structures, the cross-functional ownership, and the cryptographic inventory processes that a real migration requires — will definitely emerge from this transition fundamentally more secure. Not just quantum-safe, but cryptographically managed.

There are no point solutions for quantum-safe migration. A tool that upgrades one protocol, one application, or one vendor integration in isolation does not constitute a migration programme. What is required is a process that is embedded into the organisation, supported by leadership, and capable of running continuously. Quantum-safe migration is the catalyst. Cryptographic agility is the destination.



SECTION 5_

MANAGING QUANTUM RISK

A Framework For Action

5.1

Start With Risk, Not Technology

Don't start with the security team, start with the risk team. Quantum must be formally registered as an organisational risk before it can have a budget, a mandate, or an owner. Everything else follows from that.

The most common mistake organisations make when approaching quantum-safe migration is to treat it as an IT project from day one, jumping straight to technical remediation before establishing what the risk actually is and to whom it belongs.

The right starting point is the risk team, not the security team.

Quantum threat must first be introduced and accepted as a formal cyber risk, that is registered in the organisation's risk register, assigned an owner, assessed for likelihood and impact, and reviewed by the relevant risk governance body. This is not a formality. Until quantum risk is formally recognised as an organisational risk, it has no budget, no mandate, and no accountability. Every enterprise has well-established processes for managing cyber risk. The objective is to route quantum risk through those same processes, not to create a parallel structure.

This means engaging the Chief Risk Officer, the Risk Committee, and where relevant the Board Risk Committee, with a clear framing: there is a credible, time-bound threat to the cryptographic foundations of the organisation's systems, and we need to understand our exposure before we can act.

5.2

Understand What Is Actually at Risk

Before asking "how do we fix this?" ask "what do we actually stand to lose?" Map your products, long-lived data, and digital trust dependencies, that map becomes the scope and the business case for migration.

Once quantum has been accepted as a formal risk, the next step is a structured risk characterisation, and this must happen at the business level before it reaches the technical level.

The core question is: **which of the organisation's products, services, and data assets are actually exposed to the quantum threat?**

This breaks down into three dimensions, namely: Products and Services; Data Exposure; and Trust Dependencies.

Products and services

Which customer-facing or operational services rely on cryptography that is quantum-vulnerable? A bank offering long-tenure loans, a telecom provider securing network infrastructure, an insurer processing medical records, a government agency issuing digitally signed documents — each has a different exposure profile. The starting point is a business-level inventory of which offerings depend on the confidentiality, integrity, or authenticity guarantees that classical cryptography currently provides.

Data exposure

Which data assets does the organisation hold that are relevant to the quantum threat? The key filter is longevity: data that will remain sensitive for eight years or more is within the harvest-now-decrypt-later window. Biometric records, financial contracts, health data, regulatory filings, intellectual property, and classified communications all qualify. The risk team needs a clear picture of where this data sits and how it is protected.

Trust dependencies

Which of the organisation's processes rely on digital signatures, certificates, or cryptographic authentication in a way that would be disrupted if those signatures could be forged? Digital contracts, e-KYC flows, API authentication, software signing, and document verification are all candidates.

This business-level risk characterisation is the output that justifies the next phase of work. Without it, the conversation with the CISO team lacks grounding — and the investment in technical migration lacks a business case.

5.3

Bring in the CISO: From Business Risk to Technical Posture

Once you know what's at risk, the CISO can build the technical response, using the same NIST framework already in use for cyber risk. Identify what you have, protect the highest-priority systems first, then detect, respond, and recover.

Once the business-level risk characterisation is complete, the CISO team can engage with the right question: given what we now know about our exposure, how does quantum threat factor into the way we manage the infrastructure and systems we are responsible for?

This is where the work becomes technical, but it should be framed within the security governance structure the organisation already uses. The NIST Cybersecurity Framework provides the right organising structure here, and it maps naturally to the quantum security context:

Identify

Build a complete inventory of cryptographic implementations across the organisation's infrastructure — what algorithms are in use, where, in what systems, protecting what data. This is the Cryptographic Bill of Materials described in Section 4. Without this inventory, none of the subsequent steps are possible. Most organisations will find this inventory does not exist in any usable form.

Protect

Based on the inventory and the business-level risk characterisation, determine which systems require immediate cryptographic protection upgrades and which can be addressed over a longer programme horizon. **Implement hybrid cryptography as a protective layer on the highest-priority systems.** Establish a formal cryptographic policy backed by approved algorithms, prohibited algorithms, key management standards and enforce it.

Detect

Establish continuous monitoring of the cryptographic posture. Certificates expire, protocols degrade, new vulnerabilities emerge, and new systems are onboarded. The CBOM must be a living document, not a one-time snapshot. **Detection also includes monitoring the threat landscape: tracking the progress of quantum computing development and the evolution of regulatory guidance.**

Respond

Define a cryptographic incident response capability. What is the organisation's process for responding to the discovery of a critical quantum-vulnerable system? What is the escalation path if a certificate tied to a quantum-vulnerable algorithm is compromised? These playbooks should be developed and tested before they are needed.

Recover

Plan for cryptographic continuity. If a system's encryption is found to have been compromised through a historical HNDL collection, what is the recovery process? Which data needs to be treated as potentially exposed? How does the organisation communicate with affected customers, regulators, and counterparties?

5.4

Every Organisation's Journey Is Different

There is no single migration schedule that fits all organisations. But the logic is universal: understand your risk first, build governance before tooling, and start now — while the window for an orderly response is still open.

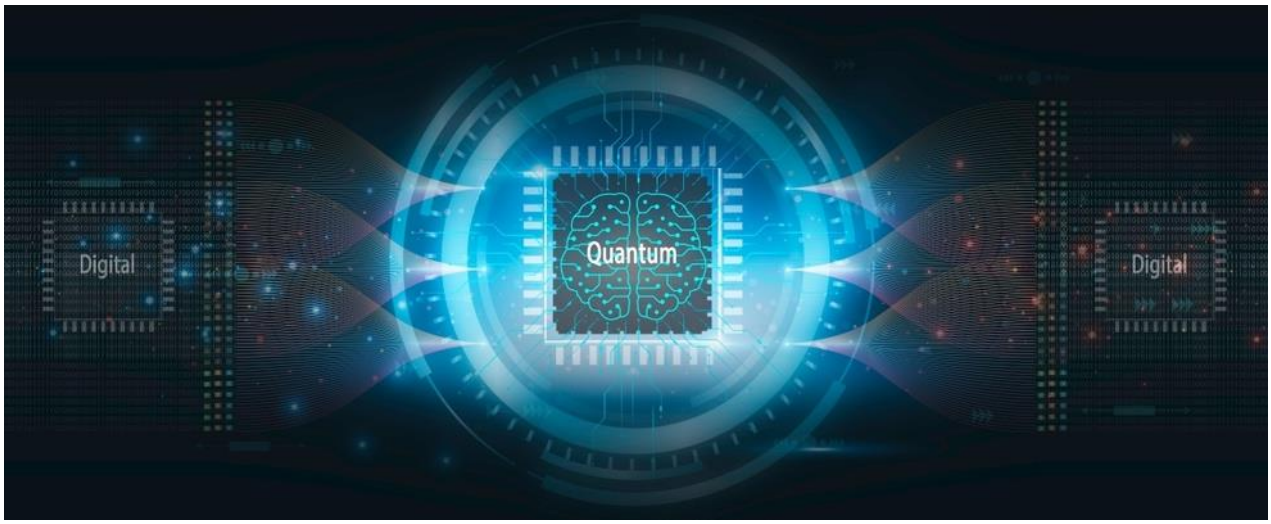
There is no universal migration timeline, and this whitepaper does not prescribe one. The appropriate pace and sequence of quantum-safe migration depends on the organisation's sector, its regulatory obligations, the longevity and sensitivity of the data it holds, the complexity of its technology estate, and its existing security maturity.

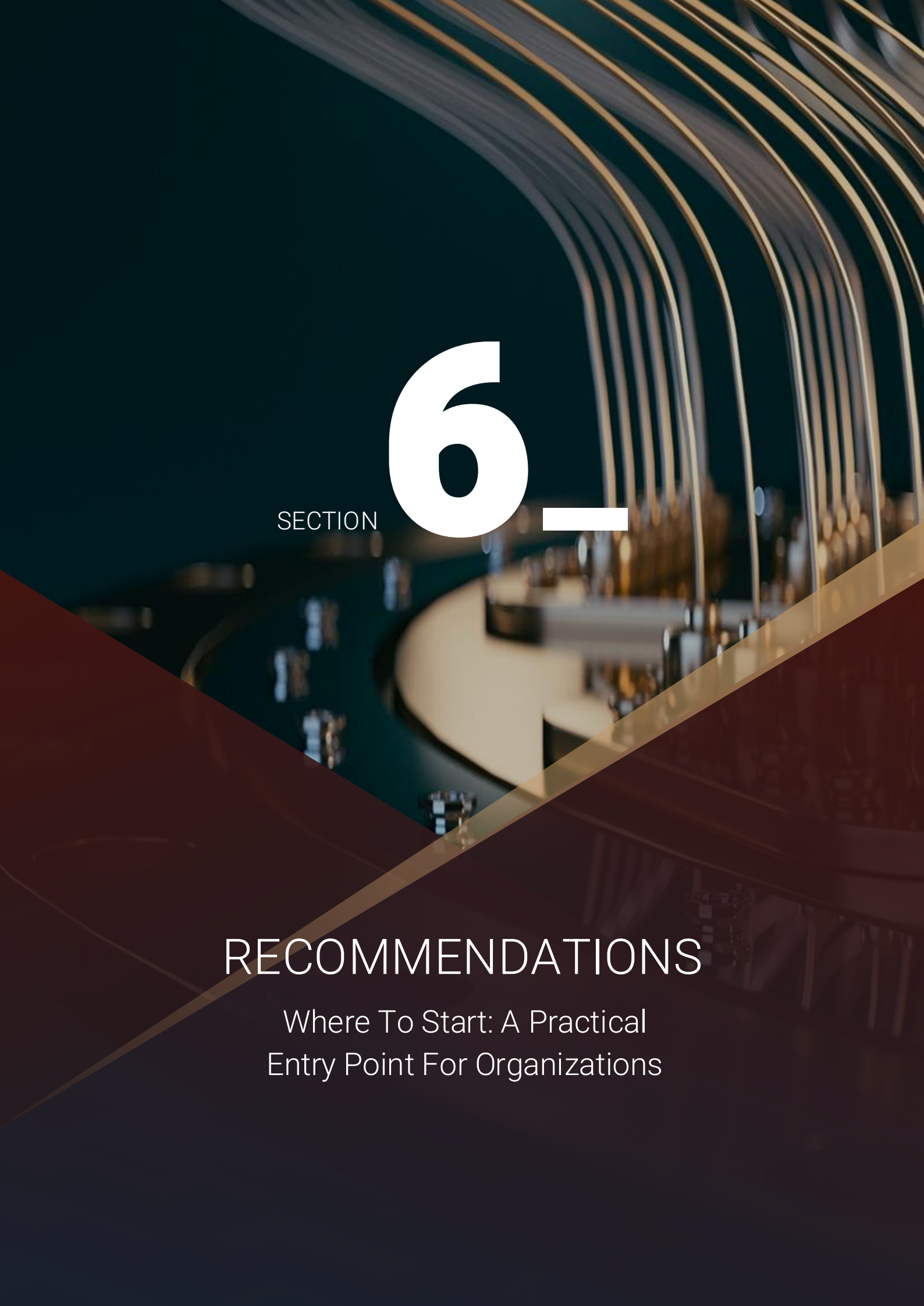
What is universal is the logic: **risk before technology, business context before technical implementation, governance before tooling.** An organisation that has formally registered quantum as a risk, characterised its exposure at the business level, and engaged its CISO team with a clear inventory and a governance framework is in a fundamentally different position from one that has not — regardless of how far along the technical migration it is.

The organisations that will navigate the quantum transition with the least disruption are those that begin this structured process now, while the window for an orderly response remains open.

The question that determines your starting point:

Before asking "how do we migrate?" ask "what would actually break, and whose data would be exposed, if our encryption were defeated tomorrow?" The answer to that question defines your programme's scope, its urgency, and its ownership.





SECTION 6_

RECOMMENDATIONS

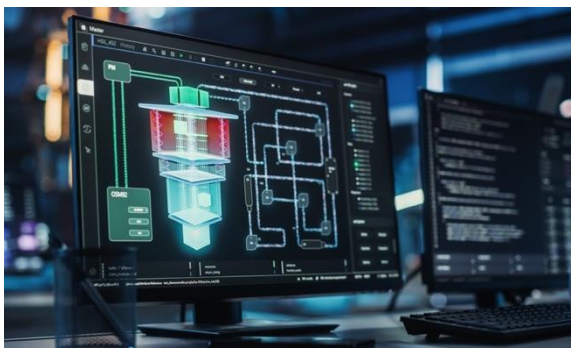
Where To Start: A Practical Entry Point For Organizations

The threat is real, the window is narrowing, and the path forward is clear. Organisations that act now — with a structured 90-day assessment, proper governance, and a risk-ordered migration plan — will be ready. Those that wait will face a harder problem in less time.

The single most important thing an organisation can do right now is not deploy PQC. It is understand its own exposure — clearly, concisely, and at a level that can drive real decisions.

There is no shortage of quantum-safe solutions available today. PQC libraries, hybrid TLS configurations, quantum-safe HSMs, and migration tooling are all mature enough to be deployed. But deploying them without a clear picture of what you are protecting, why it is at risk, and which systems are most exposed is how organisations waste budget, create new technical debt, and lose board confidence in a programme before it has genuinely begun.

The right entry point is deliberate, bounded, and low-disruption. It is a structured engagement that produces clarity — not change. Change comes later, once the foundation is in place.



6.1

Step 1: Commission a Quantum Risk Assessment

Before anything else, understand where you stand. A risk assessment is a six-week exercise that costs a fraction of what a poorly scoped migration will.

A quantum risk assessment is the first concrete step every organisation should take, regardless of sector, size, or existing security maturity. Its purpose is not to produce a report. It is to produce a prioritised view of quantum exposure that can be defended to a board, presented to a regulator, and used to sequence everything that follows.

Concretely, this means

Identify which services carry HNDL exposure:

where long-lived data (financial records, identity data, contracts, health records) is encrypted today and must remain confidential for years to come. That data is already in the threat window.

Identify which services carry TNFL exposure:

where digital signatures, transaction integrity, or certificate-anchored trust could be retroactively forged if underlying algorithms are broken.

Produce a quantum risk register, scored by service and threat type, that gives the organisation a clear, evidence-based view of where risk is concentrated.

Map current posture against the relevant regulatory framework: in Singapore, the CSA Quantum-Safe Migration Handbook; for financial institutions, the MAS Quantum Advisory and the G7 PQC roadmap for the financial sector.

This engagement requires no system changes, no cryptographic modifications, and no production access. It is an architectural exercise conducted through stakeholder interviews, service documentation review, and threat modelling, that can typically be completed in four to six weeks for an organisation with multiple critical services in scope.

The output answers the question every board and every regulator will eventually ask: do you know what your quantum risk is? Until an organisation can answer that question with evidence, it is not ready to plan a migration, let alone execute one.

6.2

Step 2: Build a Migration Plan Before Touching a System

A plan is not a delay. A plan is what makes implementation fast, sequenced, and defensible — rather than expensive, disruptive, and reversible.

Once the risk assessment is complete and a prioritised risk register is in hand, the natural instinct is to begin implementation. Resist it. The next step is a migration plan, and it matters enormously that the plan comes before any production changes.

A quantum-safe migration plan is not a high-level strategy document. It is a service-level, operationally grounded roadmap that answers the questions any implementation team will immediately encounter.

?

Which cryptographic assets exist across the in-scope services: algorithms, keys, certificates, HSM dependencies, vendor-managed components?

What must change, in what order, and what depends on vendor or ecosystem readiness before it can change?

What does the organisation's cryptographic policy need to say: which algorithms are approved, which are deprecated, what key management standards apply?

What are the operational playbooks for algorithm migration, rollback, emergency response, and vendor engagement?

What is the realistic cost, effort, and timeline: not as a theoretical estimate, but as a scoped, sequenced plan grounded in actual inventory?

6.3

From Plan to Practice: Operationalising PQC

A migration plan identifies what needs to change. The harder challenge is making that change safely inside a live environment, without disrupting systems, services, or the connected ecosystems that depend on them.

This subsequent sub-sections outline a practical framework for doing exactly that, structured across three horizons: vendor engagement and ecosystem assessment, testing and controlled rollout, and sustained cryptographic management. Taken together, they define the path from knowing what to change to being genuinely capable of managing cryptography as a continuous organisational discipline.

6.4

Vendor Engagement: PQC Support Is Not PQC Readiness

When a vendor claims PQC support, that claim requires structured scrutiny. **Organisations should formally assess vendors across four dimensions before activating anything in production:**

- **Standards alignment:** Is the implementation aligned to finalised NIST FIPS 203/204/205 standards, not earlier drafts?
- **Hybrid mode availability:** Can the system operate in hybrid classical/PQC mode during the transition period, maintaining compatibility with connected systems not yet upgraded?
- **Performance impact:** What is the actual latency, throughput, and key generation benchmarks under load? Larger PQC key sizes carry measurable overhead that must be understood before activation.
- **Rollback mechanism:** What is the tested procedure for reverting the change if it causes a problem in production?

Critically, enabling PQC on a single system does not make it quantum-safe. Whether PQC is actually used depends on whether every system on the other side of each connection also supports it: both internal services and external partners, payment networks, and cloud platforms. This ecosystem dependency must be mapped before any activation decision is made.

6.5

Testing, Validation, and a 12–24 Month Rollout

PQC activation should follow a four-stage approach, progressing from non-production validation through graduated production rollout: with clear rollback criteria defined at each stage before proceeding to the next:

Stage	Activity
Non-Production Validation	Confirm handshake success, algorithm selection, and performance baselines in a staging environment that mirrors production
Controlled Pilot	Enable PQC for a bounded subset of production traffic; monitor availability, performance, and negotiation behaviour
Graduated Rollout	Expand progressively across in-scope systems; pre-defined rollback thresholds enforced throughout
Ecosystem Verification	Confirm end-to-end PQC operation across connected systems through active testing, not vendor assurance

This is not a big-bang upgrade. It is a phased engagement across 12 to 24 months, spanning vendor readiness assessments, internal team alignment, environment preparation, piloting, and live rollout, progressing in a sequence that keeps production risk contained at every step.

6.6

The True North Star: Cryptographic Agility

The goal is not to complete the PQC migration. The goal is to build the organisational capability to change cryptography: quickly, safely, and without disruption, whenever the need arises. This is cryptographic agility, and it cannot be purchased off a shelf. It must be built into the organisation.

It requires four standing capabilities:

- **A living Cryptographic Bill of Materials (CBOM):** continuously maintained, not a one-time snapshot
- **Algorithm governance and policy enforcement:** clear standards for what is approved, what is deprecated, and how compliance is enforced across procurement and development
- **Operational playbooks:** documented procedures for every class of cryptographic component: who owns it, how to change the algorithm, how to roll back, and which connected systems must move in concert
- **Emergency response readiness:** a pre-tested scenario for urgent algorithm replacement, so that when a vulnerability is disclosed, the organisation responds in days, not weeks

Organisations that emerge from this 12 to 24 months engagement with these four capabilities in place will find that the next cryptographic transition is not a crisis, but is a managed process.

Quantum-safe migration is the catalyst. Cryptographic agility is the destination

6.7

What This Looks Like in Practice

Four phases. Roughly 12 to 24 months. No system disruption. A cryptographically agile organisation at the end.

For most organisations, a structured entry into quantum-safe migration and the journey to sustained cryptographic posture management looks like this:

Phase	What Happens	Timeframe	Outcome
Phase 1: Quantum Risk Assessment	Architectural threat modelling, service-level HNDL/TNFL analysis, cryptographic attack surface mapping, risk register, CSA Handbook alignment	~6 weeks	Prioritised quantum risk register; defensible to board and regulators; Phase 2 scope agreed
Phase 2: Migration Planning	OSI-layer cryptographic mapping, mixed manual + automated inventory, cryptographic policy definition, PQC gap assessment, costed migration plan, operational playbooks	~10 weeks	Executable migration plan for 1–2 critical services; five operational playbooks; cryptographic policy document
Phase 3: PQC Implementation	Vendor PQC readiness assessment; ecosystem dependency mapping (internal and external); hybrid mode validation; staged activation in non-production, then controlled production pilot, then graduated rollout; performance and availability testing at each stage; rollback procedures exercised	~6–12 months	PQC active on priority systems; validated end-to-end quantum-safe operation; performance and availability baselines confirmed; all system owners and vendors aligned
Phase 4: Cryptographic Agility	Living CBOM established and tooled for continuous maintenance; algorithm governance policy enforced across procurement and development; operational playbooks maintained and exercised for all cryptographic component classes; emergency algorithm-replacement scenario rehearsed; continuous monitoring of cryptographic posture in place	Ongoing from Month 12	Organisation can change, rotate, or replace cryptographic algorithms quickly and safely — without service disruption; ready for the next transition before it becomes urgent

This is not a multi-year transformation programme. It is a sequenced, governed engagement designed to take an organisation from risk awareness through to a standing capability it will never have to rebuild from scratch again.

The critical point remains the sequence. Phase 1 before Phase 2. A plan before a single production change. Phase 3 in graduated stages, not a big-bang cutover. And Phase 4 not as a separate initiative that follows implementation, but as the standing discipline that implementation builds towards. Organisations that follow this sequence will find that implementation is faster, cheaper, and far less disruptive than those that attempt to shortcut it, and that the next cryptographic transition, when it comes, is a managed process rather than a crisis.

The end goal is not a completed migration. It is an organisation that knows what cryptography it holds, can change it deliberately, and never again has to start from the beginning.

6.8

The Cost of Waiting

The window for an orderly response is still open. It will not remain open indefinitely.

Cryptographic migration is not like a software patch. It touches every system that relies on encryption, digital signatures, or authenticated communication — which, in a modern enterprise, is nearly every system of consequence. It involves vendors, ecosystem partners, standards bodies, and regulatory timelines that are outside any single organisation's direct control. It takes time — not because the technology is immature, but because the coordination required is inherently complex.

The organisations that will navigate this transition well are those that begin the structured process now: not with implementation, not with tooling procurement, but with a clear-eyed assessment of their own exposure and a plan built on that evidence. That starting point is a risk assessment and a migration plan is available to any organisation today, at a cost and a timeline that is accessible relative to the risk of inaction.

The alternative is to begin in urgency, under regulatory pressure, with an incomplete picture and a compressed timeline. That is a significantly more expensive place to start.

SECTION 7_

CONCLUSION AND NEXT STEPS

Quantum-safe migration is not a future problem. The threat is already active, in the form of data being harvested today, in regulatory frameworks being set now, and in migration timelines that are already running. The question is not whether organisations need to act. It is whether they act in an orderly, structured way or in urgency, under pressure, with a compressed window and an incomplete picture.

The path forward is clear. What follows are the concrete steps that both government and enterprise need to take.

For Governments and Regulators

Government has a unique and non-delegable role in this transition. It sets the frameworks, mandates the timelines, and provides the assurance infrastructure that enterprises depend on. The following actions are needed now:

1. **Formalise national migration timelines with sector-specific deadlines**. Guidance and advisories are a starting point, and not an endpoint. Governments must move from awareness circulars to mandated, time-bound migration schedules, with specific deadlines for Critical Information Infrastructure operators, financial institutions, and government agencies. India's DST Task Force roadmap and Singapore's CSA Quantum-Safe Migration Handbook are strong models. The task now is enforcement, not elaboration.

2. **Mandate cryptographic asset disclosure for regulated entities.** From a defined date, organisations operating in regulated sectors such as banking, payments, telecommunications, healthcare, defence should be required to submit Cryptographic Bills of Materials to the relevant regulator. This creates accountability, surfaces systemic risk, and allows regulators to prioritise intervention where it matters most.

3. **Build and fund national testing and certification infrastructure.** Enterprises cannot migrate to quantum-safe cryptography if the products they need to deploy have not been evaluated and certified. Governments must accelerate the establishment of national PQC testing labs, assurance frameworks, and approved product lists, so that certified quantum-safe solutions are available at the pace the migration demands.

4. **Coordinate internationally, but act nationally.** Quantum risk is a shared challenge. Governments should participate actively in bilateral and multilateral coordination (i.e.) on standards, on threat intelligence, on migration timelines, while ensuring their domestic frameworks move at the pace the national threat exposure demands, not the pace of the slowest international consensus.

For Private Enterprises

Enterprises do not need to wait for regulatory mandates to begin. The risk is real, the frameworks are available, and the engagement model is accessible. The following three steps define a practical, low-disruption starting point:

STEP 1

Register Quantum as a formal organisational risk

Before any technical work begins, quantum risk must be entered into the enterprise risk register — with a named owner, an assessed likelihood and impact profile, and a mandate for structured response. Engage the Chief Risk Officer, the Risk Committee, and — for regulated entities — the Board Risk Committee. Until quantum is a formal risk, it has no budget, no owner, and no accountability. Everything else follows from this step.

STEP 2

Commission a Quantum Risk Assessment

With governance in place, the next step is a structured, service-level risk assessment: identifying HNDL and TNFL exposure across critical services, mapping the cryptographic attack surface, and producing a prioritised quantum risk register that is defensible to boards and regulators. This is a six-week engagement. It requires no system changes. It produces the evidence base that justifies and sequences everything that follows.

STEP 3

Build a Migration Plan before touching production

A risk assessment tells you what is at risk. A migration plan tells you what to do about it, in what order, at what cost. Start with one or two high-priority services. Map cryptography layer by layer. Define a cryptographic policy. Produce operational playbooks. Build a costed, sequenced migration plan that your teams can actually execute, not a strategy document, but an operational roadmap. Only then begin implementation.

The Closing Principle

There is a version of this transition that goes well, and a version that does not. The difference is not technical capability. The technology is ready. The difference is sequence: organisations that understand their risk before they act, that build a plan before they change a system, and that establish governance before they deploy tooling will navigate this transition with confidence. Those that skip steps or wait until regulatory pressure forces action will definitely pay a significantly higher price for the same outcome.

The window for an orderly response is still open. The cost of starting now, with a structured assessment and a grounded plan, is modest. The cost of starting late, without one, is not.

Quantum-safe migration is not a sprint to a finish line. It is the establishment of a permanent capability with the ability to monitor, adapt, and update cryptographic infrastructure as the threat landscape evolves. The organisations that build that capability now are not just protecting against a future threat. They are building the cryptographic resilience that modern digital infrastructure requires, permanently.

SECTION 8_

ANNEXURES

Annexure 1: List of Abbreviations

#	Abbreviation	Details
1	AI	Artificial Intelligence
2	API	Application Programming Interface
3	CBOM	Cryptographic Bill of Materials Guide
4	CERT-In	Indian Computer Emergency Response Team
5	CISO	Chief Information Security Officer
6	CTO	Chief Technology Officer
7	DPI	Digital Public Infrastructure
8	DST	Department of Science and Technology (India)
9	ECC	Elliptic Curve Cryptography
10	ECDH	Elliptic Curve Diffie-Hellman
11	ECDSA	Elliptic Curve Digital Signature Algorithm
12	EMA	European Medicines Agency (Europe)
13	ENISA	European Union Agency for Cybersecurity (Europe)
14	FDA	Food and Drug Administration (USA)
15	FIPS	Federal Information Processing Standards (USA)
16	FN-DSA	Fast-Fourier Lattice-based Digital Signature Algorithm
17	FSDC	Financial Stability and Development Council
18	GSTN	Goods and Services Tax Number
19	HNDL	Harvest Now, Decrypt Later
20	HSM	Hardware Security Module
21	IRDAI	Insurance Regulatory and Development Authority of India (India)
22	IT	Information Technology
23	KYC	Know Your Customer
24	MEITY	Ministry of Electronics and Information Technology (India)
25	ML-DSA	Module-Lattice-Based Digital Signature Algorithm
26	ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism
27	NBFC	Non-Banking Financial Corporation
28	NIST	National Institute of Standards and Technology (India)
29	PFRDA	Pension Fund Regulatory and Development Authority (India)
30	PKI	Public Key Infrastructure
31	PQC	Post Quantum Cryptography
32	RBI	Reserve Bank of India (India)
33	SEBI	Securities and Exchange Board of India (India)
34	TLS	Transport Layer Security
35	TNFL	Trust Now, Forge Later
36	UPI	Unified Payment Interface

Annexure 2: References

Standards & Regulatory Sources

NIST (August 2024). NIST Releases First 3 Finalized Post-Quantum Encryption Standards. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

Cloud Security Alliance (August 2024). NIST FIPS 203, 204 and 205 Finalized. https://cloudsecurityalliance.org/blog/2024/08/15/nist-fips-203-204-and-205-finalized-an-important-step-towards-a-quantum-safe-future

Post Quantum (February 2026). India's Task Force Releases Quantum-Safe Roadmap. https://postquantum.com/security-pqc/indias-quantum-safe-roadmap/

DST Task Force (February 2026). Implementation of Quantum Safe Ecosystem in India. https://dst.gov.in/sites/default/files/Report_TaskForce_PQMigration_4Feb26%20(v1).pdf

Google Blog (March 2026). Quantum Frontiers May Be Closer Than They Appear. https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/

Cloudflare (April 2026). Cloudflare Targets 2029 for Full Post-Quantum Security. https://blog.cloudflare.com/post-quantum-roadmap/

The Quantum Insider (February 2026). New Architecture Could Cut Quantum Hardware to Break RSA-2048 by Tenfold. https://thequantuminsider.com/2026/02/13/new-architecture-could-cut-quantum-hardware-needed-to-break-rsa-2048-by-tenfold-study/

Quantum Computing Report (February 2026). Iceberg Quantum Launches Pinnacle Architecture. https://quantumcomputingreport.com/iceberg-quantum-launches-pinnacle-architecture-to-accelerate-the-fault-tolerant-era/

India Policy & Regulatory Sources

Press Information Bureau, Government of India (April 2023). Cabinet Approves National Quantum Mission at ₹6,003.65 Crore. https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1917888

Department of Science and Technology, Government of India. National Quantum Mission (NQM) — Official Page. https://dst.gov.in/national-quantum-mission-nqm

RMAI / National Quantum Mission (July 2025). India Unveils Roadmap for Quantum-Safe Cybersecurity. https://rmaindia.org/india-unveils-roadmap-for-quantum-safe-cybersecurity/

Press Information Bureau (June 2025). India's UPI Revolution — Over 18 Billion Monthly Transactions. https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=154912&ModuleId=3

Economic Times BFSI (May 2025). UPI Clocks 602 Million Daily Transactions, Records 18.68 Billion Volume in May 2025. https://bfsi.economictimes.indiatimes.com/articles/upi-surges-to-602-million-daily-transactions-a-milestone-for-digital-payments

Gulf News (April 2025). How India's Aadhaar Became the World's Largest Biometric System. https://gulfnews.com/special-reports/how-indias-aadhaar-became-the-worlds-largest-biometric-system-1.500100130

BEF (April 2023). Cabinet Approves National Quantum Mission, Allocates USD 729.99 million (₹6,003 crore). https://www.ibef.org/news/cabinet-approves-national-quantum-mission-allocates-nearly-us-729-99-million-rs-6-003-crore

QNu Labs (April 2026). RBI's Authentication Push: Necessary, But Not Quantum-Ready. https://www.qnulabs.com/blog/rbis-authentication-push-necessary-but-not-quantum-ready

Industry, Research & Global Sources

World Economic Forum (2025). Global Cybersecurity Outlook 2025. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/in-full/

PQShield (2026). PQC Transition Roadmaps and Guidance — Global Overview. https://pqshield.com/pqc-transition-roadmaps-and-guidance/

ENISA. Post-Quantum Cryptography: Current State and Quantum Mitigation. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Post-Quantum%20Cryptography%20Current%20state%20and%20quantum%20mitigation.pdf

European Commission (April 2024). EU Recommendation on Post-Quantum Cryptography. https://postquantum.com/quantum-policy/eu-recommendation-post-quantum/

UK Government (2023). National Quantum Strategy Missions. HM Government. https://www.gov.uk/government/publications/national-quantum-strategy/national-quantum-strategy-missions

Yale Journal of International Affairs (December 2023). China's Quantum Ambitions. https://www.yalejournal.org/publications/chinas-quantum-ambitions

About Primus Partners

PRIMUS PARTNERS®
Solutions for Tomorrow

Primus Partners is a leading Indian-global management consulting firm. Primus Partners works extensively in the Digital space with clients in the public and private sector across the whole digital transformation journey. In addition, there is a dedicated Digital Solutions subsidiary company working in areas of family ID based welfare, ESG realisation, project management, etc.

Primus Partners is actively working in the Quantum space. Primus brings to quantum-safe migration what a technical platform alone cannot: the organisational, policy, and regulatory fluency required to embed a migration programme into the governance structures of Indian enterprises.

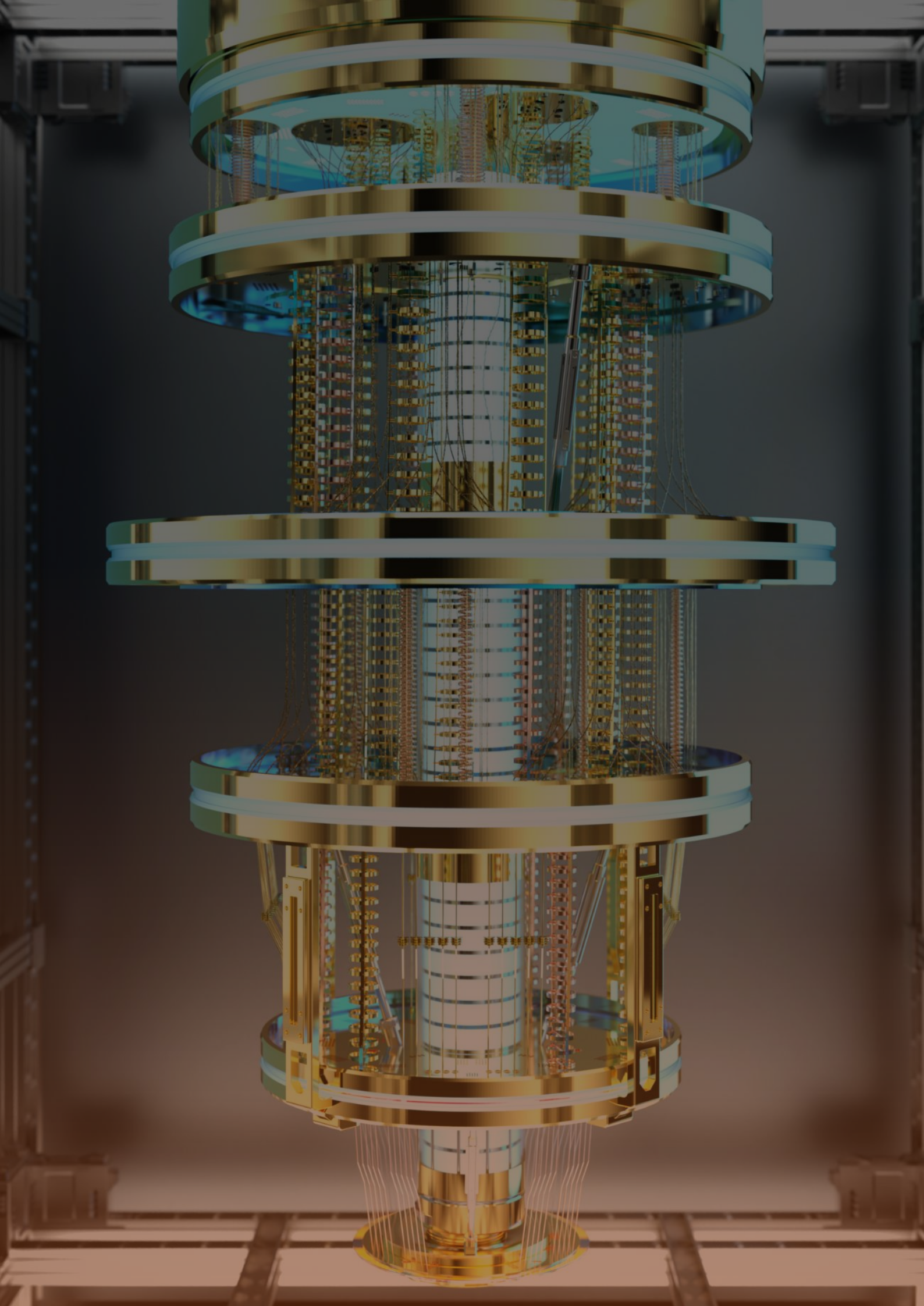
About PQ Station

PQSTATION

PQStation is a quantum security company born out of NTU Singapore, with eight years of foundational R&D in post-quantum cryptography and over 1,000 academic citations. The team contributed directly to the NIST PQC standardisation process — the process that produced the FIPS 203–206 standards on which all enterprise migration programmes should now be based.

PQStation co-authored Singapore's Quantum-Safe Migration Handbook, published by the Cyber Security Agency of Singapore in 2025, and jointly published a whitepaper on the quantum threat to financial services with Mastercard. The company is an active recipient of Singapore's CyberSG R&D Programme grant.

PQStation's flagship platform, QVision, is a cryptographic management platform that enables organisations to discover, govern, and enforce quantum-safe cryptographic policy across their entire infrastructure. QVision produces and maintains the CBOM — the living cryptographic inventory that makes migration possible — and provides the governance dashboard through which CISOs and their teams can track migration progress, manage policy exceptions, and demonstrate regulatory compliance. QVision is currently deployed in pilots across banks, government agencies, and telcos in Singapore, Indonesia, and India, in partnership with Standard Chartered Bank India, OCBC Singapore, and others.



PASSION
for providing solutions to help clients achieve their goals

RESPECT
for all and alternate viewpoints

INTEGRITY
of thoughts and actions

MASTERY
of our chosen subject to drive innovative and insightful solutions

US
representing the Primus collective, where each individual matters

STEWARDSHIP
for building a better tomorrow

PRIMUS PARTNERS®
Solutions for **Tomorrow**

Primus Partners has been set up to partner with clients in 'navigating' India, by experts with decades of experience in doing so for large global firms. Set up on the principle of 'Idea Realization', it brings to bear 'experience in action'. 'Idea Realization'— a unique approach to examine futuristic ideas required for the growth of an organization or a sector or geography, from the perspective of assured on ground implementability.

Our core strength comes from our founding partners, who are goal-oriented, with extensive hands-on experience and subject-matter expertise, which is well recognized in the industry. Established by seasoned industry leaders with extensive experience in global organizations, Primus Partners boasts a team of nearly 400 consultants and advisors, showcasing some of the finest talent in the nation.

The firm has a presence across multiple cities in India, as well as UAE, USA and KSA. In addition, the firm has successfully executed projects across Africa, Asia Pacific and the Americas.

India Offices

Bengaluru
91 Springboard
Business Hub 175, 176
Bannerghatta Rd,
Dollars Colony,
Bengaluru – 560076

Chandigarh
4th Floor, Netsmartz,
Plot No. 10, Rajiv
Gandhi Chandigarh
Technology Park,
Chandigarh – 160019

Chennai
The Executive Zone,
Shakti Tower, 766,
Anna Salai,
Chennai,
TamilNadu - 600002

Delhi
1 to 7, UG Floor,
Tolstoy House,
Tolstoy Road,
Connaught Place
New Delhi - 110001

Kolkata
Collab Deck (Cabin W1021)
Kankaria Center, 2/1 Russel
Street, Park Street Area,
Kolkata - 700071

Mumbai
156/157, 15th Floor,
Nariman Bhavan, NCPA
Road, Nariman Point,
Mumbai – 400021

International Offices

Dubai
United Arab Emirates
(UAE)

Dammam
Kingdom of Saudi Arabia
(KSA)

Washington D.C
United States of America
(USA)

www.primuspartners.in | info@primuspartners.in | Primus Partners India | @partners_primus | @primuspartners7128