URONiYX

SECURE. SCALABLE. SMART

Quantum Risk Exposure Report – India 2026

Indian BFSI & Pharmaceutical Sectors

Prepared by Uroniyx Technologies

Assessing cryptographic vulnerabilities and the path to quantum-safe infrastructure

March 2026

BFSI SECTOR | PHARMACEUTICAL SECTOR | POST-QUANTUM CRYPTOGRAPHY

Table of Contents

Prepared by Uroniyx Technologies · March 2026

Executive Summary

Algorithms such as RSA, ECC, and Diffie-Hellman—currently used to secure global digital infrastructure—are expected to become vulnerable once sufficiently powerful quantum computers become operational. According to NIST's Post-Quantum Cryptography Standardisation Programme (NIST IR 8413, 2022), these algorithms will be rendered insecure by cryptographically relevant quantum computers (CRQCs) — projected to emerge between 2030 and 2035. Two industries in India face particularly high exposure: **Banking & Financial Services (BFSI)** and **Pharmaceutical & Life Sciences**. These sectors handle highly sensitive information that must remain confidential for decades.

Attack models such as **Harvest Now, Decrypt Later (HNDL)** make it possible for attackers to capture encrypted data today and decrypt it in the future when quantum capabilities mature. The NSA's Commercial National Security Algorithm Suite 2.0 (CNSA 2.0, 2022) and ETSI's Quantum-Safe Cryptography standards both identify HNDL as an active, present-day threat requiring immediate enterprise action. This report evaluates the exposure landscape for these sectors and outlines practical steps enterprises should take to begin their transition toward quantum-safe infrastructure.

Cryptographic Vulnerability

RSA, ECC, and Diffie-Hellman at risk from quantum-powered Shor's Algorithm attacks.

High-Risk Sectors

BFSI and Pharmaceutical sectors face the greatest long-term exposure in India.

Immediate Threat

HNDL attacks allow adversaries to harvest encrypted data now for future decryption.

Proactive Action

Enterprises must begin quantum-safe migration planning before quantum computers mature.

Global Standards Response

NIST, NSA (CNSA 2.0), and ETSI have all issued post-quantum cryptography mandates, signalling an industry-wide transition is underway.

Quantum Threat Landscape

Modern cybersecurity relies heavily on public-key cryptography. Protocols such as TLS, IPSec, digital certificates, and secure key exchange mechanisms depend on mathematical problems that classical computers find extremely difficult to solve. However, quantum computers running **Shor's Algorithm** will be able to solve these problems efficiently, breaking many widely used encryption schemes. As a result, data protected today may become vulnerable in the future.

Recognising this risk, global standards bodies have initiated **post-quantum cryptography (PQC)** programmes to develop new cryptographic algorithms resistant to quantum attacks. Organisations that delay assessment risk being caught unprepared as quantum hardware capabilities accelerate beyond current projections.

Harvest Now, Decrypt Later

What Is HNDL?

The Harvest Now, Decrypt Later model represents one of the most immediate threats from quantum computing. Attackers intercept and store encrypted traffic today, waiting until quantum computers become powerful enough to decrypt it — potentially years or decades from now.

Why It Matters Now

Industries that retain sensitive data for long periods are especially vulnerable. Financial records, clinical research, and intellectual property must remain confidential for decades, making them highly attractive targets for long-term interception campaigns. The threat is active *today*, even before quantum computers are operational.

Data encrypted today may be decrypted by adversaries in the future — the window of risk has already opened.

BFSI Sector Exposure

India's financial sector — comprising over 140 scheduled commercial banks, 1,500+ NBFCs, and a payments ecosystem processing over 100 billion UPI transactions annually — faces systemic quantum risk exposure. The Reserve Bank of India (RBI) Cybersecurity Framework mandates long-term data retention, while SEBI's Circular (SEBI/HO/ITD-11T/CSC_EXT/P/CIR/2024/13) has directed regulated financial entities to begin PQC migration planning, while the National Quantum Mission (NQM) under the Department of Science and Technology (DST) is driving India's quantum-safe ecosystem readiness. Approximately 95% of sensitive traffic is encrypted using RSA or ECC-based protocols — all of which are vulnerable to quantum attack.

TLS Infrastructure

Online banking portals rely on TLS encryption that is directly vulnerable to quantum-powered attacks.

Payment Gateways

Card processing systems and payment gateways use cryptographic protocols at risk from Shor's Algorithm.

Public Key Infrastructure

PKI used for authentication across banking systems will require complete cryptographic migration.

SWIFT & Interbank Networks

Interbank communication networks carry high-value transaction data requiring long-term confidentiality.

Cloud Banking Platforms

Cloud-hosted banking infrastructure introduces additional exposure through shared cryptographic dependencies.

Regulatory Exposure

RBI's data localisation and retention mandates mean financial data encrypted today must remain secure for 7–15 years — well within the HNDL threat window.

BFSI Sector Exposure — Cryptographic Risk by Infrastructure Component

The table below maps common BFSI infrastructure components to their cryptographic dependencies, data longevity requirements, and indicative quantum risk levels.

Infrastructure Component	Algorithms at Risk	Data Longevity	Quantum Risk
TLS / HTTPS (Web & API)	RSA / ECDSA / ECDHE	Medium	🔴 Critical
VPN / IPSec	DH / ECDH	Medium	🔴 Critical
PKI / Digital Certificates	RSA / ECDSA	Long	🔴 Critical
Backup Archives & Storage	RSA / ECC key protection	Very Long	🟠 High
Code Signing	RSA / ECDSA	Long	🟠 High–Critical
Database Encryption	AES-256	Very Long	🟡 Medium
Email Encryption (S/MIME)	RSA / ECC	Long	🟠 High
IoT / OT Device Communications	RSA / ECC	Long	🔴 Critical
Cloud Key Management	RSA / ECC authentication	Medium	🟠 High
Internal Auth / SSO	RSA / ECDSA	Short	🟡 Medium

Risk levels are indicative and should be validated through a formal Quantum Risk Exposure Assessment. Source: Uroniyx Technologies analysis, aligned with NIST IR 8413 and NSA CNSA 2.0 guidance.

Pharmaceutical Sector Exposure

India's pharmaceutical sector — the world's third-largest by volume and contributing over $50 billion in annual exports — holds some of the most valuable long-lived intellectual property in any industry. Drug patents typically protect formulations for 20 years, and clinical trial data must be retained for 15–25 years under CDSCO and ICH E6 guidelines. MeitY's cybersecurity strategy identifies life sciences as a critical infrastructure sector requiring enhanced data protection. A single successful HNDL attack on a pharma R&D database could expose decades of proprietary research.

R&D Databases

Research and development databases containing proprietary drug formulations and compound libraries are prime targets for long-term interception.

Clinical Trial Data

Cloud storage containing clinical trial results must remain confidential well beyond the duration of any current encryption guarantee.

Digital Supply Chain

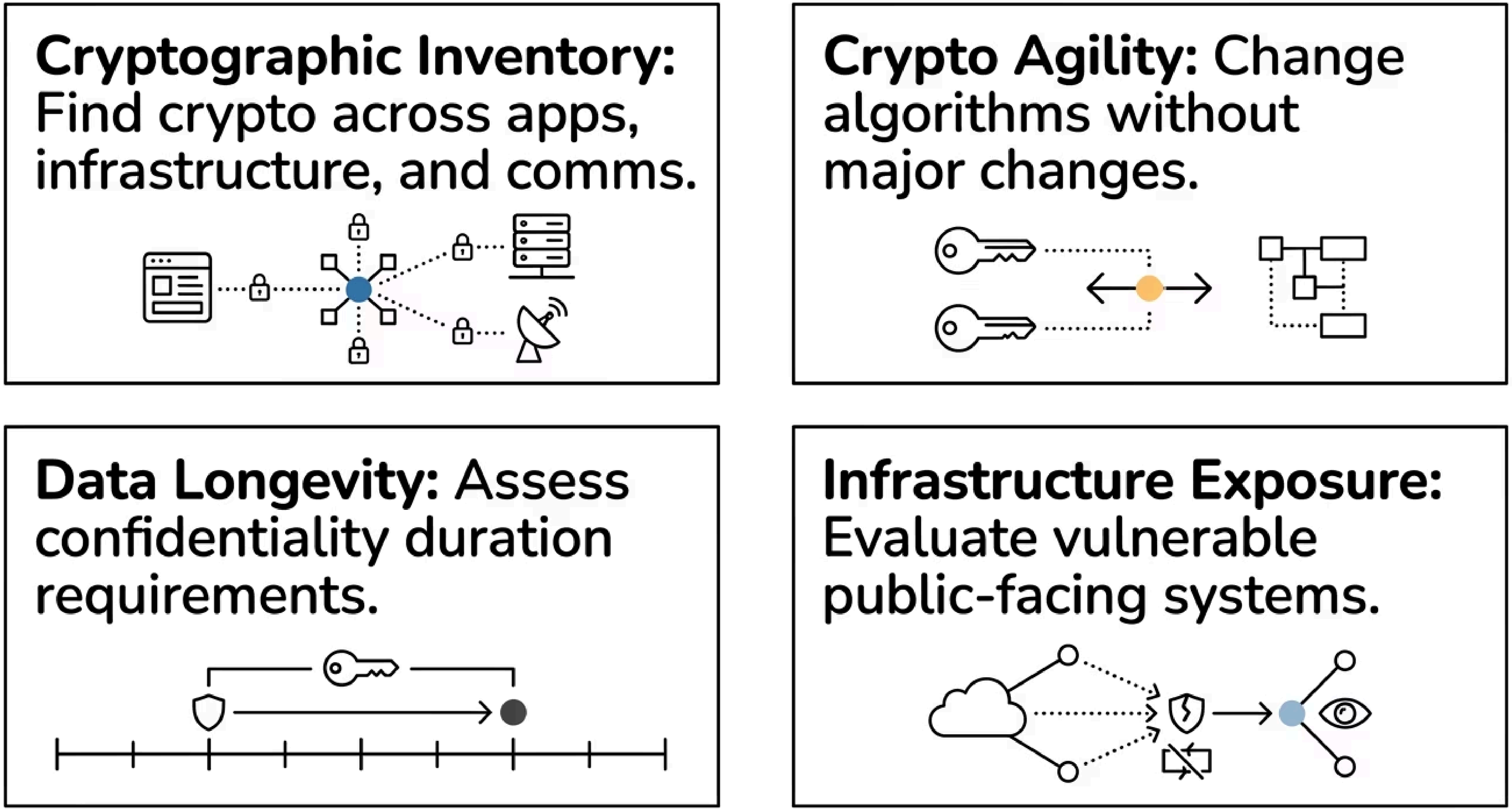
Digital supply chain platforms connecting manufacturers, distributors, and regulators carry sensitive operational and compliance data.

Manufacturing Automation

Manufacturing automation systems rely on encrypted communications that could be compromised through HNDL-style attacks targeting production IP.

Quantum Risk Exposure Model

Uroniyx evaluates enterprise quantum readiness using four core dimensions. Together, these dimensions provide a comprehensive picture of an organisation's current vulnerability and its capacity to transition toward quantum-safe infrastructure. Each dimension must be assessed independently before a coherent migration strategy can be developed.



Cryptographic Inventory: Find crypto across apps, infrastructure, and comms.

Crypto Agility: Change algorithms without major changes.

Data Longevity: Assess confidentiality duration requirements.

Infrastructure Exposure: Evaluate vulnerable public-facing systems.

Enterprise Readiness Challenges

Many enterprises lack visibility into their cryptographic infrastructure, making it difficult to assess true quantum risk exposure. Common challenges span technical, organisational, and vendor-related dimensions, and collectively represent a significant barrier to timely quantum-safe migration.

Unknown Cryptography

Unknown or undocumented cryptographic implementations exist across applications and services, creating blind spots in risk assessment.

Vendor Dependencies

Vendor-dependent encryption implementations mean organisations cannot unilaterally update cryptographic algorithms without supplier cooperation.

Legacy Infrastructure

Legacy infrastructure that cannot easily adopt new algorithms represents a structural obstacle to quantum-safe migration at scale.

Limited Internal Expertise

Limited internal expertise in post-quantum cryptography leaves organisations unable to evaluate risk or plan migration without external support.

India Regulatory Guidance on Quantum Security

India's regulatory bodies are actively signalling quantum readiness expectations for enterprises. The SEBI Circular (SEBI/HO/ITD-11T/CSC_EXT/P/CIR/2024/13, dated August 20, 2024) and the Department of Science and Technology (DST)'s National Quantum Mission (NQM) framework — Implementation of Quantum Safe Ecosystem in India outline a phased, milestone-driven approach for regulated entities to assess and migrate their cryptographic infrastructure.

SEBI Directive on Quantum Computing & Cybersecurity

SEBI has directed Regulated Entities (REs) to take the following actions in response to quantum computing risks:

- Maintain a comprehensive inventory of cryptographic assets for Post-Quantum Cryptography (PQC) migration and assess IT infrastructure capabilities.
- Develop strategies to protect assets that cannot be immediately migrated.
- Upgrade employee skills, periodically revise policies, and conduct proof-of-concept trials to address cybersecurity challenges arising from quantum computing.
- Adopt PQC technologies including Quantum Key Distribution (QKD).

Source: SEBI Circular SEBI/HO/ITD-11T/CSC_EXT/P/CIR/2024/13, dated August 20, 2024

Why This Matters for SEBI-Regulated Entities

SEBI's quantum computing directive carries direct compliance and governance implications for all Regulated Entities. The following dimensions highlight the key areas where immediate action is required.

Immediate Compliance Obligation

SEBI's circular is not advisory — it is a directive. Regulated Entities (REs) are expected to demonstrate active steps toward PQC readiness within SEBI's supervisory framework.

Cryptographic Inventory as a Starting Point

REs must begin with a full discovery of cryptographic assets across applications, APIs, databases, and third-party integrations — forming the basis of a PQC migration roadmap.

Vendor & Third-Party Risk

Many REs rely on vendor-managed encryption. SEBI's directive implicitly requires REs to engage vendors on their PQC migration timelines and contractual obligations.

Board-Level Accountability

Quantum risk should be elevated to board and risk committee agendas, with clear ownership assigned for PQC migration planning and execution.

Source: SEBI Circular SEBI/HO/ITD-11T/CSC_EXT/P/CIR/2024/13, dated August 20, 2024

National Quantum Mission (NQM) — Quantum Safe Ecosystem Roadmap

The Department of Science and Technology (DST), Government of India, under the National Quantum Mission (NQM), has established a Task Force — chaired by Dr. Rajkumar Upadhyay, CEO of C-DOT — to drive the Implementation of Quantum Safe Ecosystem in India. The framework sets out a structured, three-milestone roadmap for Critical Infrastructure (CCI) and enterprises to achieve full Post-Quantum Cryptography (PQC) adoption.

Milestone 1: Build Foundations

Timelines: CCI by 2027 | Enterprises by 2030

- Establish leadership, governance, and cross-functional quantum risk committees.
- Conduct cryptographic asset discovery and risk assessment across all systems.
- Initiate pilot projects and early migration of high-priority systems.
- Identify quantum-sensitive assets for critical infrastructure.
- Prioritise adoption of Cryptographic Bills of Materials (CBOMs).
- Comply with NCIIPC guidelines and establish PQC as a guiding principle across procurement and architecture decisions.

Milestone 2: Migrate High-Priority Systems

Timelines: CCI by 2028 | Enterprises by 2030

- Convert pilots into full migration programs with measurable KPIs.
- Enforce "no new classical-only deployments" policy across all new systems.
- Transition all new digital signatures to PQC-ready versions.
- Ensure supplier accountability and continuous monitoring of cryptographic dependencies.
- Develop quantum-safe communication channels where immediately feasible.
- Integrate PQC into DevSecOps pipelines and procurement processes; develop cryptographic incident response playbooks.

Milestone 3: Full PQC Adoption

Timelines: CCI by 2029 | Enterprises by 2030

- Complete enterprise-wide PQC/hybrid adoption across all systems and services.
- Operate fully from a quantum-safe baseline; all digital signatures are quantum-safe.
- Maintain long-term vendor oversight, audits, and continuous algorithm monitoring.
- Implement layered risk management for remaining legacy systems that cannot be immediately migrated.

Source: DST / National Quantum Mission (NQM) — Implementation of Quantum Safe Ecosystem in India | Task Force chaired by Dr. Rajkumar Upadhyay, CEO, C-DOT

Why Enterprises Need a Quantum Readiness Partner

Post-quantum cryptography migration is not a simple software update — it is a multi-year, organisation-wide transformation that touches every layer of the technology stack. Most enterprises lack the internal expertise, tooling, and frameworks to navigate this transition alone.

Complexity at Scale

Cryptographic dependencies span thousands of applications, APIs, certificates, and devices. Identifying and prioritising them requires specialised tooling and expertise most IT teams do not have in-house.

Evolving Standards

NIST finalised its first PQC standards in 2024 (FIPS 203, 204, 205). Staying aligned with evolving global mandates from NIST, NSA, ETSI, and RBI requires dedicated monitoring and interpretation.

Regulatory Pressure

Regulators in India and globally are beginning to signal PQC readiness expectations. Enterprises that delay risk non-compliance with future RBI, SEBI, and MeitY cybersecurity directives.

The Cost of Waiting

Every day of delay increases HNDL exposure. Data harvested today cannot be 'un-harvested'. The cost of a breach from future quantum decryption far exceeds the cost of proactive migration.

Uroniyx exists to make quantum-safe migration structured, measurable, and achievable for Indian enterprises.

Uroniyx Quantum Readiness Framework

Uroniyx Technologies provides a structured, phased approach to help enterprises evaluate and mitigate quantum risk. The framework guides organisations from initial awareness through to full deployment of quantum-resistant cryptographic solutions, ensuring that each step builds on the last in a coherent and measurable progression.

Phase 1 — Awareness

Executive briefings and leadership workshops explaining quantum threats and their implications for the organisation's specific risk profile.

Phase 2 — Assessment

Quantum Risk Exposure Assessment and development of a Cryptographic Bill of Materials (CBoM) across all systems and infrastructure.

Phase 3 — Planning

Development of a quantum-safe migration roadmap aligned with global post-quantum cryptography standards and regulatory requirements.

Phase 4 — Implementation

Deployment of quantum-resistant cryptographic solutions and crypto-agility frameworks across the enterprise technology estate.

Recommended Enterprise Action Plan

Organisations should begin preparing for quantum threats today, well in advance of quantum computers reaching operational capability. The following five steps represent a practical, prioritised starting point for any enterprise in the BFSI or pharmaceutical sectors seeking to reduce their quantum risk exposure.

1

Build a Cryptographic Inventory

Map all cryptographic usage across systems, applications, and communication channels to establish a baseline for risk assessment.

2

Identify Long-Term Sensitive Data

Locate and classify data requiring long-term confidentiality — financial records, clinical research, IP — that is most vulnerable to HNDL attacks.

3

Evaluate Crypto-Agility

Assess whether existing infrastructure can switch cryptographic algorithms without major architectural changes or vendor dependencies.

4

Monitor PQC Standards

Track evolving post-quantum cryptography standards from NIST and other global bodies to ensure migration plans remain aligned with best practice.

5

Initiate Pilot Deployments

Begin pilot deployments of quantum-safe cryptographic technologies in lower-risk environments to build internal capability and confidence.

Conclusion

Quantum computing will reshape the cybersecurity landscape in ways that demand proactive, long-term planning. Enterprises that begin evaluating their quantum risk exposure today will be better positioned to secure their digital infrastructure in the future. For sectors such as BFSI and pharmaceuticals — where confidentiality horizons extend decades into the future — proactive planning is not optional; it is essential.

Organisations should initiate cryptographic visibility programmes and develop long-term migration strategies toward quantum-safe infrastructure without delay. The window between today and the arrival of cryptographically relevant quantum computers is the critical period in which preparation must occur.

> Enterprises that begin evaluating their quantum risk exposure today will be better positioned to secure their digital infrastructure in the future.

Prepared by Uroniyx Technologies · March 2026

For further information on the Uroniyx Quantum Readiness Framework, contact: Info@uroniyx.com · +91-9025033742

About Uroniyx Technologies

Uroniyx Technologies is an Indian cybersecurity company specialising in quantum-safe security advisory, cryptographic risk assessment, and post-quantum migration strategy. Founded to address the emerging threat of quantum computing to enterprise digital infrastructure, Uroniyx works with organisations in the BFSI, pharmaceutical, and critical infrastructure sectors to build long-term cryptographic resilience.

Our Mission

To make Indian enterprises quantum-ready — through structured assessment, expert guidance, and practical deployment of post-quantum cryptographic solutions.

Our Platform Vision

A future where every Indian enterprise has full visibility into its cryptographic posture and a clear, actionable roadmap to quantum-safe infrastructure — before quantum threats become operational.

Quantum Risk Assessment

Comprehensive Quantum Risk Exposure Assessments and Cryptographic Bill of Materials (CBoM) for enterprise environments.

PQC Migration Advisory

Structured migration roadmaps aligned with NIST FIPS 203/204/205, NSA CNSA 2.0, and Indian regulatory frameworks.

Crypto-Agility Enablement

Implement, operate, and govern cryptography so algorithms can be securely upgraded or replaced without disrupting systems or services.

Uroniyx Technologies Pvt Ltd · Navi Mumbai, India · Info@uroniyx.com · +91-9025033742

URONiYX

SECURE. SCALABLE. SMART

Get in Touch

Uroniyx Technologies — Quantum Security Advisory

To learn more about the Uroniyx Quantum Readiness Framework or to schedule a Quantum Risk Exposure Assessment, reach out to our team.

Address

Uroniyx Technologies Pvt Ltd, 801, Trishul
Goldmine, Palm Beach Road, Sector 15, CBD
Belapur, Navi Mumbai, 400614

Phone

+91-9025033742

Email

Info@uroniyx.com