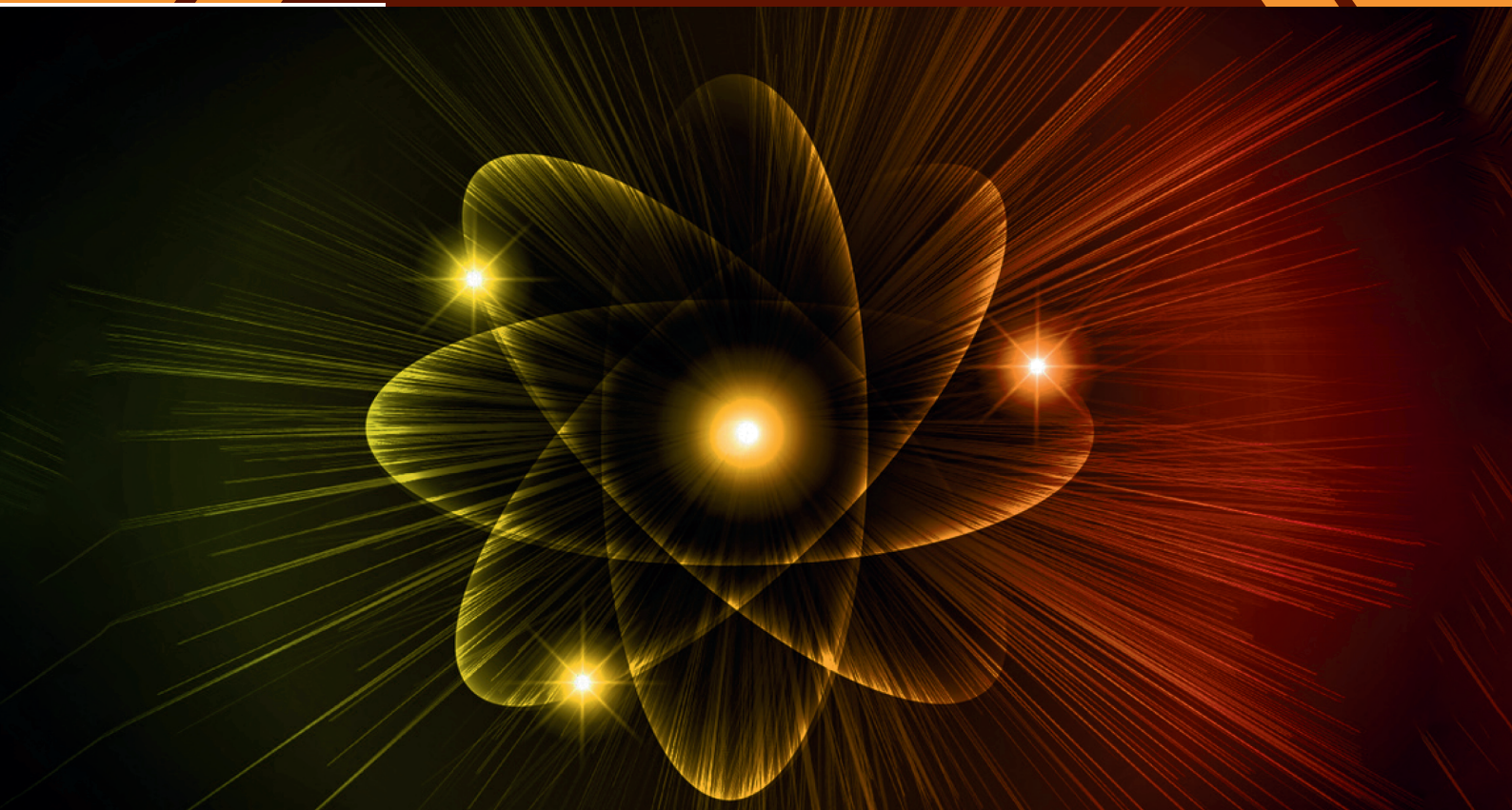
विज्ञान एवं प्रौद्योगिकी विभाग
DEPARTMENT OF
SCIENCE & TECHNOLOGY
सत्यमेव जयते

National Quantum Mission

Report on

Quantum-Safe Ecosystem in India

ROADMAP TO QUANTUM RESILIENCY



Government of India
Department of Science & Technology
National Quantum Mission

May 2026

Quantum-Safe Ecosystem in India

ROADMAP TO QUANTUM RESILIENCY

Government of India
Ministry of Science & Technology
Department of Science & Technology
National Quantum Mission

May 2026

डॉ० जितेन्द्र सिंह
राज्य मंत्री (स्वतंत्र प्रभार),
विज्ञान एवं प्रौद्योगिकी मंत्रालय;
राज्य मंत्री (स्वतंत्र प्रभार) पृथ्वी विज्ञान मंत्रालय;
राज्य मंत्री, प्रधान मंत्री कार्यालय;
राज्य मंत्री कार्मिक, लोक शिकायत एवं पेंशन मंत्रालय;
राज्य मंत्री परमाणु ऊर्जा विभाग तथा
राज्य मंत्री अंतरिक्ष विभाग
भारत सरकार

सत्यमेव जयते

Dr. JITENDRA SINGH
Minister of State (Independent Charge)
of the Ministry of Science and Technology;
Minister of State (Independent Charge)
of the Ministry of Earth Sciences;
Minister of State in the Prime Minister's Office;
Minister of State in the Ministry of Personnel,
Public Grievances and Pensions;
Minister of State in the Department of Atomic Energy and
Minister of State in the Department of Space
Government of India

MESSAGE

India stands at a pivotal moment in its technological journey, where the rapid expansion of digital public infrastructure is transforming governance, economic growth, and citizen services.

Under the visionary leadership of the Hon'ble Prime Minister, India has embarked on an ambitious path to harness the transformative potential of quantum technologies through the National Quantum Mission. The Prime Minister has consistently emphasised the importance of positioning India at the forefront of next-generation technologies, while ensuring that innovation is aligned with national priorities of security, self-reliance, and inclusive growth.

Quantum technologies hold immense promise to drive innovation across sectors. At the same time, they necessitate a forward-looking approach to safeguarding our digital systems. Preparing for a transition towards quantum-resilient security is therefore not only prudent but essential for maintaining trust, continuity, and national security.

In this context, the report of the Task Force on Implementation of a Quantum Safe Ecosystem in India provides a comprehensive and strategic roadmap. It outlines a balanced approach towards the adoption of Post-Quantum Cryptography (PQC), complemented by quantum communication technologies such as Quantum Key Distribution (QKD), wherever appropriate. The emphasis on phased implementation, prioritisation of critical infrastructure, and development of indigenous capabilities is particularly significant.

This initiative strongly aligns with the vision of Atmanirbhar Bharat and reinforces India's commitment to building secure, trusted, and future-ready digital systems. It also highlights the importance of coordinated efforts across government, industry, academia, and research institutions in addressing emerging technological challenges.

I commend the efforts of the Task Force, experts, and all stakeholders who have contributed to this important report. Their work will play a crucial role in guiding India's transition towards a robust and resilient quantum-safe ecosystem.

(Dr. Jitendra Singh)
MBBS (Stanley, Chennai)
MD Medicine, Fellowship Diabetes (AIIMS, New Delhi)
MNAMS Diabetes & Endocrinology
FICP (Fellow, Indian College of Physicians)

Anusandhan Bhawan, 2, Rafi Marg
New Delhi-110001
Tel. : 011-23316766, 23714230,
Fax : 011-23316745

Prithvi Bhawan, Lodhi Road,
Opp. India Habitate Centre,
New Delhi-110003
Tel. : 011-24629788, 24629789

South Block, New Delhi-110011
Tel. : 011-23010191 Fax : 011-23017931
North Block, New Delhi-110001
Tel. : 011-23092475 Fax : 011-23092716

अजय के. सूद
भारत सरकार के प्रमुख वैज्ञानिक सलाहकार
Ajay K. Sood
Principal Scientific Adviser to the Govt. of India

सत्यमेव जयते

कर्तव्य भवन 3, जनपथ, नई दिल्ली - 110001
Kartavya Bhavan 3, Janpath, New Delhi-110001
Tel. : +91-11-24011867, 24011868
E-mail : sood.ajay@gov.in, office-psa@nic.in
Website : www.psa.gov.in

MESSAGE

India's digital public infrastructure has evolved into a strong and trusted foundation for governance, financial services, healthcare, and communications. These systems operate at an unprecedented scale and are relied upon daily by millions of citizens and institutions. At the core of this ecosystem lies cryptography, which ensures confidentiality, data integrity, and secure transactions.

As quantum computing advances globally, it is important to anticipate its long-term implications for digital security. While these technologies hold great promise, they also require us to prepare for challenges that may impact current cryptographic approaches. A timely and well-planned transition to quantum-resilient security will be essential to ensure continuity, trust, and reliability across critical systems.

In this context, the report of the Task Force on Implementation of a Quantum Safe Ecosystem in India provides a comprehensive and forward-looking framework. It outlines a practical pathway for adopting Post-Quantum Cryptography (PQC), complemented, where appropriate, by quantum communication technologies such as Quantum Key Distribution (QKD). The report also emphasizes the importance of phased migration, risk-based prioritisation, and readiness across sectors.

I appreciate the efforts of the Task Force members, partner institutions, and all stakeholders who have contributed to this report. Their work provides valuable guidance for strengthening India's preparedness for the evolving technological landscape.

(Ajay K. Sood)

Dated: 6th April, 2026

सत्यमेव जयते

प्रो. अभय करंदीकर
Prof. Abhay Karandikar

सचिव
भारत सरकार
विज्ञान एवं प्रौद्योगिकी मंत्रालय
विज्ञान एवं प्रौद्योगिकी विभाग
Secretary
Government of India
Ministry of Science and Technology
Department of Science and Technology

07th April, 2026

MESSAGE

The Department of Science and Technology (DST) has been consistently supporting frontier research and promoting technologies that enhance national capabilities. With the launch of the National Quantum Mission, India has taken a decisive step toward building sovereign capabilities in quantum computing, communication, sensing and materials.

As quantum technologies continue to evolve, the security implications for modern digital systems are becoming increasingly evident. Quantum computers, once sufficiently powerful and stable, will be capable of breaking several widely deployed cryptographic algorithms that currently secure the Internet, banking systems, telecom networks, and government communications.

Recognising this need, DST constituted the Task Force on the Implementation of a Quantum Safe Ecosystem in India to develop a structured roadmap for the transition to quantum resilient security. The Task Force brings together expertise from academia, government, industry, and research institutions, reflecting the multidisciplinary nature of this challenge.

The report outlines a phased and strategic transition, focusing on early assessment, prioritisation of critical systems, and the gradual adoption of new cryptographic standards. It also highlights the importance of establishing robust testing and certification infrastructure, building ecosystem readiness, and promoting the development of indigenous solutions. These measures will help ensure that the transition is secure, efficient, and aligned with both national requirements and global developments.

I commend the Chairman of the Task Force and other members, experts, and stakeholders for their valuable contributions. Their collective efforts underscore the importance of coordinated national action in addressing emerging technological challenges.

(Abhay Karandikar)

Technology Bhavan, New Mehrauli Road, New Delhi - 110016
Tel: +91 11 26511439 / 26510068 | Fax: + 91 11 26863847 | e-mail: dstsec@nic.in | website: www.dst.gov.in

विज्ञान एवं प्रौद्योगिकी विभाग
DEPARTMENT OF
SCIENCE & TECHNOLOGY

National Quantum Mission

Table of Contents

Preface

Advances in quantum computing pose a credible long-term risk to the cryptographic mechanisms that secure national digital infrastructure. India has initiated coordinated efforts to ensure the security, resilience, and continuity of its information and communication ecosystems. The National Quantum Mission (NQM) provides a strategic framework for strengthening indigenous capabilities in quantum technologies and enabling the adoption of quantum-safe cryptographic solutions.

Under the aegis of the Department of Science and Technology (DST), a Task Force was constituted to suggest measures for a phased transition to Post-Quantum Cryptography (PQC), formulate an appropriate framework, and anchor measures for the testing and evaluation of quantum-safe solutions and products. The Task Force, chaired by Dr. Rajkumar Upadhyay, Chief Executive Officer, C-DOT, brought together stakeholders from academia, research and development laboratories, government departments, and industry to address the challenges of the post-quantum transition.

To effectively address these objectives, two dedicated sub-groups were formed under this Task Force. The first sub-group, led by the Telecommunication Engineering Centre (TEC) under the Department of Telecommunications, developed a unified structure and a minimum framework for the testing and certification of quantum-safe products and solutions. The second sub-group, led by the Data Security Council of India (DSCI), developed a strategy for PQC migration, quantum resiliency, and crypto-agility.

This document has been prepared following the deliberations of the expert group and the outcomes of the two sub-groups. It provides a coherent framework for policy guidance, technical alignment, and coordinated national action, and recommends pathways for the secure and orderly transition of India’s digital ecosystem to quantum-safe security.

Executive Summary

The digital economy and governance systems of every nation rely on cryptography to ensure secure communication, trusted digital identities, safe financial transactions, and protection of sensitive and strategic information. Cryptographic mechanisms form the backbone of modern digital infrastructure, enabling citizens, businesses, and government institutions to operate with confidence online. As India establishes itself as a global leader in digital transactions, with one of the largest and fastest-growing Internet user bases, the protection of its digital communication infrastructure is critical to sustaining trust, resilience, and growth across sectors. Rapid and sustained advances in quantum computing and quantum algorithms now pose a fundamental challenge to the long-term security assumptions on which most of today's cryptographic systems rest.

Quantum computers, once sufficiently powerful and stable, will break several widely deployed cryptographic algorithms that secure the Internet, banking systems, telecom networks, and government communications. This risk is neither hypothetical nor distant. Adversaries may already be intercepting and storing encrypted data today under "Harvest Now, Decrypt Later" (HNDL) and "Trust Now, Forge Later" (TNFL) campaigns, intending to decrypt it once quantum capabilities mature. The transition to quantum-safe security is therefore a matter of strategic foresight, national security, and economic resilience. Governments, standards bodies, and industry consortia worldwide have already initiated coordinated efforts to develop, standardise, and deploy quantum-safe cryptographic solutions.

A structured view of recent global developments indicates a compression of the quantum risk timeline. Many analysts believe that "Q-Day" — when quantum computers break widely used public-key cryptography — may arrive within three years. In late 2025, a leading company compared today's quantum computing to artificial intelligence five years before its disruptive acceleration. Together, these signals suggest that quantum capability may advance at an unprecedented pace while cryptographic migration remains slow and linear — a systemic risk to national digital infrastructure that requires urgent action.

Realising this, the Department of Science & Technology, under the National Quantum Mission, constituted a Task Force to implement a quantum-safe ecosystem in India. Under this Task Force, two dedicated sub-groups were formed. The first sub-group developed a unified structure and a minimum framework for the testing & certification of quantum-safe products and solutions. The second sub-group formulated a strategy for PQC migration, quantum resiliency, and crypto-agility. This report integrates the findings of both subgroups into a policy-oriented format for multi-sectoral stakeholders. It describes the nature of the quantum threat, reviews global developments, and outlines India's institutional approach under NQM. It also sets out time-bound recommendations, including the launch of PQC and hybrid (classical + PQC) pilots in high-priority systems, the establishment of a National PQC Testing and Certification Programme, the adoption of common PQC procurement requirements, the positioning of existing quantum security solutions in strategic sectors, enterprise-wide PQC implementation, the development of PQC-ready PKI systems and national testbeds for composite PQC–QKD solutions and the deployment of QKD for strategic and critical communication links to create a national quantum-secure backbone aligned with the country's requirements. The roadmap emphasises progressive adoption of indigenously developed quantum-safe products, platforms, and infrastructure, while maintaining interoperability with global standards.

Glossary

ACVP	Automated Cryptographic Validation Protocol
AE	Authenticated Encryption
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AES-CTR	AES Counter mode
AES-GCM	AES in Galois/Counter Mode
AI	Artificial Intelligence
BFSI	Banking, Financial Services and Insurance
BIS	Bureau of Indian Standards
BOM	Bill of Materials
C-DOT	Centre for Development of Telematics
CA	Certification Authority
CAVP	Cryptographic Algorithm Validation Program
CB	Certification Body
CBOM	Cryptographic Bill of Materials
CC	Common Criteria
CEA	Central Electricity Authority

CEO	Chief Executive Officer
CERC	Central Electricity Regulatory Commission
CERT-In	Indian Computer Emergency Response Team
CI/CD	Continuous Integration / Continuous Deployment
CII	Critical Information Infrastructure
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CPU	Central Processing Unit
CRQC	Cryptographically Relevant Quantum Computers
CVSS	Common Vulnerability Scoring System
DPA	Differential Power Analysis
DPDP Act	Digital Personal Data Protection Act
DRDO	Defence Research and Development Organisation
DSA	Digital Signature Algorithm
DSCI	Data Security Council of India
DST	Department of Science and Technology

DWDM	Dense Wavelength Division Multiplexing
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ESG	Environmental, Social, and Governance
FIPS	Federal Information Processing Standards
GPU	Graphics Processing Unit
GUI	Graphical User Interface
HBOM	Hardware Bill of Materials
HMAC	Hash-based Message Authentication Code
HNDL	Harvest Now, Decrypt Later
HQC	Hamming Quasi-Cyclic KEM
HSM	Hardware Security Module
ICCS	Institute of Commercial Cryptography Standards
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IKEv2	Internet Key Exchange version 2
IoT	Internet of Things
IPsec	Internet Protocol Security

IRDAI	Insurance Regulatory and Development Authority of India
ISO	International Organisation for Standardisation
ISRO	Indian Space Research Organisation
IT	Information Technology
ITSM	Information Technology Service Management
KAT	Known Answer Test
KEM	Key Encapsulation Mechanism
KMAC	Keccak Message Authentication Code
KMS	Key Management System
KPI	Key Performance Indicator
MDPI	Multidisciplinary Digital Publishing Institute
MeitY	Ministry of Electronics and Information Technology
ML-DSA	Module-Lattice-Based Digital Signature Algorithm
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism
ML-SIS	Module Short Integer Solution
MLWE	Module Learning with Errors
NABL	National Accreditation Board for Testing and Calibration Laboratories
NCCS	National Centre for Communication Security

NIST	National Institute of Standards and Technology
NQM	National Quantum Mission
NQSN	National Quantum Safe Network
NQSN+	National Quantum Safe Network Plus
NTRU	NTRU: Nth degree TRUncated polynomial ring
OEM	Original Equipment Manufacturer
ONGC	Oil and Natural Gas Corporation
OT	Operational Technology
OTA	Over-The-Air
PKI	Public Key Infrastructure
PoC	Proof of Concept
PPP	Public-Private Partnership
PQC	Post-Quantum Cryptography
PUF	Physically Unclonable Function
QBOM	Quantum Bill of Materials
QEMU	Quick Emulator
QKD	Quantum Key Distribution
QRNG	Quantum Random Number Generator

RBI	Reserve Bank of India
REE	Rich Execution Environment
RFC	Request for Comments
RFP	Request For Proposal
RNG	Random Number Generator
RSA	Rivest–Shamir–Adleman (cryptographic algorithm)
SBOM	Software Bill of Materials
SCA	Side-Channel Analysis
SE	Secure Element
SEBI	Securities and Exchange Board of India
SHA	Secure Hash Algorithm
SHAKE	Secure Hash Algorithm KECCAK Extendable-Output Function
SPA	Simple Power Analysis
SPHINCS+	Stateless Hash-Based Signature Scheme
SSH	Secure Shell
STQC	Standardisation Testing and Quality Certification
SUPERCOP	System for Unified Performance Evaluation Related to Cryptographic Operations
T-Hub	Technology Hub

TEC	Telecommunication Engineering Centre
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TNFL	Trust Now, Forge Later
ToR	Terms of Reference
TPM	Trusted Platform Module
TRAI	Telecom Regulatory Authority of India
TRL	Technology Readiness Level
TRNG	True Random Number Generator
TVLA	Test Vector Leakage Assessment
USD	US Dollars
VA/PT	Vulnerability Assessment / Penetration Testing
VPN	Virtual Private Network

1.0 Introduction

Cryptography is the foundation of digital trust. It enables secure communication over open networks such as the Internet by ensuring that:

- Messages remain confidential and readable only by intended recipients.
- Data cannot be altered without detection.
- Identities of users, systems, and services can be verified and trusted.

Cryptography enables citizens to access e-governance services securely, allows banks to protect financial transactions, supports telecom networks in authenticating users and signalling traffic, and underpins national digital identity systems.

Public-key cryptography, symmetric encryption, and cryptographic hash functions together form the security foundation of modern digital systems. These mechanisms have been trusted for decades because the underlying mathematical problems were considered computationally infeasible to solve using even the most advanced classical computers.

As India establishes itself as a global leader in digital transactions, with one of the largest and fastest-growing Internet user bases, the protection of its digital communication infrastructure is critical to sustaining trust, resilience, and growth across sectors. As cyber-attacks grow more sophisticated, the need for robust safeguards is acute. The IBM Cost of a Data Breach Report 2025 reports an average breach cost of USD 4.44 million — more than 15% higher than in 2020 [1]. Breaches also inflict reputational damage and create strategic vulnerabilities for enterprises and governments.

2.0 Emerging Threat from Advancements in Quantum Computing

Quantum computing represents a shift in computation. Unlike classical computers, which process information in binary form, quantum computers exploit quantum-mechanical properties to perform certain calculations far more efficiently. Recent advances in quantum computing and quantum algorithms promise to solve problems beyond the reach of classical systems — from optimising logistics and supply chains to accelerating drug discovery and materials science. Rapid progress by leading nations, including China and other major technology powers, has accelerated the global timeline toward practical, large-scale quantum computing.

This computational power also introduces a critical challenge: the potential to break widely used encryption methods that protect today's digital communications and financial systems. Several widely deployed cryptographic algorithms will become vulnerable once large-scale, cryptographically relevant quantum computers become operational. This vulnerability exists regardless of implementation quality because it arises from fundamental mathematical breakthroughs enabled by quantum computation. Developing quantum-safe solutions is therefore urgent, so that innovation strengthens rather than compromises global security.

Many categories of sensitive information require long-term confidentiality. Government records, strategic communications, financial data, and personal information often need protection over decades. If such data is compromised, the consequences include national security risks, economic losses, legal challenges, strategic setbacks, and erosion of public trust in digital systems.

Preparing for quantum-safe security is therefore not a technical exercise alone but a strategic necessity, addressed well in advance through policy formulation, long-term planning, and coordinated national action.

3.0 Need for Quantum-Safe Security

The security of most existing cryptographic systems rests on the assumption that certain mathematical problems — for example, prime factorisation of a large integer — are infeasible to solve in practical time. Advances in quantum computing and quantum algorithms challenge this assumption. Shor's algorithm enables efficient solutions to problems such as integer factorisation and discrete logarithms, directly undermining the security of widely used public-key cryptographic algorithms, including Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC).

Grover's algorithm provides a quadratic speed-up for brute-force attacks on symmetric encryption and cryptographic hash functions. While this does not fully break symmetric cryptography, it requires larger key sizes and revised security parameters to maintain acceptable security levels.

A critical risk associated with quantum computing is the HNDL strategy. Adversaries may intercept and store encrypted communications today, even though current technologies cannot decrypt them; once sufficiently capable quantum computers become available, the stored data can be decrypted retroactively.

This risk is particularly acute for information with a long shelf life, including government communications, defence secrets, financial records, healthcare data, and critical infrastructure control systems. Industry assessments indicate that quantum capability is entering a phase of accelerated, non-linear growth, raising the risk that cryptographic disruption may occur with limited warning.

Given the long lifecycle of digital infrastructure and cryptographic deployments, delayed action will result in rushed transitions, higher costs, and increased security risk. Early planning and phased migration enable organisations to manage risk systematically, minimise operational disruption, and align national efforts with evolving global standards.

4.0 Global Efforts Towards Quantum-Safe Security

Several economies have already announced phased migration plans for quantum-safe security. A common global pattern is the recognition that the migration is a multi-year process requiring early preparation, testing, and policy support.

United States of America

The United States has adopted a federally coordinated transition to post-quantum cryptography aligned with the National Institute of Standards and Technology (NIST) standardisation efforts [2]. Federal agencies are required to maintain cryptographic inventories, assess quantum-vulnerable systems, and initiate migration planning. Widely used public-key algorithms such as RSA-2048 and ECC-256 are expected to be deprecated around 2030 and fully disallowed after 2035, with complete migration of federal systems targeted by 2035 [3]. The Department of Homeland Security, in coordination with NIST, has issued guidance and roadmaps; the estimated migration cost is approximately USD 7.1 billion over 2025–2035 [2, 4].

European Union

The European Union has adopted a coordinated implementation roadmap for the transition to Post-Quantum Cryptography (PQC), identifying it as the primary mitigation strategy and recommending standardised hybrid PQC mechanisms, including PQC–Quantum Key Distribution (QKD) combinations, where appropriate [5–6]. Member States are required to initiate national PQC transition strategies, including a cryptographic asset inventory and risk assessment, by the end of 2026 [7–8]. High-risk and critical systems will be migrated by 2030; remaining systems will be transitioned by 2035, with emphasis on cryptographic agility and cross-border interoperability [9–10].

United Kingdom

The United Kingdom's PQC migration is guided by the National Cyber Security Centre (NCSC) through a phased national roadmap issued in March 2025 [11]. Organisations are expected to complete discovery and assessment of cryptographic dependencies by 2028, migrate high-priority systems by 2031, and complete PQC transition across systems, products, and services by 2035 [12–14].

Australia

Australia's PQC transition, led by the Australian Signals Directorate under the Information Security Manual, requires organisations to develop PQC transition plans by the end of 2026 [15]. Migration of critical systems commences by 2028, and the use of quantum-vulnerable asymmetric cryptographic algorithms — including RSA and elliptic-curve schemes — ceases by the end of 2030 [15–16].

Canada

Canada has established a federal roadmap for PQC migration under ITSM.40.001, effective June 2025 [17]. Federal departments are required to submit initial PQC migration plans by April 2026 and provide annual progress reports thereafter [18]. Migration of high-priority systems is targeted for completion by the end of 2031, with remaining systems transitioned by 2035 [17, 19].

Singapore

Singapore has adopted an integrated PQC and QKD approach through the National Quantum-Safe Network (NQSN), which operated as a testbed from 2022, and the National Quantum-Safe Network Plus (NQSN+), launched in 2023 for nationwide operational deployment [20–21]. The infrastructure supports the integration of PQC and QKD within production networks. In 2025, the Cyber Security Agency of Singapore released a Quantum-Safe Handbook and a Quantum Readiness Index to support organisational preparedness and quantum-risk assessment [22].

United Arab Emirates

The Emirates has initiated post-quantum preparedness through guidelines issued by the Dubai Electronic Security Centre in May 2025 [23]. These guidelines require organisations to assess quantum cybersecurity risks, evaluate data sensitivity and longevity, and document cryptographic dependencies. The transition is phased, beginning with inventory and risk assessment and followed by short- and long-term strategies toward quantum-safe cryptography [23]. In parallel, the Technology Innovation Institute has released PQC software libraries to support secure communications in the quantum era [24].

South Korea

South Korea's Post-Quantum Cryptography Master Plan targets nationwide transition by 2035 through a sector-wise rollout announced by the government in 2023 [25]. Pilot deployments are being conducted during 2025–2028 in public administration, energy, and healthcare, followed by phased expansion to telecommunications, defence, automotive, finance, space, and IoT [25]. The roadmap includes deployment of PQC and evaluation of hybrid PQC–QKD architectures, particularly for telecommunications and financial infrastructure, supported by industry pilots and public–private collaboration [26–28].

China

China has not publicly disclosed a PQC migration timeline. It is, however, pursuing quantum-safe networking at pace. China has launched its own PQC standardisation initiative, bypassing the NIST process as part of a broader strategy for cryptographic sovereignty and self-reliance. Through its domestic cryptographic standards body, the Institute of Commercial Cryptography Standards (ICCS), China has invited proposals for quantum-resistant public-key encryption, digital signatures, hash functions, and block ciphers, signalling intent to develop and deploy indigenous quantum-safe algorithms rather than adopt NIST-selected algorithms [29]. China has also leveraged its leadership in quantum communication infrastructure to extend space-based QKD links and pursue global coverage, and aims to launch a global quantum communication service by 2027, deploying quantum satellite constellations to connect strategic partners, including BRICS nations, with ultra-secure transmissions [30].

5.0 Indian Context: National Quantum Mission and Task Force

While global initiatives reflect collective recognition of the quantum threat, each nation must translate these efforts into strategies aligned with its own priorities, economic ambitions, and security imperatives. Nations are increasingly emphasising digital sovereignty as a matter of strategic autonomy.

For India, one of the world's major economies, investing in quantum technologies is essential to strengthen national security, drive innovation, enhance cybersecurity, and sustain economic growth.

The National Quantum Mission, approved by the Union Cabinet in April 2023, has a ₹6,003.65 crore outlay for the period 2023–24 to 2030–31. It aims to accelerate scientific and industrial R&D, foster innovation, and drive quantum technology-led economic growth, strengthening India's position in quantum technologies and applications.

NQM has established four Thematic Hubs (T-Hubs) at premier academic and research institutions, each dedicated to a critical quantum technology domain: the Quantum Computing Hub at the Indian Institute of Science, Bengaluru, advancing scalable quantum processors; the Quantum Communication Hub, hosted by the Indian Institute of Technology Madras with the Centre for Development of Telematics (C-DOT), developing secure quantum communication systems, including long-distance fibre-based and satellite-based QKD links; the Quantum Sensing and Metrology Hub at the Indian Institute of Technology Bombay, advancing ultra-precise quantum sensors and measurement standards; and the Quantum Materials and Devices Hub at the Indian Institute of Technology Delhi, driving innovation in quantum materials and device engineering. The hubs operate under a Hub–Spoke–Spike model linking 152 researchers from 43 institutions across 17 states and 2 Union Territories, integrating multidisciplinary expertise across technology development, capacity building, startup engagement, and industry collaboration.

A key objective of NQM is to translate indigenous R&D into field-deployable, production-grade systems. Quantum-Safe security initiatives under this roadmap will therefore leverage domestically developed PQC, QKD, cryptographic hardware, and supporting platforms, strengthening India's self-reliance and trusted supply chains.

In Quantum Communication, NQM's objectives include inter-city QKD networks spanning up to 2,000 km over existing optical fibre infrastructure, and satellite-based secure quantum communication links between ground stations over distances of up to 2,000 km within India and with other countries. Together these will enable a nationwide quantum-secure communication backbone. To achieve these objectives of quantum-secure communications, a Task Force on implementation of Quantum-Safe Ecosystem was constituted under which two focused sub-groups were formed.

Both sub-groups have produced detailed reports covering the technical, institutional, and policy dimensions. Their summaries appear in Section 6.0 and Section 7.0, respectively.

6.0 Summary of Report of Sub-Group I

Led by the Telecommunication Engineering Centre (TEC), this sub-group has developed the "Framework for Testing and Certification of PQC based Quantum-Safe Products and Solutions".

The framework establishes a national, risk-based, and measurement-driven approach to testing, validating, and certifying PQC-enabled products, systems, and services across finance, telecom, energy, healthcare, defence, and critical infrastructure. It serves as a common reference for sectoral regulators, government agencies, industry, start-ups, testing laboratories, and certification bodies. While the framework is not itself a regulatory mandate, it enables regulators to define sector-specific timelines and enforcement mechanisms for PQC adoption.

Assurance Levels (L1–L4)

The framework defines four hierarchical assurance levels, aligned to usage context and risk criticality:

Level 1 (L1) – Basic Conformance

- For low-risk, non-sensitive, consumer-grade environments.
- Focus on the correct implementation of PQC, interoperability, and baseline performance.

Level 2 (L2A / L2B / L2C) – Secure Software and Hardware Assurance

- For medium-risk deployments handling sensitive data.
- L2A: Software security assurance.
- L2B: IT/IoT hardware security assurance.
- L2C: Operational Technology (OT) hardware security assurance.

Level 3 (L3) – Enterprise Infrastructure Security

- For high-risk, enterprise-grade environments (e.g., banking, telecom, healthcare).
- Focus on long-term security, crypto-agility, resilience, and enterprise integration.

Level 4 (L4) – Critical Infrastructure Security

- For very high-risk, sovereign, and national critical infrastructure.
- Focus on indigenous cryptographic implementations and hardware to reduce dependence on external validation ecosystems and strengthen sovereign assurance.

Higher assurance levels inherently include compliance with all lower levels.

Tiered Testing Laboratory Structure

To support scalable and credible certification, the framework proposes a three-tier national laboratory model:

Tier-1 Laboratories

- Conduct Level-1 testing.
- Focus on functional correctness, standards conformance, and interoperability.
- Already designated TEC/BIS labs may be upgraded for this role.

Tier-2 Laboratories

- Conduct Level-2 testing (software and hardware assurance).
- Focus on security testing, vulnerability assessment, and hardware resilience.
- BIS, STQC, CERT-In empanelled, and NCCS-designated labs may be leveraged.

Tier-3 Laboratories

- Conduct advanced Level-3 and Level-4 evaluations.
- Focus on enterprise-grade, sovereign-grade security, crypto-agility, TRNG/QRNG validation, and indigenous algorithm assessment.
- Certification and Migration Roadmap.

The framework outlines an end-to-end certification lifecycle covering product submission, pre-assessment, testing, validation, certificate issuance, and post-certification surveillance. Certification validity is risk-aligned, with provisions for re-testing on major upgrades or newly identified vulnerabilities. Certificates are issued with defined assurance levels (L1–L4) and risk-aligned validity periods — ranging from three years for L1 to ten years for L4 — subject to ongoing surveillance and re-assessment.

A phased national migration roadmap is proposed, with critical systems transitioning to PQC first, supported by timely establishment and upgrading of the national testing and certification infrastructure.

Key Challenges and Way Forward

The report identifies challenges including limited domestic PQC testing capability, dependence on foreign validation ecosystems, evolving global standards, and constraints in validating hardware-based cryptographic modules. It recommends public consultation, upgrading of existing laboratories, alignment with global standards bodies, adoption of indigenously developed quantum-safe solutions subject to security, performance, and interoperability requirements, and the establishment of Centres of Excellence and national PQC testbeds.

The framework provides a foundational blueprint for India's structured, credible, and sovereign transition to quantum-safe security, balancing global interoperability with national strategic autonomy, and enabling regulators and industry to adopt PQC with confidence.

In addition to the framework measures, the following points shall be incorporated:

- An interim approval mechanism will apply while the national testing and certification framework is being operationalised, which is expected to take 12–18 months. Deferring product certification in the interim would delay PQC migration for critical infrastructure and increase security risk. The existing approval framework for quantum-safe products will continue until the new infrastructure and processes are operational.
- A nationally defined list of cryptography-dependent product categories will be prepared, drawing on the US Cybersecurity and Infrastructure Security Agency (CISA) report of 23 January 2026, which identifies hardware and software products acquired by federal agencies that rely on cryptographic functions such as key establishment and digital signatures (see Annexure A). The Indian list will be contextualised to domestic requirements by additionally including automated cryptographic discovery and inventory

solutions, and mobile phones, given their central role in India's digital ecosystem. Indian vendors have already developed quantum-safe solutions for next-generation platforms — including satellites, drones, automotive systems, sensors, and IoT endpoints — and alternative approaches such as firmware-based upgrades may be considered. Inclusion in this category constitutes a future compliance requirement for vendors.

Note: The complete report of Sub-Group I is given in Annexure B.

7.0 Summary of Report of Sub-Group II

The "Strategic Roadmap for Quantum-Safe Migration Timelines" provides India's enterprises with a structured roadmap to achieve quantum resiliency under NQM. With rapid advances in quantum computing, current public-key cryptography (RSA, ECC, Diffie–Hellman) faces obsolescence, placing sensitive data, financial transactions, and operational systems at long-term risk. Enterprises must plan and execute a phased transition to PQC.

Key Drivers and Threats

- Cryptographically Relevant Quantum Computers (CRQCs) can render existing cryptographic algorithms ineffective.
- Data encrypted today may be vulnerable to HNDL & TNFL attacks.
- Enterprise systems are interconnected; cryptographic failure in one sector can cascade, creating systemic risk.
- Transition requires long-term planning, governance, resources, and skilled teams.
- Recent advancements in Artificial Intelligence (AI) & Quantum computing may accelerate cryptanalysis and side-channel attacks, compounding the urgency of migration.

Approaches to Quantum Resiliency

- **Algorithmic Solutions (PQC):** Upgrade cryptographic algorithms on existing infrastructure to resist quantum attacks. PQC based solutions are implemented through software libraries or dedicated hardware. PQC is a more pragmatic & scalable approach to build quantum resilience.
- **Quantum Communication (QKD):** Hardware-intensive key distribution systems leveraging quantum properties, may be suited for limited high-assurance/research-focused environments.
- **Composite Approaches:** Given QKD only provides key establishment, and not (Cryptographic) signatures, organisations adopting QKD must also combine PQC to build comprehensive security. A balanced approach combines widespread PQC deployment with limited & targeted QKD investment for a limited set of use cases.

Phased Milestones

Critical Information Infrastructure (CII) sectors are treated as urgent adopters with accelerated timelines compared to regular enterprises.

Milestone 1 – Build Foundations (CII: by 2027 | Enterprises: by 2028)

- Establish leadership, governance, and cross-functional quantum risk management.
- Inventory cryptographic assets and assess quantum risk.
- Initiate pilot projects and early migration of high-priority systems.
- Begin adopting PQC/hybrid (classical + PQC) signatures for critical software and systems.
- Introduce PQC readiness requirements in procurement, including phased adoption of Cryptographic Bills of Materials (CBOMs).

- Conduct quantum risk analysis, adopt crypto-agility as a guiding principle, and mandate CBOM submissions from vendors starting FY 2027–28.

Milestone 2 – Migrate High-Priority Systems (CII: by 2028 | Enterprises: by 2030)

- Convert pilots into full migration programs with KPIs.
- Enforce "no new classical-only deployments".
- Upgrade PKI, HSMs, KMS, and libraries to PQC-ready versions.
- Mandate PQC-capable digital signatures.
- Ensure supplier accountability and continuous monitoring.
- Contain classical-only systems within controlled enclaves where immediate migration is not feasible.
- Develop cryptographic incident response playbooks and integrate PQC training into cybersecurity, DevOps, and IT programmes.

Milestone 3 – Full PQC Adoption (CII: by 2029 | Enterprises: by 2033)

- Complete enterprise-wide PQC/hybrid (classical + PQC) adoption.
- Operate PQC-only trust chains and ensure all digital signatures are quantum-safe.
- Maintain long-term vendor oversight, audits, and continuous algorithm updates.
- Implement layered risk management for the remaining legacy systems.

PQC Personas – Prioritisation Framework:

- **Urgent Adopters:** Critical infrastructure and high-risk organisations (e.g., Power Sector, Telecom Sector, ISRO, DRDO, ONGC) – accelerated migration across all milestones.
- **Regular Adopters:** Enterprises with moderate risk – follow standard milestones (2028–2033).
- **Technology Providers & Enablers:** Vendors of cryptography-related solutions – lead by example and support the broader ecosystem.

An enterprise may identify with more than one persona; in such cases, the highest-risk persona should guide priorities.

Technology Considerations for Quantum-Safe Migration Across CII:

For CII sectors, the adoption of quantum-safe technologies is shaped less by the algorithms themselves and more by how they interact with existing architectures, operational constraints, and ecosystem dependencies.

Key considerations include:

- **Latency Sensitivity:** PQC overhead is manageable in millisecond-level systems but problematic in microsecond-level environments (e.g., defence, telecom).
- **Handshake Frequency:** Systems with long-lived sessions face minimal impact, while frequent TLS renegotiation or short-lived sessions amplify PQC costs.
- **User/Service Tolerance:** Some services can absorb modest delays, but safety-critical or financial systems cannot tolerate even small performance degradation.
- **Hardware Constraints:** Long-lived hardware platforms, embedded devices, and certified systems may lack compute headroom for PQC, requiring PQC-capable HSMs/KMS or interim controls until refresh cycles.
- **Vendor Dependence:** Migration depends on OEMs and third-party platforms for firmware updates, interoperability, and backward compatibility.
- **Cross-Border Dependencies:** Many critical systems rely on international standards and protocols, so migration must align with global bodies to ensure interoperability.

Critical Principles:

- **Crypto-Agility:** Establish the ability to rapidly update algorithms, keys, and protocols without business disruption.
- **Governance & Risk Management:** Board-level oversight, resource allocation, and cross-functional accountability.
- **Continuous Assurance:** Independent validation, monitoring, and capacity-building for sustained progress.
- **Vendor and Ecosystem Alignment:** Ensure CBOM submissions, PQC readiness, and ongoing support for enterprise adoption.
- **Contingency Planning:** Prepare interim quantum-safe solutions (e.g., proxies, tunnels, VPNs, gateways, and QRNG/TRNG) in case of accelerated quantum breakthroughs.
- **ESG Implications:** PQC algorithms may require greater processing power and energy, so sustainability and long-term technology investment strategies must factor this in.

Key Challenges in Post-Quantum Migration:

Migration to post-quantum cryptography represents a fundamental shift in digital trust, not a routine technology upgrade. Enterprises will face multi-dimensional challenges spanning technology, governance, skills, and ecosystem coordination.

Key challenges include:

- **Legacy System Complexity:** Diverse and inflexible legacy infrastructures, often lacking crypto-agility, will require redesign or replacement.
- **Interoperability During Transition:** Coexistence of classical and quantum-safe cryptography increases complexity and introduces risks of downgrade or insecure fallback.
- **Vendor Readiness Gaps:** Uneven PQC preparedness among vendors may delay migration and disrupt enterprise timelines.
- **Performance and Operational Impact:** Quantum-Safe algorithms can increase computational overhead, necessitating performance testing and infrastructure optimisation.
- **Skills Shortage:** Limited availability of PQC-skilled professionals highlights the need for targeted capacity building and continuous training.
- **Governance and Investment Continuity:** Sustained executive oversight, funding, and programme discipline are essential to move beyond pilots to enterprise-wide adoption.
- **Assurance and Validation Gaps:** Independent validation is critical to ensure correct implementation and prevent reversion to vulnerable cryptography.
- **Cross-Sector Coordination Risks:** Inconsistent migration approaches across interconnected sectors could undermine interoperability and trust chains.

Addressing these challenges requires a coordinated, phased approach, supported by vendor enablement, performance engineering, skills development, and independent assurance. Embedding crypto-agility and continuous governance as core capabilities is essential to manage evolving standards and long-term quantum risk. PQC remains the most deployable approach, while QKD provides strategic, high-assurance capabilities for specific use cases.

In addition to the measures outlined in the report of Sub-Group II, the Task Force intends to incorporate that, under the Preferential Market Access framework, procurement by both public and private organisations accord preference to indigenously developed solutions, in alignment with India's 'Atmanirbhar Bharat' policy, and to ensure technological sovereignty through domestic control over cryptographic capabilities protecting critical assets. Interoperability requirements, wherever applicable, must be considered to ensure seamless integration and standards compliance.

Note: The complete report of Sub-Group II is given in Annexure C.

8.0 Looking Ahead: Strategic Roadmap for Post-Quantum Security

As India advances toward the post-quantum era, the outputs of the two sub-groups provide the foundation for coordinated national action, defining clear priorities, transition pathways, and indicative timelines for safeguarding critical digital infrastructure against emerging quantum threats. Aligned with the objectives of NQM — particularly long-distance fibre-based and satellite-enabled quantum communication networks — a phased, targeted deployment of QKD for strategic and mission-critical communication links will be essential. This approach will create a national quantum secure backbone while complementing the large-scale adoption of PQC across enterprise and end-user environments.

Global market trends reinforce the urgency of this dual-track strategy: the PQC market is projected to reach approximately USD 2.84 billion by 2030 [31], and the QKD market is expected to exceed USD 2.63 billion by 2030 [32], reflecting rapid adoption across defence, finance, telecommunications, and critical infrastructure. India must therefore move decisively from research and pilots to structured deployment and ecosystem readiness.

Under NQM, an inter-city QKD backbone network has been envisioned, connecting multiple intra-city QKD networks across various topologies. Where fibre infrastructure is unavailable at last-mile nodes or end users, quantum-secure connectivity is supplemented using PQC. As illustrated in Figure 1, in City A, local nodes (yellow) establish keys via QKD links (blue) and relay them to a QKD node (blue). That QKD node supplies encryption keys to PQC-compliant encryptors that carry traffic over the existing Dense Wavelength Division Multiplexing (DWDM) link (black dashed line). In intermediate regions (City B), a QKD hub node (red) connects multiple QKD nodes and relays keys securely to the next city using trusted relay nodes (yellow). PQC nodes (green) ensure end-to-end quantum-resistant security. The QKD nodes (blue) and QKD relay nodes (yellow) will also be PQC compliant for resiliency, supplying composite QKD–PQC keys to the encryptors.

The transition also presents an opportunity to scale indigenous quantum-safe technologies, enabling India to move from pilots to deployment-led leadership in PQC and QKD systems. The next phase must therefore focus on operationalising this vision through clear mandates, coordinated procurement, sector-specific migration planning, and accelerated deployment of indigenous solutions.

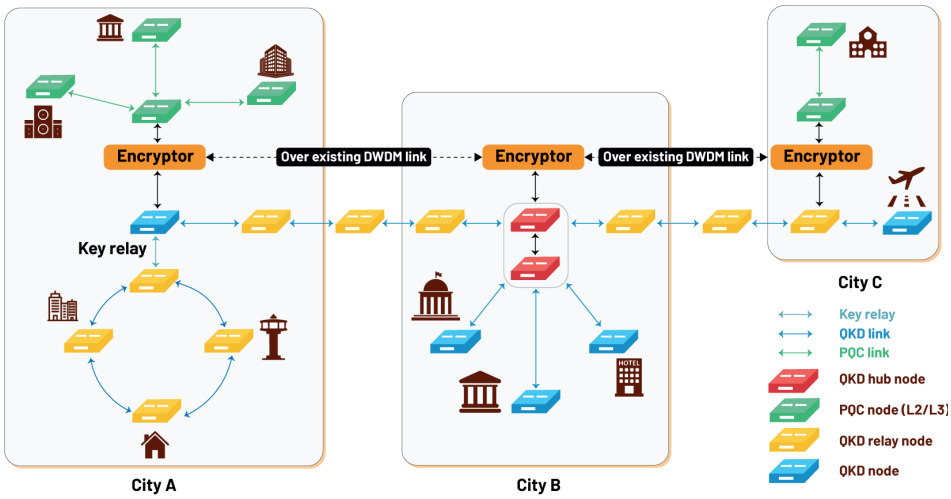


Figure 1: Pictorial representation of inter-city quantum secure network

9.0 Recommendations of the Task Force

The recommendations outlined in this section must be viewed in the context of a rapidly compressing quantum threat horizon. At the World Economic Forum, Davos, in January 2026, the CEO of IonQ warned that "Q-Day"—when quantum computers can break widely used public-key cryptography—may arrive within the next three years [33], while Google has observed that quantum computing today is at a stage comparable to artificial intelligence five years ago, just before its rapid and disruptive acceleration [34]. Bain & Company has issued a sharp warning in its recent study: the quantum threat is no longer a distant possibility but an imminent reality [35]. An alarming 70% of executives expect quantum-enabled cyberattacks within the next five years, and nearly a third believe it could strike in just three. Despite this looming danger, most organisations remain passive, waiting for someone else to take the lead. This complacency is perilous; the countdown has already begun, and hesitation will be the weakest defence. This indicates that quantum disruption may occur abruptly rather than gradually. Accordingly, the following recommendations are not merely preparatory but constitute essential risk-containment measures to prevent irreversible compromise of sensitive data, critical national systems, and economic structure.

CII sectors — government, strategic, defence, power, telecom, transport, and Banking, Financial Services and Insurance (BFSI) — will follow accelerated timelines: Foundations by 2027, High-Priority Migration by 2028, and Full PQC Adoption by 2029. Other enterprises will follow the baseline timelines of 2028, 2030, and 2033 respectively.

All cryptographic transition planning shall proceed under an "assume-breach" principle, recognising the risk of HNDL attacks and the infeasibility of retrospective mitigation after Q-Day. Prioritisation is not restricted to designated critical sectors alone; any network handling data with a long shelf life or extended confidentiality requirements shall be prioritised. Organisations shall strengthen existing cryptographic protections — for example, migrating from AES-128 to AES-256 — to enhance resistance to cryptanalytic and quantum-assisted attacks. The following mandatory actions are recommended, phased to mitigate near-term quantum-enabled cryptographic risk and align with projected Q-Day timelines.

A. Short-Term Actions (By 2028 | CII by 2027)

- Launch PQC/hybrid (classical + PQC) solution sandbox pilots in high-priority systems (e.g., banking and finance sector, government organisations, etc.).
- Communicate the report to other ministries (Railways, Finance, Power, etc.) and regulators (SEBI, RBI, CERC, etc.) to initiate sector-specific guidance, including necessary legal and regulatory frameworks for implementation and compliance.
- All relevant ministries and regulators are to establish and maintain their Cryptographic Asset Repository to enable inventory, lifecycle management, risk assessment, and coordinated migration of cryptographic systems.
- Establish a National PQC Testing & Certification Program under TEC/STQC/BIS, operationalising Tier-1 and Tier-2 labs (As designated in Section 6.0) by December 2026.
- Adopt a Public–Private Partnership (PPP) model to expeditiously develop dedicated laboratory infrastructure for PQC testing and certification.
- Enhance existing laboratory capabilities, which already support testing of QKD systems, to enable comprehensive certification of QKD and related products.

- Adoption of common procurement requirements across all government RFPs shall ensure crypto-agile[1] and PQC-compliant assets, along with compulsory Bill of Materials (BOM)[2].
- Mandate preferential consideration of indigenously developed quantum-safe products and solutions in both public and private organisations, subject to technical suitability and interoperability.
- Organise workshops/seminars to spread awareness on the emerging threats and the urgency to adopt quantum-safe networking.
- The existing approval framework for quantum-safe products will continue until the new infrastructure and processes are operational.
- Mandate the Thematic Hub for the Quantum Communication vertical and technical groups under NQM to:
  - Identify sector-wise post-quantum migration products and solutions in a time-bound manner
  - Promote the adoption of existing indigenous quantum-safe solutions developed by government R&D labs, industries, and startups in India.
  - Undertake gap analysis and fund focused indigenous R&D, in collaboration with academia and industry, to bridge the gap.
  - Focus on developing and deploying gateway devices or quantum-safe middleware solutions to safeguard legacy systems requiring continued protection where full quantum-safe migration may not be immediately feasible.
  - Enable indigenous solutions to reach Technology Readiness Level (TRL) 9 through real-world pilots and financial assistance.
  - Create a pool of available technologies and solutions for post-quantum migration.
- Initiate foundational work for medium- and long-term actions recommended subsequently in the Report.

[1]Crypto-agile: Ability to quickly adapt cryptographic systems, algorithms, and protocols in response to evolving security threats, new standards, or emerging technologies (like quantum computing).

[2]Bill of Materials (BOM) is used as a generic umbrella term. In the context of this report, BOM is a structured, machine-readable inventory of components that constitute a cryptographic system, covering software, hardware, cryptographic primitives, algorithms, libraries, protocols, and dependencies, including their versions, provenance, and security attributes. BOM includes, as applicable, Software Bill of Materials (SBOM), Hardware Bill of Materials (HBOM), and Cryptographic Bill of Materials (CBOM).

- Software Bill of Materials (SBOM): An inventory of software components, libraries, modules, and dependencies used in a cryptographic product or system.
- Hardware Bill of Materials (HBOM): An inventory of hardware components used to implement or support cryptographic functions.
- Cryptographic Bill of Materials (CBOM): A detailed inventory of cryptographic components and configurations used by a system, including algorithms, modes of operation, key sizes, protocols, libraries, random number generators, and cryptographic parameters, covering both classical and quantum-safe cryptography.

B. Medium-Term Actions (By 2030 | CII by 2028)

- Migrate high-priority and long-lifetime systems as well as validate migration through independent testing.
- Upgrade select labs to Tier-3 sovereign-grade (focusing on CII protection) PQC/QKD testing facilities.
- Develop PQC-ready PKI systems and establish national testbeds as foundational infrastructure for crypto-agility and composite PQC–QKD solutions.
- Leverage these national testbeds to support scaling, validation, and sectoral pilots for testing indigenous PQC, QKD, and crypto-agile platforms.
- Organise events and publish lessons learned during the PQC migration cycle.
- Accelerate capacity building through training programs for Chief Information Security Officers (CISOs), DevOps[3] teams, cybersecurity professionals, as well as other stakeholders such as auditors, compliance officers, and risk management personnel.

C. Long-Term Actions (By 2033 | CII by 2029)

- PQC will become the default for all communication systems, assets, and business processes (i.e., complete migration to PQC).
- Establish inter-city QKD networks connecting multiple intra-city QKD networks as a national QKD backbone supporting a composite QKD-PQC architecture.
- Implement a rating framework for organisations based on their post-quantum security adoption, encouraging compliance and progress. Concerned ministries and regulators will define relevant metrics to track migration towards post-quantum security.
- Support the Indian industry in developing indigenous PQC algorithms and facilitate their adoption across critical and strategic sectors through sustained procurement, certification, and lifecycle support.
- Establish continuous monitoring and algorithm lifecycle governance aligned with evolving global standards.

Also, the Task Force recommends that an India-specific list of cryptography-dependent products be prepared, referencing the CISA list, while additionally including mobile phones and automated cryptographic discovery and inventory solutions, and recognising indigenous quantum-safe capabilities across next-generation platforms. This should be clearly communicated as a future compliance requirement for vendors.

Government and CII deployments must act as anchor adopters for validated indigenous quantum-safe technologies, accelerating ecosystem maturity while ensuring national security and supply-chain resilience.

Collaboration with international government agencies actively engaged in PQC migration will ensure India remains aligned with global best practices and emerging trends.

Failure to act within the current planning window may result in irreversible compromise of confidential data, erosion of trust in digital governance, exposure of financial systems, and forced emergency migration under crisis conditions.

This report positions India to navigate the post-quantum era with confidence and strategic clarity. With this roadmap, India joins the league of nations that have formally defined national PQC migration timelines, setting the stage for secure and resilient digital infrastructure.

[3]DevOps: A set of practices and cultural philosophies that integrates software development (Dev) and IT operations (Ops) to enable faster, reliable, and automated delivery of applications through collaboration, continuous integration, and continuous deployment.

10.0 References

1. Cost of a Data Breach Report 2025, The AI Oversight Gap, IBM. URL: https://www.ibm.com/reports/data-breach
2. The Quantum Insider. (2024, August 12). White House report: U.S. federal agencies brace for USD 7.1 billion post-quantum cryptography migration. URL: https://thequantuminsider.com/2024/08/12/white-house-report-u-s-federal-agencies-brace-for-7-1-billion-post-quantum-cryptography-migration/
3. USA cybersecurity in 2030: A geopolitical and policy analysis (2025, June 25). URL: https://cybercenter.space/2025/06/25/usa-cybersecurity-in-2030-a-geopolitical-and-policy-analysis/
4. U.S. Department of Homeland Security. URL: https://www.dhs.gov/quantum
5. Ministry of Digital Affairs of Poland. EU coordinated roadmap for the transition to post-quantum cryptography. URL: https://www.gov.pl/attachment/a4f64757-dd71-4c3c-a222-43a28e0b446e
6. EU reinforces its cybersecurity: Post-quantum cryptography. URL: https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography
7. EU calls for transition to post-quantum cryptography – Are we prepared? URL: https://www.genua.eu/knowledge-base/eu-calls-for-transition-to-post-quantum-cryptography-are-we-prepared/
8. National Cyber and Information Security Agency (NÚKIB). EU member states warn of the quantum threat and call for the transition to post-quantum cryptography. URL: https://nukib.gov.cz/en/infoservis-en/news/2209-eu-member-states-warn-of-the-quantum-threat-and-call-for-the-transition-to-post-quantum-cryptography
9. InCyber. EU unveils roadmap for post-quantum cryptography. URL: https://incyber.org/en/article/eu-unveils-roadmap-post-quantum-cryptography/
10. PQShield. EU PQC workstream publishes a coordinated implementation roadmap for the transition to post-quantum cryptography. URL: https://pqshield.com/eu-pqc-workstream-publishes-a-coordinated-implementation-roadmap-for-the-transition-to-post-quantum-cryptography
11. WiredGov. (2025, March 20). Cyber chiefs unveil new roadmap for post-quantum cryptography migration. URL: https://www.wired-gov.net/wg/news.nsf/articles/Cyber%2Bchiefs%2Bunveil%2Bnew%2Broadmap%2Bfor%2Bpostquantum%2Bcryptography%2Bmigration%2B20032025152500
12. Infosecurity Magazine. (2025). NCSC sets post-quantum cryptography migration timelines. URL: https://www.infosecurity-magazine.com/news/ncsc-post-quantum-cryptography
13. National Cyber Security Centre. (2025). Post-quantum cryptography migration timelines. URL: https://www.ncsc.gov.uk/pdfs/guidance/pqc-migration-timelines.pdf
14. The Register. (2025, March 20). UK NCSC sets out post-quantum cryptography migration roadmap. URL: https://www.theregister.com/2025/03/20/ncsc_post_quantum_cryptography

15. Australian Cyber Security Centre. Planning for post-quantum cryptography. URL: https://www.cyber.gov.au/business-government/secure-design/planning-for-post-quantum-cryptography
16. Post-Quantum. ACSC's post-quantum cryptography policy. URL: https://postquantum.com/quantum-policy/acscs-post-quantum
17. Canadian Centre for Cyber Security. (2025). Roadmap for the migration to post-quantum cryptography for the Government of Canada (ITSM.40.001). URL: https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001
18. Post-Quantum. Canada's post-quantum cryptography roadmap. URL: https://postquantum.com/quantum-policy/canada-pqc-roadmap/
19. PQShield. (2025). Canada publishes new PQC migration roadmap. URL: https://pqshield.com/canada-publishes-new-pqc-migration-roadmap/
20. Infocomm Media Development Authority. National Quantum-Safe Network Plus (NQSN+). URL: https://www.imda.gov.sg/about-imda/emerging-technologies-and-research/national-quantum-safe-network-plus
21. Fraunhofer Singapore. National Quantum-Safe Network (NQSN). URL: https://www.fraunhofer.sg/en/about/solutions/national-quantum-safe-network--nqsn-.html
22. Cyber Security Agency of Singapore. (2025). CSA releases a Quantum-Safe Handbook and Quantum Readiness Index. URL: https://www.csa.gov.sg/news-events/press-releases/csa-releases-a-quantum-safe-handbook-and-quantum-readiness-index/
23. Khaleej Times. (2025, May). UAE issues cybersecurity guidelines to prepare for quantum computing. URL: https://www.khaleejtimes.com/business/tech/uae-cybersecurity-guidelines-quantum-computing
24. Technology Innovation Institute. Abu Dhabi's TII unveils first post-quantum cryptography library in the UAE. URL: https://www.tii.ae/news/abu-dhabis-tii-unveils-first-post-quantum-cryptography-library-uae
25. Asiae. (2025, March 14). South Korea unveils post-quantum cryptography master plan targeting 2035. URL: https://cm.asiae.co.kr/en/article/2025031409333595112
26. Thales Group. SK Telecom and Thales collaborate on post-quantum cryptography. URL: https://www.thalesgroup.com/en/news-centre/press-releases/sk-telecom-and-thales-collaborate-post-quantum-cryptography-enhance
27. Toshiba Digital Solutions. Toshiba and KT demonstrate hybrid quantum-secure communications with Shinhan Bank. URL: https://asia.toshiba.com/press-release/english/toshiba-digital-solutions-and-kt-demonstrate-hybrid-quantum-secure-communications-with-south-koreas-shinhan-bank
28. SEALSQ Corp. (2025, September 22). SEALSQ and the Seoul Metropolitan Government sign MoU to establish a post-quantum semiconductor personalisation, research and design center in Seoul. GlobeNewswire. URL: https://www.globenewswire.com/de/news-release/2025/09/22/3153752/0/en/SEALSQ-and-the-Seoul-Metropolitan-Government-Sign-MoU-to-Establish-a-Post-Quantum-Semiconductor-Personalization-Research-and-Design-Center-in-Seoul.html

29. The Quantum Insider. (2025, February 18). China Launches Its Own Quantum-Resistant Encryption Standards, Bypassing US Efforts. URL: https://thequantuminsider.com/2025/02/18/china-launches-its-own-quantum-resistant-encryption-standard-bypassing-us-efforts/
30. The Quantum Insider. (2025, March 14). China Establishes Quantum-Secure Communication Links With South Africa. URL: https://thequantuminsider.com/2025/03/14/china-established-quantum-secure-communication-links-with-south-africa/
31. MarketsandMarkets™. (2025, October). Post-Quantum Cryptography Market. URL: https://www.marketsandmarkets.com/Market-Reports/post-quantum-cryptography-market-126986626.html
32. MarketsandMarkets™, (2025, February). Quantum Key Distribution Market. URL: https://www.marketsandmarkets.com/Market-Reports/quantum-key-distribution-qkd-market-80654677.html
33. The Economic Times. (2026, January 22). Q-Day may arrive within 3 years, warns IonQ CEO at World Economic Forum, Davos. URL: https://economictimes.indiatimes.com/news/international/globaltrends/q-day-may-arrive-within-3-years-warns-ionq-ceo-at-world-economic-forumdavos/articleshow/127039283.cms?from=mdr
34. The Quantum Insider. (2025, December 2). Google and Intel Veterans Make Bullish Bets on Quantum's Near-Term Payoff. URL: https://thequantuminsider.com/2025/12/02/google-and-intel-veterans-make-bullish-bets-on-quantums-near-term-payoff/
35. sdxcentral. (2026, January 23).Quantum threats loom, but 90% of executives lack a security plan. URL: https://www.sdxcentral.com/news/quantum-threats-loom-but-90-of-executives-lack-a-security-plan/

विज्ञान एवं प्रौद्योगिकी विभाग
DEPARTMENT OF
SCIENCE & TECHNOLOGY

National Quantum Mission

Annexure A

CISA's List of Product Categories for PQC Adoption

Widely Available Hardware and Software Product Categories That Use PQC Standards	
Product Category*	**Example Products/Service Categories***
Cloud Services	Platform-as-a-service (PaaS), infrastructure-as-a-service (IaaS)
Collaboration Software	Chat/messaging
Web Software	Web browsers, web servers
Endpoint Security	Data at rest (DAR) security, full disk encryption

* Some of these categories may have implemented PQC for key encapsulation and key agreement but have not yet widely implemented PQC for digital signatures and authentication.

Hardware and Software Product Categories Transitioning to Use PQC Standards	
Product Category	**Example Product Type**
Networking Hardware	Proxy servers, routers, firewalls, switches, appliances
Networking Software	Software-defined network (SDN), domain name service (DNS), network operating systems
Cloud Services	Software-as-a-service (SaaS)
Telecommunications Hardware	Desk phones, fax machines, voice over IP (VoIP), radio
Computers (Physical and Virtual)	Operating systems, hypervisors, containers
Computer Peripherals	Wireless keyboards, wireless headsets
Storage Area Network	Appliances, operating systems, applications
Identity, Credential, and Access Management (ICAM) Software	Identity management systems, identity provider and federation services, certificate authorities, access brokers, access management software, public key infrastructure (PKI) management software
Identity, Credential, and Access Management (ICAM) Hardware	Hardware security modules (HSM), authentication tokens, badges/cards, badge/card readers
Collaboration Software	Email clients, email servers, conferencing, file sharing
Data	Database, Structured Query Language (SQL) server

Endpoint Security	Password managers, antivirus/anti-malware software, asset management
Enterprise Security	Continuous diagnostics and mitigation (CDM) tools, intrusion detection/monitoring, inspection systems, security information, and event monitoring (SIEM)

विज्ञान एवं प्रौद्योगिकी विभाग
DEPARTMENT OF
SCIENCE & TECHNOLOGY

National Quantum Mission

Annexure B

Framework for Testing and Certification of PQC-based Quantum-Safe Products and Solutions

Introduction

Post-Quantum Cryptography (PQC) comprises cryptographic algorithms designed to remain secure against large-scale, fault-tolerant quantum computers, which can break widely used public-key schemes such as RSA, Diffie–Hellman, and ECC using quantum algorithms like Shor's algorithm. Complementing PQC, Quantum Key Distribution (QKD) enables provably secure key exchange based on the laws of quantum physics, offering information-theoretic security. Rapid global advances in quantum computing, including processors with hundreds of qubits and significant state-level investments, have heightened the HNDL risk, making timely migration to quantum-safe cryptographic mechanisms essential to protect long-term data confidentiality, authentication, and critical infrastructure.

Therefore, there is an urgent need for transition to quantum-safe security in India which requires not only adoption of global Post-Quantum Cryptography (PQC) algorithms but also the establishment of a sovereign, measurement-driven assurance ecosystem. The absence of a national validation and certification framework for PQC creates gaps in trust, exposes systems to implementation-level vulnerabilities and increases dependence on foreign validation mechanisms, thereby eroding strategic autonomy. Therefore, PQC and QKD together form the foundation of future quantum-safe cryptographic ecosystems, making early adoption, testing, and migration essential for ensuring long-term security, trust, and national digital sovereignty.

Global PQC testing and validation

a. Algorithm Validation (Correctness and Standards Conformance)

At the global level, post-quantum cryptographic testing begins with algorithm validation, which ensures that implementations of PQC primitives strictly conform to standardised specifications and produce correct, deterministic outputs. This layer focuses on validating core cryptographic operations such as key generation, encapsulation/decapsulation, and signature generation/verification using authoritative test vectors and Monte-Carlo methods. Internationally, this role is anchored by the Cryptographic Algorithm Validation Program (CAVP) operated by NIST, with automated execution supported through the Automated Cryptographic Validation Protocol (ACVP). Algorithm validation is a prerequisite for higher-level certification, as it establishes that an implementation correctly realizes standardised PQC algorithms before any claims of security, performance, or assurance are made.

b. Cryptographic Module Validation (FIPS / ISO-Based Assurance)

Beyond algorithm correctness, global practice mandates cryptographic module validation, which evaluates the security of the complete cryptographic boundary rather than isolated algorithms. This includes validation of key management, roles and authentication, self-tests, secure states, physical protection, and mitigation of side-channel and fault-based attacks. Internationally, this assurance layer is defined by FIPS 140-3 and its technically equivalent standard IS/ISO/IEC 19790, with testing methodologies prescribed in IS/ISO/IEC 24759. Validation is conducted under structured programs such as the Cryptographic Module Validation Program (CMVP). For PQC, this layer is being progressively extended to include quantum-safe algorithms, hybrid cryptographic constructions, and crypto-agility requirements.

c. Product and System Security Evaluation (Common Criteria Framework)

When PQC is embedded within complete products or systems—such as security gateways, hardware appliances, identity systems, network perimeter devices, post-quantum gateway, single sign-on service or operational technology devices—global practice relies on product-level security evaluation frameworks. The most widely adopted model is Common Criteria (IS/ISO/IEC 15408), which evaluates products against a defined Security Target and specified assurance components. Common Criteria assessments verify not only cryptographic mechanisms but also system architecture, access control, trusted execution, secure boot, update mechanisms, and operational assumptions. This approach enables sovereign and sectoral authorities to assess whether PQC-enabled products meet defined assurance expectations in real deployment environments rather than only at the cryptographic module level.

d. Protocol Conformance and Interoperability Validation

Post-quantum security must operate within real communication protocols, making protocol conformance and interoperability testing a critical global validation category. This layer ensures that PQC and hybrid cryptographic mechanisms integrate correctly into standardised protocols such as TLS, IPsec, SSH, S/MIME etc., without introducing downgrade vulnerabilities or interoperability failures. Globally, this work is driven by the Internet Engineering Task Force (IETF) through evolving protocol specifications and by implementer guidance from standards bodies such as the ETSI. Validation at this level includes cross-vendor interoperability testing, negotiation behavior verification, downgrade-resistance testing, and assurance that PQC adoption does not break existing security guarantees or operational performance.

Scope of the Framework

This framework will be a guiding document for the sectoral regulators (RBI, TRAI, IRDAI, SEBI, CERC etc.) to facilitate the migration to PQC based implementations in a structured, measurable, and trustworthy manner. The document introduces a testing and certification framework for PQC based solutions (systems/devices/services) to be deployed in critical sectors or services that rely on public digital key infrastructure or IT infrastructure. The guidelines are designed to support a wide range of stakeholders, including industry, start-ups, user agencies, certifying bodies, govt organisations, critical information infrastructure users & providers.

The framework maps different types of PQC based solutions to increasing levels of assurance as per their use and risk appetite. Each assurance level ensures that the PQC based solution has undergone listed test cases against the assurance level. The test cases are grouped under the different sub-headings; cryptographic, interoperability, performance and security checks. The cryptographic check ensures correct implementation of cryptographic algorithms including basic functional check. The interoperability ensures cross library/cross platform/cross language validation of PQC based implementation including hybrid implementation using both classical and PQC based cryptography and IETF RFC conformance/validation. The performance validation ensure basic performance like key generation time, throughput etc. at lower levels and compute & storage optimizations at higher levels. The security checks ensure hardware and software security like side channel resistance, vulnerability assessment, penetration testing etc. If a product is compliant under higher assurance level, it is implicit that it complies with lower assurance levels as well. The framework recommends Level 1 for low-risk usage to Level 4 for very high-risk usage. The framework also splits Level 2 into three sub-levels: Level 2A for security testing towards software implementation, Level 2B for security testing for on-premises

hardware security testing (IT/IoT devices) and Level 2C for security testing of hardware parts for Operational Technology devices (like SCADA, PLC, etc.). The framework could be a reference document across all the sectors, the test cases required for sector specific requirements may be appended while evolving their respective framework. Efforts shall be made to harmonize this framework with global standardisation bodies such as NIST PQC standards, IETF RFCs, ETSI Quantum-Safe specifications, and ITU-T/ISO/IEC etc., It does not constitute a legal or regulatory mandate. Adoption, timelines, and enforcement may be determined by the respective sectoral regulators and competent authorities.

Roadmap for implementation of PQC based Quantum-Safe ecosystem in India

The below figure shows an end-to-end framework for testing and certification of Post-Quantum Cryptography (PQC)-based quantum-secure products and solutions. The process begins with mapping PQC products/solutions to defined assurance levels followed by the preparation of a comprehensive test guide that specifies requirements, test methodologies, and evaluation criteria. In parallel, suitable testing laboratories or evaluation bodies are designated as per the test guide, and a validation methodology is established to assess customized or indigenous PQC algorithms/implementations. Products are then submitted by vendors to the designated labs in accordance with the test guide, where they undergo systematic testing and evaluation. The test results are subsequently verified, and certificates are issued for compliant products. This structured approach ultimately enables a trusted and orderly migration from classical cryptographic systems to PQC based quantum-resilient security solutions.

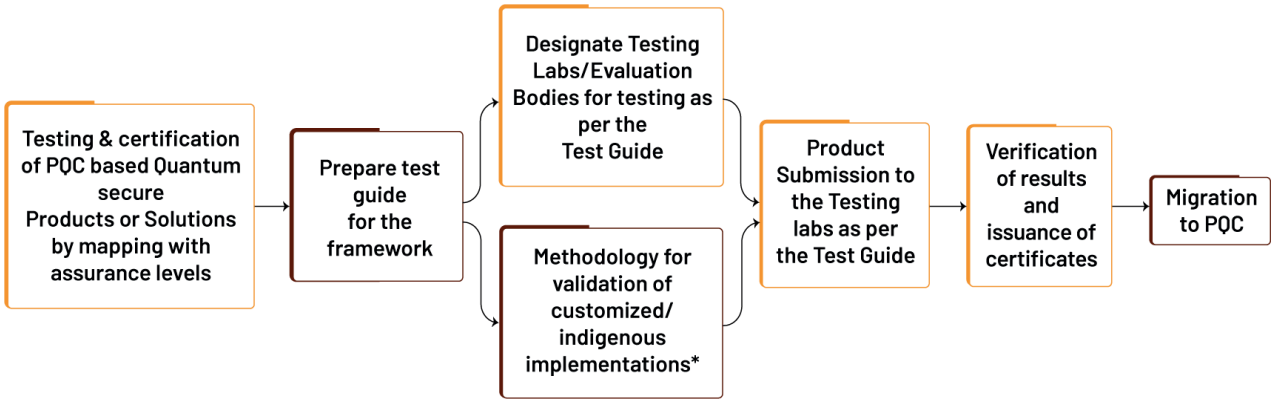


Figure 2 – Schematic representation of testing and certification for PQC migration

**Note: Formal Verification of indigenous/customized algorithm by cryptographers' community and validation of implementation by lab post standardisation by verification team*

In order to facilitate sovereign independence in cryptographic technologies, a dedicated focus group may be constituted to promote indigenous development of post-quantum software libraries, cryptographic protocols, PQC-enabled hardware, and system-level solutions. This group shall coordinate with academia, start-ups, MSMEs, and national laboratories to support design guidance, reference implementations, and test readiness for indigenous products.

The roadmap envisages three basic requirements:

I. Testing requirements as per assurance levels:

This framework document proposes a multiple assurance levels testing framework based on the use and risk appetite in alignment with IS/ISO/IEC 19790 – 'Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules'. However, the test requirements mentioned in this framework goes beyond the scope of IS/ISO/IEC 19790 in which each security level is restricted to the protection of the cryptographic module only. Instead, this framework covers test requirements to validate complete PQC based solution including correctness of PQC/classical cryptographic operations, interoperability checks, software and hardware security, enterprise grade security and critical infra security requirements.

The framework defines four distinct assurance levels organised in a hierarchical structure that addresses escalating security requirements and risk scenarios:

Table 1- Assurance level with usage types, risk category and focus

Level	Name	Risk Category	Usage Type	Primary Focus
1	Basic conformance of PQC implementation	Low Risk	Non-sensitive consumer grade environment	Basic PQC adoption with compliance, interoperability and performance checks
2A	Secure Software Assurance	Medium Risk	Sensitive data consumer grade environments	Secure Software including Cloud-integrated implementations
2B	Secure Hardware Assurance (IoT/IT)	Medium Risk	Hardware resilient Consumer Grade	IT/IoT Edge deployments with hardware resilience
2C	Secure Hardware Assurance (OT)	Medium Risk	Hardware resilient Consumer Grade	Operational technology environments
3	Enterprise Infrastructure Security	High Risk	Enterprise Grade	Long-term enterprise security for sectors like finance, telecom, healthcare etc.
4	Critical Infrastructure Security	Very High Risk	Sovereign Grade	Critical information infrastructure protection

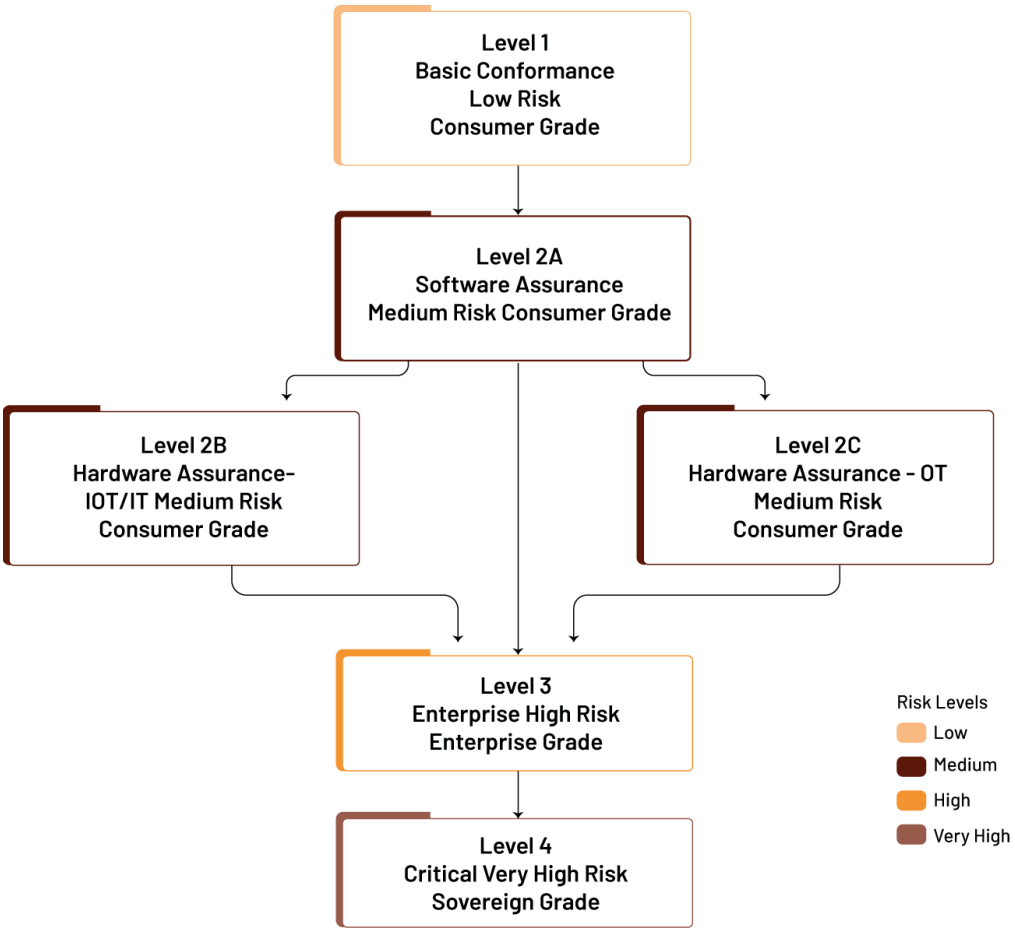


Figure 3 – Assurance Levels vis-a-vis risk level

The detailed test cases under each assurance level are mentioned in **Annexure-I (refer to Page 62)**. Synopsis of the test cases under different parameter category for each assurance level is given below:

Table 2- Synopsis of the test cases under different parameter category for each assurance level

Parameter Categories	**Level 1 : Basic conformance of PQC implementation**	**Level 2A : Secure Software Assurance**	**Level 2B :Secure Hardware Assurance (IoT/IT) & Level 2C-Secure Hardware Assurance (OT)**	**Level 3: Enterprise Infrastructure Security**	**Level 4: Critical Infrastructure Security**
Cryptographic Checks	• Functional verification of PQC Algorithms (ML-KEM, ML-DSA etc.) • Functional verification of Classical algorithms (AES, DSA, RSA, ECC, Hashing algorithm like SHA etc.) * • Verification of Random Number Generator (RNG) including performanc-e through statistical test suite.	• Includes up to Level 1. • Key lifecycle managemen t for cloud based HSMs. • Validation of multi-person (M-of-N) authorizat-ion controls with multifactor authenticat-ion for all cryptograp-hic. operations • Resistance to PQC Parameter Downgrade Attacks.	• Includes up to Level 2A. • Validation of Key lifecycle managemen t with agility for on-premises Hardware Security Module (HSM)/Trus-ted Platform Module (TPM).	• Includes up to 2B/2C as applicable. • Conformanc e to PQC Algorithm. • Crypto-agility Validation. • TRNG/ QRNG entropy validation - validation of claimed physical entropy source for non-repudiati-on, integrity, and non-repetition of quantum-sourced seed material.	• Includes up to Level 3. • Validation of hybrid implement-ation - fetching key from QKD module (as per sector requireme-nts). • Customized implement-ation of verified indigenous algorithm. • Strategic Resilience and Algorithm Diversifica-tion Capability.

Interoperability	• Interoperability with Standardized APIs or reference implementation. • Conformance with published RFCs by IETF of TCP/IP protocols (IPSec, TLS, HTTPS, API)*. • Validation of Hybrid implementations (Classical + PQC based implementations) • Cross-Library/Cross platform (Linux, windows etc.)/Cross language (C, Java etc.) Testing.				
Performance Considerations	Basic performance testing (throughput, latency, key generation and revocation time, Encapsulation/Encryption/Signature generation Time, Decapsulation/Decryption/Signature Verification Time, HMAC Computation Time, Hashing Throughput).			Includes basic performance as per initial levels with rigorous performance testing including memory usage, CPU/GPU usage & acceleration, power usage, scalability, bandwidth overhead, crypto-agility performance.	Includes performance as per Level 3 • Validation of disaster resilience and business continuity.
Security Assurance	• Error Handling & Robustness against: o Wrong inputs. o Signature or cipher text forgery attempts.	• Up to Level 1 • Fuzz testing, Negative and Mutation Testing • Vulnerability Analysis (VA)/Penetration Testing (PT)	• Level 2A security included • Hardware root of trust (Trusted Execution Environment, Secure boot & attestation)	• Includes up to Level 2B/2C as applicable • Continuous Integration (CI)/Continuous Deployment (CD) integration and automation	• Includes up to Level 3 • Zero Trust Architecture Compliance-explicit testing of Secure Failure Modes. • Red Team Testing

	o PQC Input Falsification Resistance. • Static Vulnerability Analysis.	• Source code review – test reports or Self declaration of conformity from OEM. • Memory Analysis. • Adoption of Secure Coding Practices. • Timing Attack - Side channel resistance.	• Side channel resistance testing including at session boundaries. • Physical Tamper Resistance. • Hardware specific security testing of IoT/IT Testing - Level 2B. o OT Specific Testing – Level 2C	• Automated vulnerability discovery. • Security assessment/ audit. • Supply chain security - including hardware, firmware, software, and critical components • Validation of secure Key Derivation Function (KDF). • Validation of secure integration with centralized cryptographic management systems.	• Semi-Formal Verification of Critical Components. • Rigorous Supply Chain Security Verification – semiconductor level assurance. • Nation-State Attack Simulation.
Other requirements	• Documentation & Metadata- Clear documentation of: o Algorithm used. o Security level. o Sets of Parameter. o Version and source of implementation.	-	-	Sector specific Regulatory Compliances and cryptographic policies (energy, Telecom, finance etc.)	Additional Compliance as per strategic sectors – not part of this framework.

Note –

1. *EMI/EMC, Safety, Environment, Technical conformance (including RF conformance & others) to be tested as per Indian requirements.*
2. *Higher Level of assurance needs to comply with requirements of lower assurance levels.*
3. *Already available test results/compliance certificate (like FIPS 140-2) may be accepted against Functional validation of classical cryptographic algorithms (AES, DSA, RSA, ECC, SHA etc.) as per guidelines from sectoral regulators. List of Cryptographic Algorithms and globally available Standards for Quantum Technologies is attached as **Annexure-IV** and **Annexure-V** respectively.*
4. *Migration timeline to use of PQC based PKI certificates may be decided by Sectoral regulators as per their PQC migration guidelines.*
5. *In case IETF RFC is not yet published for PQC (country specific standards) based implementation, functional validation may be done as per existing RFCs using packet analysers. PQC integrated RFC as and when published shall be applicable and the device conformance shall be tested as per the latest RFC.*
6. *Indigenous PQC implementation is recommended to be used by critical sectors, however, other sectors may use standardised algorithms. Parameters for testing and validation of customized/indigenous algorithms/implementations is attached as **Annexure-II**.*
7. *Higher assurance levels (L1–L4) shall require proportionally higher PQC security categories with corresponding increases in key sizes and parameter sets to provide proportionally stronger resistance to cryptanalytic and quantum attacks.*
8. *As increased security may degrade performance, sectors may define the required performance benchmarks based on their specific requirements and prevailing market forces. Hardware and software baselining shall be conducted before measuring performance parameters.*

II. Criteria for designating testing labs-

To ensure consistency, trust, and international recognition of PQC testing outcomes, laboratories conducting testing shall have the eligibility criteria as under:

a. Eligibility Criteria

- Shall meet eligibility under IS/ISO/IEC 17025 (general requirements for the competence of testing and calibration labs) verified by accreditation bodies (e.g., NABL) or sectoral regulators.
- Demonstrate expertise in cryptographic testing including PQC, side-channel analysis, interoperability testing, VA/PT etc.
- Availability of qualified personnel with relevant certifications (e.g., CISSP, CEH, Crypto-specific qualifications).
- Secure facilities for handling sensitive data in compliance with national cybersecurity guidelines and privacy laws (e.g., DPDP Act).
- Additionally, any other eligibility criteria may be decided by sectoral regulators as per their requirements.

b. Designation Tiers

- Tier-1 Labs: Focused on functional compliance and interoperability testing as per Level 1. These labs also need to validate the RFC conformance such as IPSEC, TLS etc. Already designated TEC/BIS labs may be upgraded for this type of testing as per the eligibility criteria mentioned above.
- Tier-2 Labs: Capable of software and hardware assurance testing as per Level 2A/2B/2C. These labs may have test capabilities for Level 1. However, if they don't have Level 1 test capability, then they will have to liaise with Tier –I labs for Level 1 testing. BIS, STQC, CERT-In empanelled and NCCS designated labs may be upgraded for this testing as per the eligibility criteria mentioned above.
- Tier-3 Labs: Advanced facilities for enterprise-grade and sovereign-grade evaluation, including crypto-agility validation, TRNG/QRNG integration, custom algorithm validation as per Level 3 & 4. These labs may have test capabilities up to Level 2. However, if they don't have Level 2 test capability, then they will have to liaise with Tier –1 & Tier-2 labs for Level 1 & 2 testing.

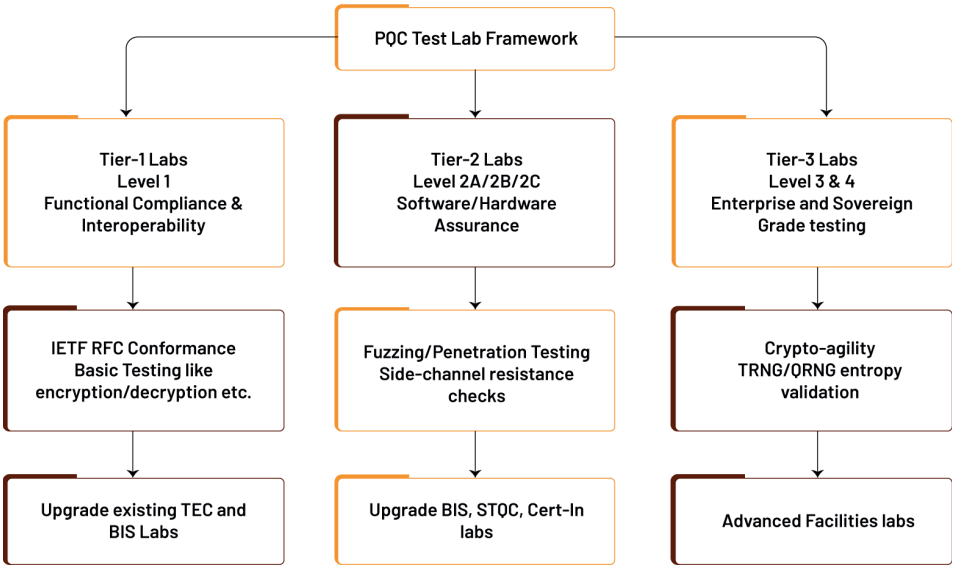


Figure 4 – Lab Designation Tiers

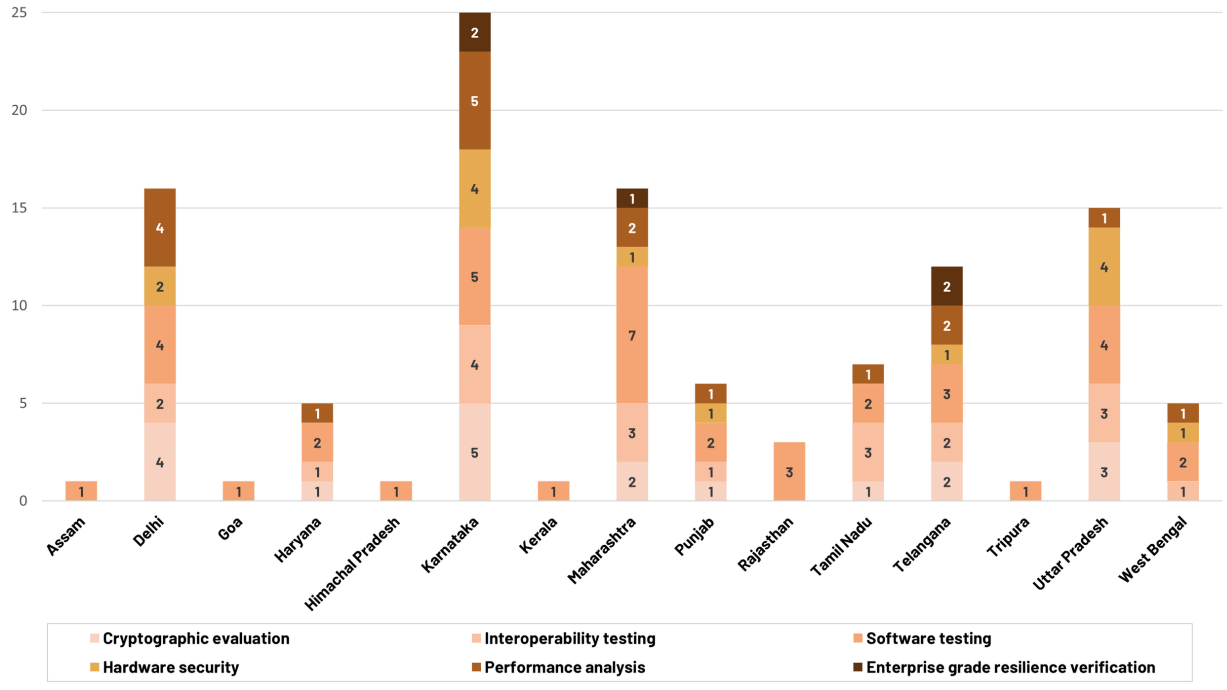
STQC's existing certification schemes, including Common Criteria, Crypto Module Validation (ISO/IEC 19790), ISMS, and product security schemes, shall be leveraged and extended to support PQC certification, including hardware and software evaluations.

c. Audit and Recognition

- Initial designation of labs may be done based on a joint inspection by the nodal agency (e.g., TEC, MeitY, BIS and sector regulators).
- Until the labs are designated, a joint witness testing can be conducted at the vendor premise by the nodal agency (e.g., TEC, BIS, MeitY and sector regulators).
- Encouragement of Mutual Recognition Agreements with accredited foreign labs shall be done for accepting mutual test results to promote cross-certification for global acceptance.
- The number of required PQC testing laboratories shall be assessed based on sectoral demand, assurance levels, and geographic distribution.
- A minimum baseline equipment list for PQC evaluation laboratories shall be separately notified and updated periodically.

d. Test Labs in the country

- The Migration strategy proposes commencing of migration to PQC of critical applications from January 2027 and to be completed by December 2029 whereas for non-critical applications these timelines are from January 2029 to December 2033. Therefore, testing and Certification of PQC labs in the country should come up by December 2026 so that one year will be there for testing of the products/solutions.
- The test labs are not specifically available in the country w.r.t. PQC testing as on date but available for testing w.r.t test areas like Vulnerability testing, Hardware testing, Performance analysis etc. for the classical cryptographic systems.
- The currently available testing labs in the country w.r.t. the testing requirements of classical cryptographic systems is attached as **Annexure-III**. These labs may be upgraded to take care of PQC products in future.
- The indicative distribution of labs as per type of test parameters is as under -



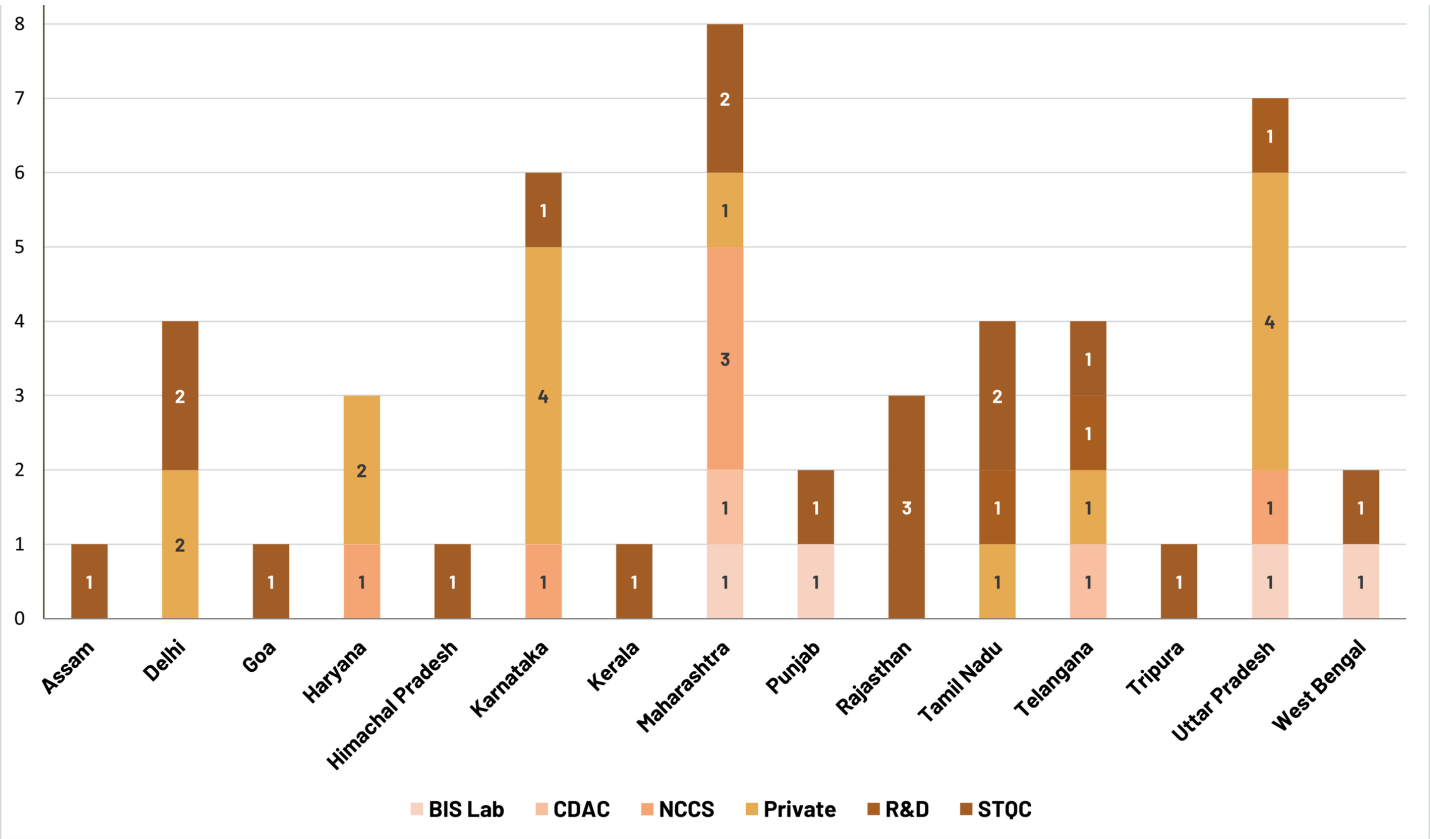


Figure 5: Bar graph showing the state-wise distribution of existing test labs

III. Certification Process

The certification process ensures that PQC based quantum-safe products and solutions meet defined assurance levels:

a. Submission & Pre-Assessment

- Vendor shall apply for certification to Certification Authority (CA)/Certification Body (CB) (e.g., TEC, STQC, BIS or sectors regulators) specifying intended assurance level (L1–L4) along with Application Form, Certification Agreement, TCF (Technical Construction File) providing compliance status of requirements along with the supporting documents and test records and reports) and Fee Receipt as part of application submission.
- Pre-assessment shall be done by CB/CA against eligibility criteria (documentation, BOM of the product including SBOM & CBOM, deployment environment).

b. Testing & Evaluation

- CB/CA assigns the lab for carrying out evaluation against submitted application. It also assigns a validator who validates the evaluation results by reviewing evaluator's observations and artifacts under evaluation. Assigned designated lab performs evaluation as per the mapped level requirements and the high-level criteria mentioned in Annexure-I of this document.
- The sectoral regulators may specify requirements in addition to the above defined levels for which the product can be tested by the lab designated for those requirements or witness testing as decided by the sector.

c. Review by Certification Authority

All Test/Evaluation reports, Validator's reports will be submitted to CB/CA for review based on which it will decide to grant/reject the certificate.

d. Issuance of Certificate

- Certificates shall be issued with clear mention of an assurance level (L1-L4) and validity period as per a pre-defined certificate template (sample template attached as Annexure-VI). However, during the validity of the certificate, the applicant has to ensure compliance to any new vulnerabilities notified by CERT-In/sectoral CERTs or change in assurance requirements within a specified time frame by the CA/CB to avoid suspension or revocation of the certificate.
- Requirement of retesting, in case of major software/hardware upgrade, may be decided by CA/CB based upon the effect on existing assurance level (L1-L4) compliance and accordingly incremental or full testing may be conducted. If compliance to existing level is not impacted (like in case of updates/patches), then SDoC (self-declaration of certificate) with internal test reports may be taken based on the impact analysis report submitted by OEM to CA/CB.
- Certification validity may be a minimum 3 years for L1, 5 years for L2, 7 years for L3 and 10 years for L4 subject to acceptance/review by sectoral regulators. Certification validity shall be risk-aligned and vulnerability-aware. Long certification periods shall be subject to mandatory surveillance, vulnerability monitoring, and re-assessment triggers. For rapidly evolving PQC implementations, shorter certification cycles with continuous compliance monitoring are recommended over long fixed validity periods.
- The requirement for re-certification in case of major software/hardware upgrade or identification of critical vulnerabilities shall be clearly mentioned in the terms and conditions of the issued certificate.

- The maximum time for testing and certification may not be more than six months subject to development of testing infrastructure in the country and as per sectoral requirements. Further, the framework encourages the use of automation, standardised test harnesses, continuous testing pipelines, and AI-assisted analysis to progressively reduce testing and certification timelines. Certification duration shall be optimized without compromising assurance.

e. Surveillance (Verification of continued compliance of certified products)

Surveillance of the products as per issued certificate may be carried out as per sector-specific regulations.

The above certification process can be diagrammatically represented as under:

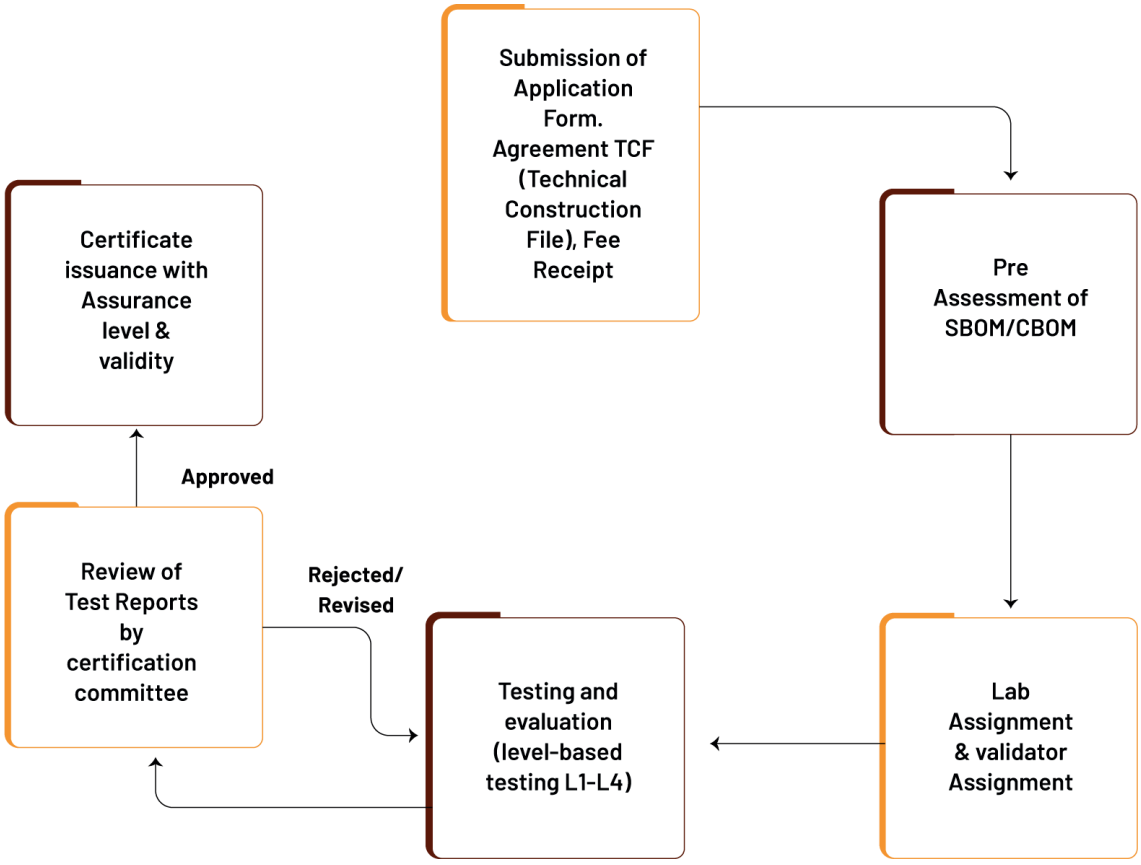


Figure 6 – Flow diagram for Certification process

Challenges and Conclusion

Cryptographic modules are essential for ensuring the protection of both data at rest and in transit. These modules can be implemented in three modes:

- Software-only
- Hardware-only
- Hybrid (software + hardware)

Globally, the IS/ISO/IEC 19790 standard (aligned with FIPS 140-3) serves as the basis for the Cryptographic Module Validation Program (CMVP). Various countries such as the USA, Canada, members of the European Union, the UK, Japan, and Korea operate their own national validation schemes based on this standard. This standard mandates an in-depth design review and white-box testing of cryptographic modules to ensure their robustness.

As per IS/ISO/IEC 19790, comprehensive documentation is required for validation. However, Original Equipment Manufacturers (OEMs) and developers often show reluctance in sharing such sensitive design and implementation details. In cases where this documentation is unavailable, testing and review may be conducted on the basis of the cryptographic bill of materials and self-test reports as an interim measure.

In other countries, hardware OEMs facilitate access to the documentation and test facilities within their jurisdictions, enabling complete validation. However, in India, these OEMs are reluctant to share the documentation part, which makes full validation of hardware-based cryptographic modules infeasible at present. Consequently, CMVP can currently be undertaken only for software-based cryptographic modules that are entirely developed within India and where the developers are willing to provide complete documentation. In future, as cryptographic integrated circuits (ICs) begin to be manufactured in India, validation of hardware or hybrid modules may become feasible provided the OEMs permit the use of their premises, facilities, and resources, and make the necessary documentation available.

Further, validation of indigenous algorithms is complicated by the lack of mature test vectors, interoperability profiles, and deployment guidance, especially as IETF RFCs for PQC integration into mainstream protocols are still under drafting, creating uncertainty around long-term interoperability and crypto-agility across heterogeneous and evolving deployments.

To address current PQC adoption and validation challenges, a coordinated national approach is essential. Public consultation should be conducted to build wider stakeholder acceptance and ensure practical, industry-aligned frameworks. Existing test laboratories must be upgraded with PQC-specific infrastructure and skills, while continuous alignment with global testing and certification practices will ensure international compatibility. Long-term sustainability requires structured collaboration among academia, industry, and standards bodies to develop expertise and evolve requirements. Establishing end-to-end PQC testbeds for indigenous modules, along with Centres of Excellence/Experience in Quantum Technologies, will enable realistic validation, interoperability testing, and workforce development. Finally, systematic promotion of indigenous algorithm design, optimized implementations, and full system-level integrations will strengthen national self-reliance while ensuring crypto-agility and global interoperability in the quantum-safe transition.

Test Requirements as per Assurance Levels

1. Level 1 - Basic conformance of PQC implementation

Objective: Verify that the implementation matches the cryptographic specification, known test vectors and protocol conformance, interoperability and performance checks. The test cases for level 1 are categorized as below:

1.1. Cryptographic Algorithm Check - Ensure cryptographic algorithm implementations strictly adhere to reference specifications, exhibit deterministic behavior where applicable, and produce outputs consistent with standardised test vectors

1.1.1. Testing Methodology:

1.1.1.1. **Known Answer Tests (KATs):** Utilize deterministic, precomputed test vectors from authoritative sources (e.g., NIST PQC Test Vectors v1.0, PQClean, github) to validate implementation behavior across all supported primitives. The test vector version tracking should be done in test reports with requirement to re-test when new test vectors are published.

1.1.1.2. **Consistency and Integrity Checks:** These tests validate algorithm correctness beyond KATs by ensuring bidirectional transformations yield expected results under various edge-case conditions.

1.1.1.3. Higher assurance levels shall mandate the use of higher PQC security categories (as defined by NIST or equivalent authoritative bodies), including increased key sizes and parameter sets. Compliance shall be demonstrated by mapping each supported PQC algorithm and parameter set to the product assurance level in the test documentation and verifying enforcement through configuration and test results.

1.1.1.4. **Error Handling & Robustness:**

- Primitive Cryptographic attacks
- Signature or cipher text forgery attempts
- Observe correct rejection and error signaling

1.1.1.5. Run automated tests to ensure key size, structure, and entropy are compliant.

1.1.1.6. Rejection Rate should be calculated for ML-KEM algorithms (ML-KEM).

1.1.1.7. Auxiliary functions associated with encryption/key exchange algorithms like hashing should also be tested.

1.1.2. Existing Test Tools for above cryptographic tests:

1.1.2.1. Reference Repositories:

- ACVP GitHub Repository
- NIST PQC Test Vectors with version tracking

1.1.2.2. PQClean Suite:Reference C implementations with deterministic testing harnesses.

1.1.2.3. Cryptographic Libraries and Interfaces:

- OpenSSL
- Command-line tools for KAT testing

1.1.2.4. Python Modules:

- pyca/cryptography, hashlib, hmac: For prototyping and functional tests across all hash-based and symmetric primitives.

1.2. RFC Conformance for TCP/IP Protocol Validation – Verifies conformance of PQC integration with IETF protocols like TLS, SSH, S-MIME, HTTPS etc.

1.2.1. Testing Methodology:

1.2.1.1. Run RFC conformance suite on the submitted product applicable as per IETF protocols like TLS, IPSEC, SSH etc. to test RFC Conformance wherever PQC enabled RFCs have been published.

1.2.1.2. Verify End-to-End Functional Testing

- Establish encrypted channels using PQC/hybrid mechanisms
- Verify successful handshake, key agreement, message encryption/decryption
- Validate signature chains (certificates, key verification)
- Tools: curl, openssl s_client, tshark, Wireshark, strongSwan, GnuPG etc

1.2.1.3. Verify Protocol Conformance Testing

- Ensure message formats, error handling, and cipher suite negotiation complies to applicable latest RFCs.
- Validate hybrid handshakes in TLS (e.g., RFC 8446 + ML-KEM integration).
- Tools: OpenSSL Test Harness,TLS Interop Test Suite (MbedTLS / NSS) etc.

1.2.1.4. If RFCs are not published

- Check Protocol Integration with packet analyser tools like Wireshark etc. for protocol used like TLS Handshake, PKI Integration etc.
- Verification of components through bill of material (hardware and software including cryptographic).
- Validation report of the source code with approved tools.
- Hybrid Protocol Validation (e.g., IPsec/IKEv2 with PQC Integration, SSH with PQC, TLS 1.3 PQC Hybrid Handshake).
- The vendor shall document PQC integration approach.

1.3. Cross-library, Cross-platform and Cross-language interoperability

1.3.1. Cross-library Compatibility Testing - Confirm that independent implementations produce interoperable outputs for key encapsulation, digital signatures, encryption/decryption, and MAC computations. For e.g.,-

- Encrypt with liboqs, decrypt with OpenSSL
- Sign with wolfSSL, verify with BoringSSL

1.3.2. Cross-platform Testing - Confirm that independent implementations produce interoperable outputs across various system under test.

1.3.2.1. Systems Under Test:

- OS: Linux (Ubuntu,Fedora), Windows, FreeBSD, macOS etc.
- Architectures: x86_64, ARM64/32, RISC-V
- Environments: Bare-metal, containers (Docker), cloud VMs)

1.3.2.2. Validation Criteria:

- Output equivalence across platforms
- Behavioral consistency under identical protocol scenarios

1.3.3. Cross-language compatibility (C ⇔ Java ⇔ Python) – Confirm that independent implementations written in different languages like C, Java, Python etc. produce interoperable outputs.

1.3.4. Testing Methodology for Cross-library, Cross-platform and Cross-language interoperability:

- All libraries compiled using consistent compiler options and PQC parameter sets.
- Reference vectors from NIST used as the base for verification.
- Encrypt/sign on one library → Decrypt/verify on another.
- Compile for different platforms and languages and test interoperability.

1.4. Performance Analysis - Measures basic performance like key generation time, throughputs etc. It is a functional testing only and may be specified on test certificate or as product specifications.

1.4.1. Key Performance Metrics (Representative Values) *

Metric	Kyber (ML-KEM)	Dilithium (ML-DSA)	SPHINCS+ (Hash-based)	McEliece (Code-based)
Key Generation Time	~0.02–0.05 ms	~0.05–0.1 ms	~5–10 ms	~10–20 ms
Encryption/Encapsulation	~0.03–0.08 ms	N/A	N/A	~0.5–1 ms
Decryption/Decapsulation	~0.04–0.1 ms	N/A	N/A	~1–2 ms
Signature Generation	N/A	~0.1–0.3 ms	~10–20 ms	N/A
Signature Verification	N/A	~0.05–0.2 ms	~5–10 ms	N/A
Public Key Size	800–1184 bytes	1312–2592 bytes	~32 bytes	~1 MB
Private Key Size	1632–2400 bytes	2528–4896 bytes	~64 bytes	~1 MB
Signature Size	N/A	2420–4595 bytes	~8–17 KB	N/A
Memory Footprint (IoT)	~10–50 KB RAM	~20–80 KB RAM	~100–200 KB RAM	>1 MB RAM

**Note - These are representative values and not absolute values which are derived from peer-reviewed evaluations published in MDPI Cryptography (2025), JISE, using liboqs v0.7.2 across server-class and edge platforms with 1000-iteration measurements at NIST Security Level-3.*

1.4.2. Tools for performance measurement: A diverse suite of tools is used to measure latency, resource consumption, and performance bottlenecks such as SUPERCOP, OpenSSL speed, Google Benchmark, perf, gprof, Valgrind (Massif / Callgrind), hyperfine, time, rdtsc(), EnergyTrace / Power Profiler Kit, QEMU, arm-none-eabi-gcc, heaptrack, cachegrind etc.

1.4.3. Test Methodology

1.4.3.1. **Setup**

- Compile with performance-optimized (disable debug options) flags
- Disable unnecessary runtime checks.
- Use real-world-sized keys and messages (e.g., 2048-bit equivalent, 1KB messages).
- Ensure uniformity across test platform used for any kind of performance testing and create hardware and software baseline.

1.4.3.2. **Measurement Process**

- Average over 1000+ iterations to reduce variance.
- Run on isolated CPU cores or dedicated testbed to eliminate OS scheduling noise.
- Use randomized test inputs to capture statistical variance.
- Acceptable performance ranges shall be within ±20% of reference values.

1.5. If PQC library is used from a clean source repository (like GitHub) without any modification, hash value from source repository of crypto implementation and implementation done by the OEM may be compared for integrity.

1.6. The standardised statistical tests shall be performed to validate the randomness, entropy, and bias resistance of all cryptographic RNGs in accordance with applicable standards.

1.7. Static Vulnerability analysis shall be done and report shall be submitted.

1.8. Verification of software, cryptographic, and hardware components shall leverage SBOM, CBOM, and QBOM frameworks as notified by CERT-In. Existing CERT-In guidelines and formats shall be adopted to ensure uniformity and auditability.

2. Level 2A – Secure Software Assurance

Objective: Verify software security, fuzz testing, robustness, fault tolerance etc.

2.1. **Fuzz Testing, Negative & Mutation Testing:**

2.1.1. Discover memory safety issues and unexpected behaviors. Test with below Inputs:

- Corrupted ciphertexts / signatures
- Null or malformed keys
- Excessively large inputs
- Truncated or padded inputs

2.1.2. Assess robustness to malformed, random, or edge-case inputs in real-time.

2.1.3. Coverage-based fuzzing shall be done to help identify crashes, memory corruptions, or undefined behavior with minimum 80% branch coverage.

2.1.4. Minimum fuzzing duration may be kept as 24 hours or 1 week.

2.1.5. Any fuzzing finding that results in a crash, memory corruption, or undefined behavior shall be classified as Critical and shall require remediation and re-testing prior to acceptance or deployment.

2.1.6. Tools: afl++, libFuzzer, Honggfuzz etc.

2.2. Timing Analysis: Check for timing variations arising from branch-dependent execution paths during the decapsulation and verification processes to ensure that operations are executed in constant time and are not influenced by secret or key-dependent data. Tools: valgrind, ctgrind etc.

2.3. The product shall enforce and validate multi-person (M-of-N) authorization controls for all critical cryptographic operations, including master key generation, activation, and destruction. Validation shall confirm that operations cannot be executed without the required quorum, that minimum M and N values are configurable based on assurance level, and that single-person compromise is technically prevented. All multi-person control events shall be securely logged, auditable, and resistant to bypass or circumvention.

2.4. The product shall enforce protocol-level protections against PQC parameter downgrade attacks, ensuring that adversaries cannot force negotiation of weaker security parameter sets when stronger options are available. Validation shall demonstrate strict enforcement of minimum approved parameter sets, rejection of downgrade attempts, immutable policy configuration, and conformance testing across supported protocols to ensure downgrade resistance cannot be bypassed.

2.5. The OEM shall ensure that Vulnerability Assessment and Penetration Testing (VA/PT) of the system is carried out by an Information Security Auditing Organisation empanelled with CERT-In (MeitY, Government of India). The VA/PT report shall be submitted and reviewed for following:

2.5.1. Ensure testing covered all application components — API endpoints, web UI, backend services, and data interfaces.

2.5.2. Verify that cloud integrations and HSM interfaces were included in testing.

2.5.3. Ensure both automated and manual testing were performed.

2.5.4. Review the VA/PT report for:

- Classification of vulnerabilities (Critical, High, Medium, Low)
- Risk rating and CVSS scoring
- Recommended mitigations and closure evidence
- Mitigation Verification

2.5.5. Check that all Critical and High vulnerabilities have been remediated and re-tested.

2.5.6. Validate that residual risk is documented and approved.

2.5.7. The validity of VA/PT reports shall be as per the re-testing requirements mentioned in Section –III of framework i.e. Certification Process- Issuance of Certificate.

2.6. Secure Coding practice shall be verified with steps as under:

2.6.1. Static Analysis using tools.

2.6.2. Manual code inspection to verify:

- Input validation and sanitization
- Proper authentication and session management
- Secure cryptographic implementations (e.g., no hardcoded keys)
- Error/exception handling without information leakage

2.6.3. Verify compliance with standards such as OWASP Top 10 etc.

2.6.4. Check for vulnerabilities in third-party libraries.

2.6.5. Confirm use of version control with restricted access (multi-factor authentication).

2.6.6. Ensure code commits and merges require peer review and approval.

2.7. The cloud based key lifecycle management shall be verified as under:

Objective: Assess security of cryptographic key generation, storage, use, rotation, and destruction using cloud HSM.

2.7.1. Verify integration of Cloud HSM (e.g., AWS CloudHSM, Azure Key Vault,Google Cloud KMS etc.)

2.7.2. All Cloud HSM deployments shall support complete cryptographic key lifecycle management, including secure key generation, storage, usage, rotation, archival, and destruction.

2.7.3. Cryptographic keys shall be generated and remain within FIPS 140-2 Level 3 (or higher) validated HSM boundaries, and plaintext export of key material shall not be permitted.

2.7.4. Access to keys shall be governed by role-based access control, enforcing least-privilege, segregation of duties and multi-factor authentication.

2.7.5. Key rotation policies shall be mandatorily enforced, with key rotation periods as per NIST SP 800-57 Part 1 Rev. 5. The key rotation periods shall be shorter for high-risk systems (i.e. for Level 3 and 4 PQC products). Longer crypto period is allowed for Root / Master keys but periodic rotation is recommended.

2.7.6. Automated rotation mechanisms shall be supported without service disruption, and previous key versions shall remain available for decryption or verification only.

2.7.7. All key lifecycle events—including creation, access, rotation, policy changes, and destruction—shall generate immutable audit logs.

2.7.8. Audit logs shall be tamper-evident, exportable to external systems with audit log retention periods as defined in alignment with NIST SP 800-57, NIST SP 800-53, ISO/IEC 11770, ISO/IEC 27001, and applicable national regulatory requirements, including CERT-In cybersecurity directions. For e.g., – The Audit logs may be retained online for a minimum of 400 days, and archived securely for a minimum period of seven years.

2.7.9. Cryptographic destruction of keys shall be irreversible and verifiable through audit evidence.

2.7.10. Validate key generation uses approved algorithms.

2.7.11. Check secure key provisioning, distribution, rotation, archival, and destruction mechanisms as per above steps.

2.7.12. Verify access control and audit logs for key usage events as per above steps.

2.7.13. Verify that only authorized services or users can access HSM APIs and review IAM policies and role-based access configurations.

2.7.14. Perform dynamic tests on key management APIs for:

2.7.15. Verify Cloud HSM complies with FIPS/ISO standards (or equivalent) at least FIPS 140-2 Level 3 (or higher) validated HSMs.

3. Level 2B & 2C - Hardware Assurance – Common testing

3.1. **Side-Channel Resistance Testing:** Verify hardware side channel resistance and mitigation techniques as mentioned below.

3.1.1. **Techniques:**

Method	**Description**
Timing Attack Analysis	Measure execution time variations
Differential Power Analysis	Analyze power consumption differentials
Simple Power Analysis	Detect patterns in power trace
Fault Injection	Inject transient faults to induce failures
Electromagnetic (EM) Leakage	Capture EM emissions to infer data
Cache Timing Attacks	Exploit cache latency variations
Branch Prediction Analysis	Leverage mispredicted branches
Memory Access Pattern Analysis	Study memory access patterns

3.1.2. **Tools for side channel resistance evaluation:** ChipWhisperer, Riscure Inspector, Dudect, Anveshak (IIT Kharagpur), Ctgrind, valgrind/cachegrind, oscilloscope + EM probes etc.

3.1.3. **Side Channel Analysis (SCA) Test cases as per cryptographic protocols:**

Algorithm Type	**SCA Test cases**
Asymmetric PQC (KEM)	Key mismatch detection, decapsulation leakage
PQC Signatures	SPA on modular arithmetic, hash collisions, fault tolerance

Symmetric Primitives	T-table lookups, MAC padding attacks, fixed key cycles
Hybrid Protocols	Combined state leakage, session key recovery
Embedded Platforms	Fault injection & EM leakages on side-channel exposed silicon

3.1.4. **Testing requirements**

3.1.4.1. Minimum number of power traces (e.g., 10,000 traces minimum)

3.1.4.2. TVLA (Test Vector Leakage Assessment) pass criteria (t-value < 4.5)

3.1.4.3. Equipment calibration certificates are required.

3.1.4.4. Validate protection against side-channel leakage across session boundaries.

3.1.5. **Mitigation Techniques**

3.1.5.1. Constant-time implementations (memcmp, loops, lookup tables)

3.1.5.2. Randomized blinding, masking, and shuffling techniques

3.1.5.3. Fault-resistant code with redundant verification

3.1.5.4. Compiler hardening (e.g., -fno-builtin, -fstack-protector-all)

3.1.5.5. Hardware defenses: EM shielding, clock jitter, secure enclaves

3.2. Inspect HSM logs and run PQC key ops via PKCS#11 interface for verifying HSM integration and secure key storage. Check for HSM agility also.

3.3. Request secure boot logs or HSM integration scripts. Example: Show that key operations are executed within PKCS#11 sessions.

3.4. Inspection to validate Secure Element (SE), Trusted Execution Environment (TEE), Physically Unclonable Functions (PUFs), Secure boot attestation, tamper proof as under:

3.4.1. **Secure Element (SE)**

3.4.1.1. **Test objective:** Validate that the SE securely stores and processes cryptographic keys, and is resistant to physical and logical attacks.

3.4.1.2. **Testing and Validation Steps:**

Category	**Test Activity**	**Description / Tools**
Functional Tests	• API compliance • Key management • Cryptographic operations	• Validate Global Platform or vendor API compliance (APDU command sequences). • Test key generation, import/export,deletion policies, and secure lifecycle transitions. • Verify crypto operations using standard test vectors (NIST CAVP).

Security Tests	• Access control enforcement • Fault injection resilience • Side-channel analysis	• Validate PIN, password, or mutual authentication protection. • Perform voltage/clock glitch and EM fault tests to ensure resistance. • Conduct DPA/SPA tests to measure leakage during crypto operations.
Certification Alignment	• Common Criteria (CC) EAL 5+/FIPS 140-3 or equivalent	• Check against CC Protection Profiles (e.g., PP0084 for SE).

3.4.2. **Trusted Execution Environment (TEE)**

3.4.2.1. **Test objective:** Verify isolation, integrity, and trust chain between REE (Rich Execution Environment) and TEE.

3.4.2.2. **Testing and Validation Steps:**

Category	**Test Activity**	**Description / Tools**
Functional Tests	• TEE Client-TA communication • Trusted App behavior	• Validate TEE Client API and Internal Core API compliance. • Verify secure storage, session management, and cryptographic functions inside TA.
Security Tests	• Memory isolation • Secure world boot & root of trust • Access control	• Confirm TEE memory isolation from REE via MMU configuration testing. • Validate secure boot chain from ROM to TEE OS. • Test privilege escalation and shared memory vulnerabilities.
Certification Alignment	• Global Platform TEE PP	• Validate compliance with TEE Protection Profile.

3.4.3. **Physically Unclonable Functions (PUFs)**

3.4.3.1. **Test objective:** Assess reliability, uniqueness, and tamper-resistance of PUF-derived keys or identifiers.

3.4.3.2. **Testing and Validation Steps:**

Metric	**Description**	**Validation Method**
Uniqueness	Different chips produce distinct responses.	Inter-chip Hamming Distance
Reliability (Stability)	Same chip produces same response under environmental variations.	Measure intra-chip HD under varying voltage, temp, aging.

Entropy and Randomness	Evaluate unpredictability of response bits.	NIST SP 800-22 randomness tests.
Tamper Resistance	PUF response alters irreversibly upon tampering.	Perform invasive probing, EM interference, decapsulation tests.
Reproducibility	Check if error correction mechanisms restore stable key.	Repeated power cycles and statistical validation.

3.4.4. **Secure Boot & Attestation**

3.4.4.1. **Test Objective:** Ensure only authenticated and unmodified firmware is executed and that device attestation is verifiable.

3.4.4.2. **Testing and Validation Steps:**

Category	**Test Activity**	**Description**
Functional Tests	• Boot chain integrity • Firmware rollback prevention	• Validate each stage's digital signature verification (ROM; Bootloader; OS). • Attempt to flash older firmware and check rejection.
Security Tests	• Root of trust validation • Remote attestation	• Verify hash/signature against a known hardware root key. • Simulate verifier–prover exchange; validate attestation certificate and nonce freshness.
Tampering Tests	• Modify bootloader or firmware	• Confirm system refuses to boot untrusted images.
Standard Alignment	• NIST SP 800-193, PSA • Certified or equivalent	• Check alignment with firmware protection and recovery guidelines.

3.4.5. **Tamper-proof & Tamper Detection Mechanisms**

3.4.5.1. **Test objective:** Verify protection against physical attacks and that detection mechanisms respond correctly.

3.4.5.2. **Testing and Validation Steps:**

Type	**Test Description**	**Expected Behavior**
Active Tamper Detection	Simulate voltage, clock, or temperature anomalies.	Device triggers tamper interrupt, erases secrets.
Passive Tamper Resistance	Try to access protected areas via probing, fault injection.	No secret leakage; hardware protection active.

Packaging & Enclosure Tests	Apply mechanical stress, thermal cycling, microprobing.	Security mesh or coating triggers alerts.
Certification Mapping	FIPS 140-3 Level or equivalent.	Validate against tamper-evident and tamper-response.

4. Level 2B - Hardware Assurance - IT/IoT specific testing

4.1. Chip provenance & authenticity – Detect counterfeit or modified chips/PCBs (using X-ray imaging, SEM, and electrical characterization).

4.2. Hardware verification – Ensure declared components based on BOM that implementation matches actual.

4.3. JTAG/UART/SWD interfaces – Test that debug ports are disabled or properly access-controlled in production.

4.4. Wireless stack validation – Test BLE, ZigBee, NB-IoT, LTE/5G interfaces for insecure implementations.

4.5. Protocol fuzzing - Bluetooth, NFC, Wi-Fi fuzzing for memory corruption or DoS.

4.6. Firmware extraction resistance – Try dumping firmware via chip-off or debug interfaces.

4.7. Update mechanism validation – Test Over the Air (OTA) or any other update mechanism for integrity, authenticity, rollback protection.

4.8. Mobile Device Specific testing

4.8.1. Baseband processor testing – Validate isolation between baseband and application processor.

4.8.2. SIM/eSIM/iSIM validation – Test secure provisioning, anti-cloning, and mutual authentication.

4.8.3. App-to-hardware interaction – Test APIs that expose sensors (camera, microphone, GPS) for unauthorized access.

5. Level 2C - Hardware Assurance - Operational Technology (OT) Specific testing

5.1. For Hardware Assurance of Operational Technology (OT), compliance with IEC 62443-3-3 (System Security Requirements) and IEC 62443-4-2 (Component Security Requirements) shall be mandatory which defines authentication, integrity, confidentiality, and availability requirements applicable to OT systems and embedded hardware. Compliance with post-quantum readiness requirements under IEC 62443 shall be demonstrated through documented crypto-agility analysis, PQC compatibility testing, and operational impact evaluation, ensuring that cryptographic transitions do not compromise OT safety, availability, or deterministic behavior.

5.2. Counterfeit detection: Inspect PLCs, controllers, and IEDs for counterfeit chips or boards.

5.3. Hardware Bill of Materials (HBOM): Verify actual components against vendor-declared HBOM.

5.4. Firmware provenance: Ensure PLC/RTU firmware matches vendor signing and hasn't been modified in transit.

5.5. Debug port lockdown – JTAG/SWD/UART interfaces must be disabled or authenticated.

5.6. Fieldbus / Industrial Ethernet: Validate integrity & authenticity of Modbus, DNP3, Profibus, OPC-UA, IEC 61850 as applicable.

5.7. Secure gateways– Test hardware firewalls/data gateways between OT and IT.

5.8. Protocol fuzzing – For industrial hardware interfaces (serial,CAN, HART, Ethernet/IP).

5.9. Encryption enforcement – Check if hardware supports TLS/DTLS/IPsec for telemetry between PLC/RTU and SCADA. Insecure protocols shall be disabled by default.

5.10. Rollback prevention – Test against downgrade attacks to reintroduce vulnerable versions.

5.11. Update path security – Verify OTA / local update process (USB, serial) is authenticated.

6. Enterprise Grade Assurance– Level 3

6.1. Verify Quantum/True RNG (QRNG/TRNG) integration using TEC GRs or equivalent standards (List of globally available Standards for Quantum Technologies mentioned in **Annexure-V**).

6.1.1. The QRNG/TRNG shall mandatorily undergo validation of its claimed physical entropy source (quantum, optical, or other physical mechanisms) to demonstrate that the entropy source is genuine, operational, and continuously active.

6.1.2. Physical mechanisms (including Quantum) can be checked through auditable scientific documentation of the physical mechanism, hardware Bill of Materials (HBOM) verification for entropy source components, calibrated test evidence demonstrating entropy generation, and continuous health monitoring of the entropy source or through test circuitries in future as and when it is available.

6.1.3. The QRNG/TRNG shall further demonstrate that the entropy source cannot be spoofed, substituted, or disabled without detection, and calibration certificates for the entropy source shall be provided as part of the validation evidence.

6.1.4. The product shall ensure non-repudiation, integrity, and non-repetition of quantum-sourced seed material used for cryptographic operations across sessions, restarts, and lifecycle events.

6.2. **Advanced performance monitoring**

6.2.1. Verify Hardware acceleration with Memory Usage (Heap / Stack) and Code Size / Binary Footprint for all algorithms and implementations.

6.2.2. Run encapsulation/decapsulation cycles and signature generation and verification for supported PQC algorithms and record CPU/GPU usage via perf or embedded monitor etc.

6.2.3. Measure power consumption (using power meter or on-board PMIC logs) during idle, average, and peak PQC workloads and compute energy per cryptographic operation.

6.2.4. Simulate multiple concurrent PQC sessions (e.g., 100, 500, 1000 parallel TLS handshakes) with mixed workload of PQC and classical to validate scalability.

6.2.5. Capture packet traces (e.g., Wireshark) to measure data size increase for key exchange and signatures and verify link utilization and QoS under heavy encryption traffic.

6.2.6. As increased security may degrade performance, sectors may determine the required performance benchmarks based on their specific requirements and prevailing market forces.

6.3. **Crypto-agility**

6.3.1. Ask the vendor to toggle between different hybrid implementations via Command Line Interface (CLI), GUI or API. Check for negligible downtime or connection reset values defined as per engineering and SLA requirements that need to be justified via risk assessment and safety analysis. For e.g., - Typical engineering values observed in industrial practice include transient disruptions below 100 ms for time-sensitive OT functions and below 1 s for non-real-time control or management functions, with minimal session loss (e.g., ≤1 session). These values are derived from IEC 61850, IEC 61784, NIST SP 800-82, and utility operational practices.

6.3.2. Validate fallback to classical key exchange when PQC module disabled or overloaded. Check for seamless transition with no data loss.

6.3.3. Ask for crypto-switching roadmap. Example: Vendor provides support lifecycle timelines for future PQC algorithm integration. Test integration with firmware updates enabling new PQC algorithms.

6.3.4. The system shall support seamless rollback to a previously validated cryptographic configuration and shall allow controlled switching between classical, hybrid, and PQC cryptographic implementations without requiring system reboot or service disruption.

6.3.5. Review crypto-upgrade policy. Example: Switching to alternate PQC/hybrid algorithm after vulnerability disclosure if it is not patched.

6.4. Verify protocol-level security through advanced attack simulations (fault injection, multi-vector).

6.5. Check for automated vulnerability discovery & formal security analysis comprehensive report.

6.6. Ask for Security Audit/assessment reports.

6.7. Validation that final encryption keys are derived using a secure Key Derivation Function (KDF) that cryptographically combines all high-assurance entropy sources, including PQC key exchange outputs, quantum seed material, and QKD-derived keys where applicable, shall be done.

6.8. The product shall support secure, validated integration with centralized enterprise cryptographic management systems for inventory tracking, status reporting, and crypto-agility monitoring. Validation shall demonstrate secure communication channels, authenticated and authorized management interfaces, and accurate reporting of cryptographic algorithm status, versions, and health metrics. Supported management protocols (e.g., SNMP, REST APIs) shall be documented and tested to ensure confidentiality, integrity, and controlled access to management functions.

6.9. Check for CI/CD integration and for automated regression validation through:

6.9.1. Incorporate tests into continuous integration pipelines for regression testing.

6.9.2. The CI/CD pipeline shall automatically trigger regression validation upon code changes, configuration updates, cryptographic algorithm modifications (including PQC or hybrid crypto-transitions), and dependency upgrades with minimum two peer code reviews.

6.9.3. Automated regression testing shall include unit tests, integration tests, security tests (e.g., static analysis, dependency scanning, fuzzing where applicable), and protocol interoperability tests relevant to the target environment.

6.9.4. The pipeline shall enforce prevention of promotion of builds that fail defined quality, security, or compliance criteria.

6.9.5. Test results, coverage metrics, and security findings shall be recorded, traceable to build artifacts, and retained for audit and rollback purposes.

6.9.6. The CI/CD process shall support repeatable builds, versioned artifacts, and automated rollback to previously validated releases in case of regression or operational impact.

6.9.7. Target multiple platforms (Linux, Windows, ARM-based embedded).

6.9.8. Tools: GitHub Actions, GitLab CI, Jenkins with Docker-based test runners etc.

6.10. The supply chain security shall be ascertained for hardware, firmware, software, and critical components.

6.11. Sector specific compliances and cryptographic policies may be added by sectors like banks, energy sector, telecom etc. as notified by their regulators from time to time.

7. Critical Infrastructure Security – Level 4

7.1. Verify customized/indigenous algorithms/implementation as per approach mentioned in Annexure-II as per sector requirements.

7.2. The product shall demonstrate validated strategic resilience by supporting rapid cryptographic diversification and pivoting capabilities in response to algorithm compromise scenarios as under:

7.2.1. Validation shall confirm the ability to transition to QKD or alternative PQC algorithms (including indigenous or non-standardised schemes) within a defined maximum transition time, without loss of security.

7.2.2. Pre-configured fallback algorithms, documented transition procedures, and simulated compromise testing shall be used to verify secure operation throughout the transition process.

7.2.3. Exclusive reliance on any single PQC standardisation shall be discouraged. Strategic resilience shall include support for algorithm diversification, indigenous cryptographic schemes (where validated), hybrid models, and alternate trust anchors to mitigate systemic risk.

7.3. Verify QKD integration readiness through TEC GRs on QKD or equivalent standards as per sector requirements.

7.4. The product shall be explicitly tested for secure behavior under cryptographic and system failure conditions, including QKD link failures, PQC decapsulation errors, hardware faults, and network partitions. Validation shall confirm that the system never fails open, and instead either terminates sessions securely or reverts to a verified secure hybrid state. High-severity alerts, fail-secure policy enforcement, and comprehensive failure documentation shall be mandatory components of this validation.

7.5. Verify disaster recovery plan with Business Continuity and multi-site resilience.

7.5.1. The product shall demonstrate a validated Disaster Recovery and Business Continuity capability ensuring continued secure operation under site-level, infrastructure-level, or catastrophic failure scenarios.

7.5.2. The product shall support multi-site deployment with logical and cryptographic state consistency, including secure replication of configuration, cryptographic material metadata (excluding private keys where prohibited), and operational policies.

7.5.3. Validation shall confirm defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) thresholds, controlled failover and failback procedures, and maintenance of cryptographic assurance during transitions.

7.5.4. Disaster recovery testing shall include simulated site failures, loss of connectivity, and partial service degradation, verifying that the system maintains availability, integrity, and security controls without data loss, key compromise, or fail-open behavior.

7.6. Verify Zero Trust Architecture Compliance. The product shall comply with Zero Trust Architecture principles, enforcing continuous verification of identity, device integrity, and authorization for all users, services, and system components.

7.7. The product shall undergo independent red team testing to simulate real-world adversarial attacks against system, network, and operational security controls. Red team exercises shall assess the effectiveness of preventive, detective, and response mechanisms, including resistance to advanced persistent threats, lateral movement, privilege escalation, and exploitation of misconfigurations. Findings shall be documented, risk-rated, remediated, and revalidated.

7.8. The product shall support rigorous supply chain security verification covering hardware, firmware, software, and critical components. This shall include verification of component provenance, integrity checks, semiconductor level assurance and trusted build processes. Controls shall be in place to detect unauthorized modifications and compromised components prior to deployment.

7.9. The product shall be evaluated against simulated nation-state-level threat scenarios, including advanced persistent attacks, supply chain compromise, cryptographic exploitation, and long-term stealthy intrusion techniques. The assessment shall consider attacker capabilities aligned with high-end threat models and evaluate the product's ability to prevent, detect, contain, and recover from such attacks.

7.10. Critical security-relevant components (e.g., cryptographic modules, secure boot, key management logic, access control enforcement) shall be subject to semi-formal verification to demonstrate correctness, absence of specified classes of vulnerabilities, and compliance with security requirements. Verification scope, assumptions, and limitations shall be documented.

7.11. Additional requirements may be added by Strategic sectors – not part of this framework.

Annexure-II

Testing and Validation of Customized/Indigenous implementations of Quantum-Safe PQC Algorithms

Sr.No.	Stage	Objective	Activities / Tests
1	Specification & Design Review	Verify correctness, completeness, and clarity of algorithm design	• Review cryptographic design documents • Verify security proofs • Assess parameter selection rationale • Threat model definition
2	Reference Implementation Development	Establish a clean, standard implementation for testing	• Implement algorithm as per specs • Conduct code walkthroughs • Ensure constant-time design (if required)
3	Functional Correctness Testing	Verify correctness of encryption/decryption, keygen, signature, verification	• Known Answer Tests (KATs)-Monte Carlo / randomized tests-Round trip functional tests
4	Interoperability Testing	Ensure algorithm works across platforms and languages	• Test cross-language/cross-platform compatibility-Validate standard I/O formats (ASN.1, JSON, etc.) • Perform end-to-end integration
5	Security Assurance Testing	Evaluate security strength against classical and quantum attacks	• Side-channel resistance testing • Fault-injection resilience • Known cryptanalytic attacks simulation • Security level estimation
6	Performance & Resource Profiling	Assess efficiency and feasibility for deployment	• Measure runtime, memory footprint, code size • Benchmark keygen, sign, verify, encaps, decaps ops-Scalability on constrained/embedded systems
7	Key Lifecycle Management	Ensure key lifecycle starting from creation to deletion	• Key generation, distribution, storage and deletion procedures • Supply-chain assurance

**Note –*

1. *Customized algorithm may require mathematical validation by cryptographers' community.*
2. *Testing to be done as per assurance level mentioned by vendor and as per user requirements.*
3. *The above requirements are advisory and may require extensive documentation separately as per sector requirements.*

Annexure-III

List of Test labs in the country in security domain

Sr. No.	Name of Lab with address	Available test facilities as per below categories					
		Cryptographic evaluation (PQC or primitive), RNG Verification	**Interoperability testing (RFC conformance, cross library and cross platform testing)**	**Software testing (vulnerability analysis, VA/PT, Fuzz/negative testing, Memory analysis)**	**Hardware security (Side channel resistance testing, hardware root if trust verification)**	**Performance analysis (Encryption/ Encapsulation time, decryption/ encapsulation time, signature generation/ verification time, throughput**	**Enterprise grade resilience verification (CI/CD, crypto agility verification,**
1	SETS Chennai				Yes Power Analysis , EM Analysis for both classical crypto-systems and Post-Quantum systems		
2	BIS WRL, Mumbai PLOT NO. E9, ROAD NO. 8, M.I.D.C, ANDHERI (EAST), Mumbai, Maharashtra - 400093	Partial: Basic cryptographic module conformance, IS 13252 hardware component checks	Partial: Network and hardware component interoperability (EMI/EMC networks)	Partial: Compliance testing for consumer electronics	Partial: EMI/EMC, electrical safety, not full side channel	Yes: Throughput, reliability for IT/IoT, hardware	NA

3	BIS NRL, Mohali B-69, Industrial Focal Point, Phase VII, Mohali, Punjab - 160059	Partial: Cybersecurity module tests, embedded hardware	Yes: Interoperability in embedded and networked devices	Yes: VA/PT, fuzz, device-level compliance	Partial: Hardware root checks, EMI/EMC, limited side-channel	Yes: Performance, throughput of IT/electronics	NA
4	BIS Central Lab, Ghaziabad 20/9, Site 4, Sahibabad Industrial Area, Ghaziabad, UP 201010	Yes: Module conformance, cryptographic hardware checks, basic RNG	Partial: Hardware interface, some telecom interoperability	Yes: Compliance, device vulnerability analysis	Partial: Security evaluation for hardware platforms, basic side channel	Yes: Hardware/ software throughput	NA
5	Criterion Network Labs, Bengaluru #2, 2nd Floor, Post Office Road, Basavanagudi, Bengaluru, Karnataka 560004	Yes: Cryptographic stack evaluation for cyber/network products	Yes: Cross-platform and protocol interoperability, IPv6, networked security	Yes: Vulnerability analysis, fuzz, negative, memory	Partial: Physical device root checks, some side-channel simulation	Yes: Performance benchmarks on security devices	Partial: Crypto-stack update simulation, basic CI/CD audits
6	GRL India, Hyderabad Pavani Windsor, 20, Jubilee Enclave, HITEC City, Hyderabad, Telangana 500081	Partial: Security stack validation, embedded RNG	Yes: Cybersecurity of CCTV/network products, protocol interoperability	Yes: Vulnerability/fuzzing for embedded/ networked IT	NA	Partial: Protocol throughput, device-level speed evaluation	Partial: Embedded software resilience, update simulation
7	Shriram Institute, Delhi 19, University Road, Delhi 110007	Partial: Cryptographic primitive testing, basic RNG evaluation for hardware	NA	Yes: Software QA, vulnerability, memory analysis	Yes: Hardware security evaluation, root verification	Partial: Hardware performance, electronics	NA

8	Testtex India Labs, Noida C-39, Sector-2, Noida, UP 201301	NA	NA	Yes: VA/PT, fuzz, memory for IT software	NA	NA	NA
9	Conformity Testing Labs, Agra 101, Industrial Estate, Sadar Bazar, Agra, UP 282010	Partial: Hardware crypto evaluation, basic side channel	NA	Partial: Device integrity, partial security tests	Yes: Hardware root verification, physical side channel	NA	NA
10	TUV Rheinland India, Kanchipuram 82/A, Kadevu Industri al Estate, Kanchipu-ram, Tamil Nadu 600301	NA	Partial: Protocol and functional electronic interoperab-ility	Partial: Electronics VA/PT, basic fuzz	Partial: Hardware component root, environme-ntal tests	Partial: Device-level throughput and reliability	NA
11	National Test House, Kolkata/Alipore	NA	Partial: Protocol functional assurance	Yes: Device software compliance and security	Yes: Component root, side-channel analysis	Partial: Reliability and throughput	NA
12	Spectro Analytical Labs, Delhi E-41, Okhla Industrial Area, Phase-II, Delhi - 110020	Partial: Basic cryptograp-hic primitive, device module checks	NA	Yes: Software QA, fuzz, VA/PT	Partial: Electronic component root, limited side channel	Partial: Basic throughput, performan-ce	NA

13	STQC IT Centre, New Delhi Electronics Niketan, CGO Complex, Lodhi Road, New Delhi – 110003	Partial – Classical crypto, RNG; PQC via TEC/BIS test cases	Partial – TLS, IPsec protocol conformance	Complete – VA/PT, memory analysis	NA	Partial – Latency, throughput	NA
14	STQC IT Centre, Bengaluru 2nd Floor, KSTDC Building, Yeshwanthpur TTMC, Bengaluru – 560022	Partial	Partial	Complete	NA	Partial	NA
15	ETDC Delhi (under STQC) Okhla Industrial Area, Phase II, New Delhi – 110020	Partial – Classical crypto	Partial – RFC conformance (IPsec, TLS)	Complete	NA	Partial	NA
16	NCCS Bengaluru City Telephone Exchange, Sampangirama Nagar, Bengaluru – 560027	Partial – Telecom crypto-stack	Complete – Telecom protocol stack (IPsec, TLS)	Complete – VA/PT for telecom	Complete – EM leakage, DPA	Partial – Telecom benchmarking	Partial – Crypto-agility for telecom
17	CDAC Pune Innovation Park, Panchavati, Pashan, Pune – 411008	Partial – PQC R&D, RNG validation	Partial – OpenSSL/liboqs, hybrid protocol testing	Complete – Fuzz, VA/PT	NA	Complete – SUPERCOP, OpenSSL speed	Partial – CI/CD in R&D

18	CDAC Hyderabad IIIT Campus, Gachibow-li, Hyderabad – 500032	Partial	Partial	Complete	NA	Partial	Partial
19	Bharat Test House Pvt. Ltd. (BTHPL) Plot No. 77, Udyog Vihar, Phase IV, Gurugram, Haryana – 122015	Partial – Classical crypto, RNG	NA	Partial – VA/PT for IT/IoT	NA	Partial – Basic metrics	NA
20	UL India Pvt. Ltd. 82 EPIP Zone, Whitefield, Bangalore – 560066	Complete – Crypto module testing	NA	Partial – Embedded VA/PT	Complete – Tamper resistance, root of trust	Partial – Power profiling	NA
21	TÜV Rheinland India Pvt. Ltd. Plot No. 32, 2nd Phase, Peenya Industri-al Area, Bengaluru – 560058	Complete – Crypto module testing	NA	Partial – Hardware VA/PT	Complete – Side-channel resistance (DPA, EM)	Partial – Benchmark-ing	NA
22	Software testing – STQC labs IT Centre Kolkata	NA	NA	eSecurity Testing (Vulnerabili-ty Assessment, Penetration Testing), ISMS Audit, Security assessmen-ts	NA	NA	NA

23	Software testing – STQC labs IT Centre Hyderabad	NA	NA	eSecurity Testing (Vulnerability Assessment, Penetration Testing), ISMS Audit, Security assessments	NA	NA	NA
24	Software testing – STQC labs IT Centre Chennai	NA	NA	eSecurity Testing (Vulnerability Assessment, Penetration Testing), ISMS Audit, Security assessments	NA	NA	NA
25	Software testing – STQC labs IT Centre Pune	NA	NA	eSecurity Testing (Vulnerabil-ity Assessment, Penetration Testing), ISMS Audit, Security assessments	NA	NA	NA
26	Software testing – STQC labs IT Centre Mumbai	NA	NA	eSecurity Testing (Vulnerability Assessment, Penetration Testing), ISMS Audit, Security assessments	NA	NA	NA
27	Software testing – STQC labs IT Centre Agartala	NA	NA	eSecurity Testing (Vulnerability Assessment, Penetration Testing), ISMS Audit, Security assessments	NA	NA	NA

28	Software testing – STQC labs IT Centre Jaipur	NA	NA	eSecurity Testing (Vulnerability Assessment, Penetration Testing), ISMS Audit, Security assessments	NA	NA	NA
29	Software testing – STQC labs IT Centre Guwahati	NA	NA	eSecurity Testing (Vulnerability Assessment, Penetration Testing), ISMS Audit, Security assessments	NA	NA	NA
30	Software testing – STQC labs IT Centre Mohali	NA	NA	eSecurity Testing (Vulnerability Assessment, Penetration Testing), ISMS Audit, Security assessments	NA	NA	NA
31	Software testing – STQC labs IT Centre Thiruv-ananthap-uram	NA	NA	eSecurity Testing (Vulnerability Assessment, Penetration Testing), ISMS Audit, Security assessments	NA	NA	NA
32	Software testing – STQC labs IT Centre Ajmer	NA	NA	eSecurity Testing (Vulnerability Assessment, Penetration Testing), ISMS Audit, Security assessments	NA	NA	NA

33	Software testing – STQC labs IT Centre Goa	NA	NA	eSecurity Testing (Vulnerability Assessment, Penetration Testing), ISMS Audit, Security assessments	NA	NA	NA
34	Software testing – STQC labs IT Centre Solan	NA	NA	eSecurity Testing (Vulnerability Assessment, Penetration Testing), ISMS Audit, Security assessments	NA	NA	NA
35	Software testing – STQC labs IIQM Jaipur	NA	NA	eSecurity Testing (Vulnerability Assessment, Penetration Testing), ISMS Audit, Security assessments	NA	NA	NA
36	Software testing – STQC labs CFR Chennai	NA	NA	eSecurity Testing (Vulnerability Assessment, Penetration Testing), ISMS Audit, Security assessments	NA	NA	NA
37	ITSAR testing - NCCS labs ACUCERT LABS LLP	NA	NA	Wi-Fi CPEs, IP Router	NA	NA	NA

38	ITSAR testing - NCCS labs DELTAPHI LABS PRIVATE LIMITED	NA	NA	OLT – PON broadband, Wi-Fi CPEs, ONT - PON broadband, IP Router	NA	NA	NA
39	ITSAR testing - NCCS labs Matrix Shell Technologies Pvt Ltd	NA	NA	IP Router, Session Management Function (SMF) of 5G	NA	NA	NA
40	ITSAR testing - NCCS labs Nemko India (Test Lab) Pvt Ltd	NA	NA	IP Router, Wi-Fi CPEs, Group-V Devices	NA	NA	NA
41	ITSAR testing - NCCS labs Compliance International Pvt Ltd	NA	NA	IP Router	NA	NA	NA
42	Hardware test labs Secure Embedded and Smart Things Laboratory (SETTLOR), IIT Kanpur	NA	NA		Research includes Far-Field Side Channel Analysis of Mixed Signal Chips, Acoustic Side Channel Attacks, etc.		

43	Hardware test labs C. R. Rao Advanced Institute of Mathematics, Statistics and CS (AIMSCS), University of Hyderabad	NA	NA		Side Channel Analysis Lab		
44	TEC LABS AA Electro Magnetic Test Laboratory Pvt. Ltd. Gurugram	NA	Partial: Protocol functional assurance	NA	NA	NA	NA
45	TEC LABS Compliance International Telecom Laboratories Delhi	NA	Partial: Protocol functional assurance	NA	NA	NA	NA
46	TEC LABS SIM TESTING FACILITY LABORATORY, IDEMIA SYSCOM INDIA	NA	Partial: Protocol functional assurance	NA	NA	NA	NA
47	TEC LABS Envitest Laboratories Private Limited, Bangalore	NA	Partial: Protocol functional assurance	NA	NA	NA	NA

48	TEC LABS M/s DELTAPHI LABS PRIVATE LIMITED, Mumbai	NA	Partial: Protocol functional assurance	NA	NA	NA	NA
49	IITM CDoT Samgnya Technolog-ies Foundati-on (upcoming)	RNG Verification	-	-	-	Performan-ce Validation	-
50	CSIR - NPL	QRNG entropy validation			Side-channel leakage characteriz-ation, electromag-netic emission measureme-nts, power analysis		

**Note –*

1. *The test facilities mentioned above may not be specifically available w.r.t. PQC but generic in nature w.r.t test areas like Vulnerability testing, Hardware testing, performance analysis etc.*
2. *The above list has been provided by BIS and STQC and also fetched from website of NCCS (https://nccs.gov.in/home/labs), TEC (https://www.tec.gov.in/Labs-Designated-by-TEC), STQC (https://www.stqc.gov.in/labs-centres) .*
3. *Above list will provide the status of available test labs/infra which can be upgraded to take care of PQC products in future.*

Annexure-IV

List of Cryptographic Algorithms

This section categorizes the cryptographic algorithms considered in PQC validation framework. It includes both quantum-resistant asymmetric algorithms and quantum-safe symmetric primitives, as both are essential for constructing secure, end-to-end cryptographic protocols in the post-quantum era. **Below is the list of such algorithms which would be updated from time to time on basis of new PQC algorithms developed globally as well as indigenous algorithms/implementations.**

Asymmetric PQC Algorithms

These algorithms provide quantum-resistant alternatives for public-key encryption, key encapsulation mechanisms (KEMs), and digital signatures. They are based on mathematical problems believed to be hard even for quantum computers.

- **Lattice-Based Cryptography:**
  - **ML-KEM** – Key Encapsulation Mechanism (KEM) based on Module Learning With Errors (MLWE). Selected for standardisation by NIST (ML-KEM).
  - **Dilithium** – Digital Signature Scheme based on Module Learning With Errors and Module Short Integer Solution (MLWE/ML-SIS). Standardised as ML-DSA.
  - **Falcon** – Compact Digital Signature Scheme using NTRU lattices.
- **Hash-Based Cryptography:**
  - **SPHINCS+** – Stateless hash-based digital signature scheme leveraging Merkle trees. Based solely on the security of cryptographic hash functions.
- **Code-Based Cryptography:**
  - **HQC** - Hamming Quasi-Cyclic Key Encapsulation Mechanism (KEM) for secure key exchange resistant to quantum attacks

Symmetric and Hash-Based Algorithms

While symmetric and hash functions are less affected by quantum computing (due to Grover's algorithm's quadratic speedup), achieving quantum security still requires stronger parameters such as longer keys or output lengths. These symmetric primitives form the backbone of encryption, hashing, authentication, and hybrid protocol construction.

- Symmetric Encryption:
  - **AES-256** – The Advanced Encryption Standard with a 256-bit key. It remains quantum-resistant against Grover-style attacks, requiring 2^128 operations for brute-force. AES-192 may also be used for lightweight cryptographic implementation like IoT devices.
- Secure Hash Algorithms:
  - **SHA-2 Family:**
    - **SHA-256, SHA-512** – Widely used hash functions for digital signatures, message digests, and HMAC.

o **SHA-3 Family:**

- **SHA3-256** – A drop-in replacement for SHA-2, based on the Keccak sponge construction.
- **SHAKE128 / SHAKE256** – Extendable-output functions (XOFs), useful for hashing, pseudorandom number generation, and KMAC.

- Message Authentication Codes (MACs):

  o **HMAC (SHA-2/ SHA-3 variants)** – Hash-based MACs used for message integrity and authentication.

  o **KMAC128 / KMAC256** – Keccak-based MACs defined in NIST SP 800-185, designed for environments adopting SHA-3.

- Authenticated Encryption (AE & AEAD):

  o AE combines encryption and authentication in a single pass, ensuring both confidentiality and message integrity.

  - AES-GCM, AES-CTR+HMAC, ChaCha20-Poly1305.

Annexure-V

List of globally available Standards for Quantum Technologies

Standards	Scope
TEC Standards and test guides(5)	
TEC 91000:2022	Standard for Generic Requirements on Quantum Key Distribution System
TEC 91010:2023	Standard for Generic Requirements on Quantum-Safe and Classical Cryptographic Systems
TEC 91020:2024	Standard for Generic Requirements on Quantum Random Number Generator
TEC 91001:2023	Test Guide on Quantum Key Distribution System
TEC 91021:2025	Test Guide on Quantum Random Number Generator
NIST FIPS Standards (7)	
FIPS 140-3	Cryptographic Module Security Requirements
FIPS 186-5	Digital Signature Standard
FIPS 197	Advanced Encryption Standard (AES)
FIPS 198-1	HMAC (Hash-Based Message Authentication Code)
FIPS 203	ML-KEM (Kyber) – Post-Quantum Public Key Encryption and Key Establishment
FIPS 204	ML-DSA (Dilithium) – Post-Quantum Digital Signature Algorithm
FIPS 205	SLH-DSA (SPHINCS+) – Stateless Hash-Based Signature Scheme
FIPS 206	FALCON

ITU Standards (7)	
ITU-T Y.3800	Overview of QKD networks
ITU-T Y.3801–Y.3804	QKD network architecture, management, and control mechanisms
ITU-T X.1701–X.1702	Security framework for QKD systems
ETSI QKD Standards (12)	
ETSI GS QKD series (002–018)	Covers use cases, interfaces, key management, security proofs, terminology, module specs, and orchestration for QKD systems
ISO/IEC Standards (4)	
ISO/IEC 23837 series	Security techniques for QKD
ISO/IEC 15408	Common Criteria for Information Technology Security Evaluation
ISO/IEC 19790	Requirements for cryptographic modules
ISO/IEC 27001 / 27002 / 27005	Information security management standards, including risk and control measures
OASIS (1)	
PKCS #11 v3.1	Cryptographic Token Interface Base Specification. July 2023

Annexure-VI

Sample Certificate Template

Government of India
Certification Authority/Certification Body
Certification of Validation

(For PQC-based Quantum-Safe Products and Solutions)

This is to certify that the product / solution described below has been evaluated and found compliant with the applicable Post-Quantum Cryptography (PQC) testing framework as per the standards and procedures laid down by the Certification Authority/Certification Body and relevant national and international specifications.

Product / Solution Details:

Product / Solution Name and Brief Description	
Version / Model	
Manufacturer / OEM	
Test Laboratory	
Test Values observed	Performance parameters Vulnerabilities found PQC/Classical Algorithms supported Interfaces supported
Validator information	
QR Code	
Test environment (with limitation and restrictions)	
Applicable Standards / References	
Certificate ID / Reference No.	

Date of Issue:

Validity:

This certification signifies compliance of the above-mentioned product/solution with framework for Testing and Certification of PQC based Quantum-Safe Products and Solutions. Continued validity is subject to surveillance audits or re-certification as per Certification Authority/Certification Body policy.

The BOM of the product (including Cryptographic Bill of Materials, libraries used) is attached.

Authorized Signatories:

(Signature) Head – Certification Authority/Certification Body	(Signature) Authorized Officer – PQC/QKD Lab

Related Documents

1. Telecommunication Engineering Centre (TEC). TEC 91000:2022 – Standard for Generic Requirements on Quantum Key Distribution System.
2. Telecommunication Engineering Centre (TEC). TEC 91010:2023 – Standard for Generic Requirements on Quantum Safe and Classical Cryptographic Systems.
3. Telecommunication Engineering Centre (TEC). TEC 91020:2024 – Standard for Generic Requirements on Quantum Random Number Generator.
4. Telecommunication Engineering Centre (TEC). TEC 91001:2023 – Test Guide on Quantum Key Distribution System.
5. Telecommunication Engineering Centre (TEC). TEC 91021:2025 – Test Guide on Quantum Random Number Generator.
6. National Bureau of Standards (NBS). Data Encryption Standard (DES). FIPS PUB 46. U.S. Department of Commerce, January 1977.
7. National Bureau of Standards (NBS). DES Modes of Operation. FIPS PUB 81. U.S. Department of Commerce, December 1980.
8. National Institute of Standards and Technology (NIST). FIPS 113 – Computer Data Authentication. May 1985.
9. National Institute of Standards and Technology (NIST). FIPS 180 – Secure Hash Standard (SHS). May 1993. (Revisions: FIPS 180-1, 180-2, 180-4).
10. National Institute of Standards and Technology (NIST).FIPS 186-5 – Digital Signature Standard (DSS). February 2023.
11. National Institute of Standards and Technology (NIST). FIPS 197 – Advanced Encryption Standard (AES). November 2001 (Updated May 2023). DOI https://doi.org/10.6028/NIST.FIPS.197-upd1
12. National Institute of Standards and Technology (NIST).FIPS 198-1 – The Keyed-Hash Message Authentication Code (HMAC). July 2008.
13. National Institute of Standards and Technology (NIST). FIPS 202 – SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. August 2015.
14. National Institute of Standards and Technology (NIST).FIPS 203 – ML-KEM (Kyber): Post-Quantum Key Encapsulation Mechanism. August 2024.
15. National Institute of Standards and Technology (NIST). FIPS 204 – ML-DSA (Dilithium): Post-Quantum Digital Signature Algorithm. August 2024.
16. National Institute of Standards and Technology (NIST). FIPS 205 – SLH-DSA (SPHINCS+): Stateless Hash-Based Digital Signature Scheme. August 2024.
17. National Institute of Standards and Technology (NIST).FIPS 206 – FALCON: Lattice-based Digital Signature Algorithm. 2025 (anticipated release).
18. National Institute of Standards and Technology (NIST).FIPS 140-3 – Security Requirements for Cryptographic Modules. 2019 (CMVP Program).
19. National Institute of Standards and Technology (NIST). SP 800-140 Series (A–D) – Derived Test Requirements for FIPS 140-3 Cryptographic Modules.

20. National Institute of Standards and Technology (NIST). SP 800-38A – Recommendation for Block Cipher Modes of Operation. December 2001.
21. National Institute of Standards and Technology (NIST). SP 800-38B – Recommendation for Block Cipher Modes: CMAC for Authentication. May 2005.
22. National Institute of Standards and Technology (NIST). SP 800-38C/D/E– Recommendations for CCM, GCM/GMAC, and XTS-AES Modes.
23. National Institute of Standards and Technology (NIST). SP 800-56A – Recommendation for Pair-Wise Key Establishment Schemes. (Rev. 2018).
24. National Institute of Standards and Technology (NIST). SP 800-56C Rev. 2 – Recommendation for Key-Derivation Using Pseudorandom Functions. 2018.
25. National Institute of Standards and Technology (NIST). SP 800-57 (Parts 1–3) – Recommendation for Key Management.
26. National Institute of Standards and Technology (NIST). SP 800-90A/B/C – Recommendations for Random Bit Generation and Entropy Sources. (Rev. 1 – June 2015).
27. National Institute of Standards and Technology (NIST). SP 800-133 Rev. 2 – Recommendation for Cryptographic Key Generation. April 2022.
28. National Institute of Standards and Technology (NIST). SP 800-175A/B – Guidelines for Using and Managing Cryptographic Standards. 2020.
29. National Institute of Standards and Technology (NIST).SP 800-185 – SHA-3 Derived Functions (cSHAKE, KMAC, TupleHash, ParallelHash). 2016.
30. National Institute of Standards and Technology (NIST). SP 800-208 – Recommendation for Stateful Hash-Based Signature Schemes (XMSS, LMS). 2020.
31. National Institute of Standards and Technology (NIST). SP 800-232 – Ascon-Based Lightweight Cryptography Standards for Constrained Environments. 2025.
32. International Telecommunication Union (ITU-T). Y.3800 (10/2019) – Overview of Quantum Key Distribution Networks.
33. ITU-T. Y.3801–Y.3804 (2020–2022) – QKD Network Architecture, Control and Management Mechanisms.
34. ITU-T. X.1701(2023) – Security Framework for Quantum Key Distribution Systems.
35. ITU-T. X.1702 (2024) – Guidelines for Evaluation and Testing of QKD Components.
36. ITU-T. X.1710(2025) – Security Requirements for Quantum-Safe Communication Networks.
37. ITU-T. Y.3810 (2025) – Integration of Quantum Key Distribution with Classical Networks.
38. ITU-T. X.509 (latest revision) – Public-Key and Attribute Certificate Frameworks.
39. European Telecommunications Standards Institute (ETSI). ETSI GS QKD 002–018 Series – Quantum Key Distribution (QKD) Specifications (Including use cases, key management, interfaces and security requirements).
40. International Organization for Standardization (ISO/IEC). ISO/IEC 23837 Series – Security Techniques for Quantum Key Distribution.
41. International Organization for Standardization (ISO/IEC). ISO/IEC 15408 (Common Criteria) – Information Technology Security Evaluation.
42. International Organization for Standardization (ISO/IEC). ISO/IEC 19790:2012 – Security Requirements for Cryptographic Modules.

43. International Organization for Standardization (ISO/IEC). ISO/IEC 18033 Series – Encryption Algorithms.
44. International Organization for Standardization (ISO/IEC). ISO/IEC 27001 / 27002 / 27005 – Information Security Management Systems (ISMS): Requirements, Controls and Risk Management.
45. Organization for the Advancement of Structured Information Standards (OASIS). PKCS #11 v3.1 – Cryptographic Token Interface Base Specification. July 2023
46. American National Standards Institute (ANSI). X9.62 – Elliptic Curve Digital Signature Algorithm (ECDSA). 1998.
47. American National Standards Institute (ANSI). X9.31 – RSA Signature Algorithm. 1998.
48. American National Standards Institute (ANSI). X9.63 – Key Agreement and Key Transport Using Elliptic Curve Cryptography. 2001.
49. RSA Laboratories. PKCS #1 v2.2 –RSA Cryptography Standard. October 2012.
50. Krawczyk, H.; Bellare, M.; Canetti, R. HMAC: Keyed-Hashing for Message Authentication. RFC 2104. February 1997.
51. Dierks, T.; Allen, C. The TLS Protocol Version1.0 (and updates through RFC 8446 – TLS 1.3).
52. Kent, S.; Seo, K. Security Architecture for the Internet Protocol (IPsec). RFC 4301, December 2005.
53. RFC 4302 – IP Authentication Header (AH), December 2005.
54. RFC 4303 – IP Encapsulating Security Payload (ESP), December 2005.
55. RFC 7296 – Internet Key Exchange Protocol Version 2 (IKEv2),October 2014.

विज्ञान एवं प्रौद्योगिकी विभाग
DEPARTMENT OF
SCIENCE & TECHNOLOGY

National Quantum Mission

Annexure C

Strategic Roadmap for Quantum-Safe Migration Timelines

Introduction

This document is the first in a planned series of ***Strategic Roadmap for Quantum-Safe Migration*** *under the National Quantum Mission, DST, India. It establishes the overall direction, timelines, and recommended activities for enterprises to build Quantum Resiliency. Subsequent documents in this series will provide detailed guidance on specific areas such as crypto-agility, Quantum Risk Assessment, Prioritisation, Pathways for Implementation. Together, these documents are intended to equip organisations across India with a clear, phased approach to achieving quantum resiliency, while serving as a reference for sectoral regulators, to give specific and binding mandates for organisations.*

India's enterprises now operate in one of the most digitized economies in the world. Banking transactions, telecom networks, energy distribution, healthcare delivery, manufacturing supply chains, and digital commerce all depend on cryptographic mechanisms that secure data, protect transactions, and maintain trust at scale. These cryptographic mechanisms are increasingly at risk with the rapid progress in quantum computing and quantum error correction.

Quantum computing is now advancing at a pace that puts today's public-key cryptography on a clear path to obsolescence. Most estimates point to a 2028–2032 horizon for practical quantum attacks, but the risk is already present. Adversaries are believed to be capturing and storing encrypted traffic today under HNDL campaigns, with the expectation that it can be exploited once quantum capability matures. For enterprises, this means customer data, trade secrets, financial records, and operational intelligence could be compromised retroactively, even if systems appear secure today.

For enterprises, the implications of this risk are far-reaching. Cryptography is embedded in authentication systems, secure communications, payment infrastructure, cloud services, and countless business applications. If the existing cryptographic protections are weakened by the advances with quantum computing, the confidentiality of sensitive data and the integrity of critical operations can no longer be assured. Preparing for this eventuality requires organisations to develop a clear understanding of where cryptography is used within their systems, to assess which functions are most critical, and to begin planning for their transition. This migration is not a short-term exercise. It will take sustained effort over many years, with leadership attention, resources, and skilled teams dedicated to the task.

This roadmap is intended to support the enterprises in building Quantum Resiliency by providing a structured path to begin, achieve and sustain this transition. This document, first in the series of many documents, defines the recommended milestones, timelines, baseline expectations and the key activities required in each of the three milestones to ensure that by the early 2030s, the systems that underpin India's economy and society are secured against threats emanating from Cryptographically Relevant Quantum Computer (CRQC).

Milestones at a glance

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

Understanding Quantum Threats

A substantial portion of today's digital infrastructure rests on public-key cryptographic systems such as RSA, elliptic curve cryptography, and Diffie–Hellman. These systems derive their strength from the difficulty of solving certain mathematical problems with classical computing. Quantum computing, however, changes this assumption. Once Quantum Computers with sufficient scale and stability are realised, these problems are believed to be solved efficiently, rendering the protections of current public-key cryptography ineffective. Recent advancements in AI may also accelerate Cryptanalysis, Side channel attack computations, etc.

The precise timeline for such capabilities remains uncertain. Estimates from the research community converge on a possible window between 2030 and 2032, but it is important to note that the threat does not begin only at that point. Data encrypted today with algorithms vulnerable to quantum computing may be at risk of future exposure if adversaries store it until decryption becomes feasible. This creates a forward-looking vulnerability for information that must remain secure for long periods, such as financial records, personal health data, strategic designs, or critical communications.

The potential impact extends beyond individual organisations. Modern enterprises operate in tightly linked digital ecosystems where authentication, secure communication, and data exchange rely on common trust anchors. A breakdown of cryptographic assurances in one sector has the potential to cascade across others, creating systemic risk to the wider economy.

The challenge is therefore twofold: to safeguard sensitive data against the long-term risk of decryption, and to prepare for a structural shift in the cryptographic foundations of digital trust. Migration to post-quantum cryptography is not simply a matter of adopting new algorithms. It requires advance planning, careful prioritisation of high-priority systems, and the institutional capacity to manage cryptographic change in an orderly way.

Ways to Achieve Quantum Resiliency

Quantum resiliency can be built through two distinct approaches. The first comprises algorithmic approaches, where cryptographic schemes are designed to withstand attacks from quantum computers while running on classical hardware. These include post-quantum key establishment mechanisms, digital signature algorithms, and supporting primitives that can be embedded within existing network protocols, software stacks, hardware security modules, and cloud platforms. The focus of these technologies is to provide quantum-resistant security without altering the underlying communication infrastructure.

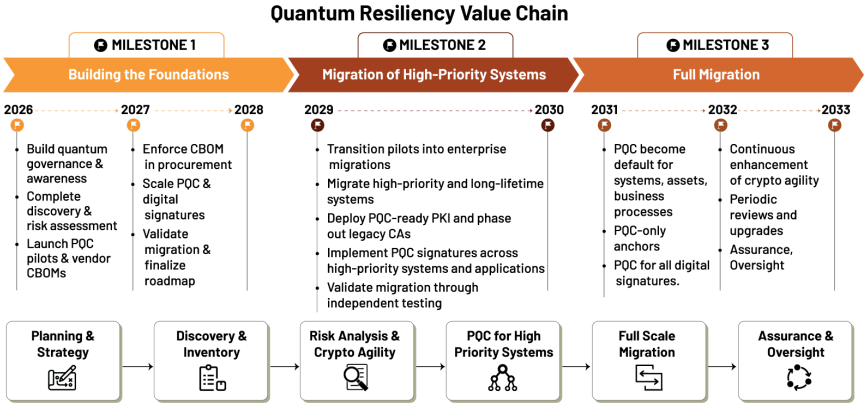
The second approach involves quantum communication technologies, exemplified by Quantum Key Distribution and related quantum-network techniques. These systems use quantum properties of light, among other parameters, to generate or distribute symmetric keys between communicating endpoints, with the ability to detect certain forms of interception. They represent a hardware-based method for key exchange, often used in controlled or point-to-point environments, and form part of ongoing global research into future quantum networking architectures.

Together, these approaches represent potential paths toward quantum resiliency. For most organisations, including CII and defence, algorithmic approach offers the broadest, immediate and pragmatic route to upgrading digital trust foundations, as they can be adopted across diverse systems with minimal changes to existing infrastructure. Quantum communication technologies, meanwhile, may remain important at the national level, supporting research goals and long-term aspirations for quantum networks. A balanced national approach can therefore combine the widespread deployment of PQC across enterprises with sustained and targeted investment in QKD, depending on each organisation's own assessment.

Steps Towards Quantum Resiliency

Timelines – At a glance

Enterprises cannot treat the migration to post-quantum cryptography as a single event. It is a staged process that requires planning, prioritisation, and disciplined execution over many years. This roadmap identifies three milestones on the path to quantum resiliency. Each milestone sets clear expectations for enterprise action, ensuring that progress is measurable and that the high-priority systems are migrated expeditiously. The intent is to provide organisations with a structured sequence of activities that begins with establishing foundations, advances through the migration of high-priority systems, and culminates in full adoption by 2033.



Milestone 1: Building the Foundations - (CII: No later than 31 December 2027, Enterprises: No later than 31 December 2028)

Milestone 1 represents the start of the quantum resiliency journey, where enterprises shift from awareness to preparedness. Milestone 1 focuses on building the leadership, governance, and foundational capabilities needed to manage quantum risk in a deliberate and coordinated manner and sets the organisational footing for the subsequent milestones that follow, ensuring that institutions have the clarity, structure, and readiness required before moving into deeper migration activities in subsequent milestones.

- Establish structured quantum awareness programmes supported by board and executive leadership, and executed by operational teams to ensure quantum risks are factored into existing risk frameworks.
    - Initiate targeted training, workshops targeted specific to sectors, and partnerships to build capabilities for managing discovery, pilots, vendor engagements, and migration activities.
- Appoint Quantum Lead or function, allocate resources, and establish cross-functional governance with board oversight.
    - **Factors for Consideration:** Discovery and Inventory Preparation Cost, Cost of Risk Assessment, Costs of Pilots – Sandboxes, Lab Setup/Augmentation, Costs associated with implementation of PQC or Remediation Activities, Costs associated with independent testing/validation/certification costs, Costs associated with deployment and operational costs, human capital and other associated costs.
- Complete discovery and inventory of cryptographic artefacts.
- Beginning from FY 2026–2027, start requesting CBOMs and Quantum Resiliency Roadmap from vendors in the procurement policy and/or service agreements.
    - Starting FY 2027–2028 mandate submission of CBOM from the vendors, through the procurement policy.
- Conduct quantum risk analysis and prioritise assets.
- Perform crypto-agility assessment and ensure adoption of crypto-agility as a guiding principle.
- Run pilots of PQC/Hybrid solutions for high-priority systems and initiate limited early migrations, while ensuring sufficient measures for business continuity and rollback plans.
- Start adopting PQC and/or Hybrid digital signatures schemes for high-priority software/firmware and systems with long shelf-life.
- Validate migration plan and activities to ensure investments are leading to building Quantum Resiliency for your organisation.
- Following the risk assessment, select an appropriate quantum-resilience strategy (PQC or QKD) after doing an internal assessment of the threat model, costs, scalability and other parameters.
- Based on their assessed risk and operating environment, enterprises may identify the approach to be taken for building quantum-resilience either through PQC or QKD or Hybrid Approach.

Milestone 2: Migration of High-Priority Systems – (CII: 31 December 2028, Enterprises: No later than 31 December 2030)

- Convert pilot learnings into funded migration programmes with clear KPIs.
- Enforce a strict "no new classical-only deployments" policy.
- Require all suppliers to submit CBOMs and their resiliency roadmaps.
- Include mandatory PQC/Hybrid cryptography and crypto-agility clauses in all contracts.
- Complete migration of high-priority systems identified in the risk assessment.
- Deploy PQC-capable PKI, enable hybrid/dual-chain certificates, and retire classical-only root of trust.
- Mandate PQC-capable digital signatures for all new software and firmware in high-priority systems, extending to medium-risk systems.
- Upgrade HSMs, KMS, and cryptographic libraries to PQC-ready versions, beginning with high-priority systems.
- Assess performance overheads arising because of adopting Quantum Resiliency products/solutions and adjust infrastructure capacity accordingly.
- Validate migration progress through independent third-party testing.
- Establish continuous monitoring for PQC performance and operational health.
- Develop cryptographic incident response playbooks for algorithm and parameter changes.
- Integrate PQC training into cybersecurity, DevOps, and IT learning programmes.
- Capture lessons from early migration phases and develop practical guidance for teams.
- Extend PQC awareness training to procurement, policy, and legal functions.
- Maintain a register of external products, services, and vendor dependencies affecting migration timelines.
- Define contingency plans for accelerated quantum breakthroughs, using interim quantum-safe controls where necessary.
- Track and document residual exposure to classical cryptography until full migration is complete.
- Contain classical-only systems within controlled enclaves where immediate migration is not feasible.
- Continuously monitor developments in PQC and QKD and see how these developments are impacting your resiliency plan. Reassess the implications and your strategy based on the developments and enhancements in PQC and QKD at that point in time.

Milestone 3: Full Migration – (CII: 31 December 2029, Enterprises: No later than 31 December 2033)

- Make PQC the default standard across all organisational systems and business processes.
- Periodically review algorithms, parameters, and key lengths as part of strengthened cryptographic lifecycle management.
- Complete enterprise-wide transition to PQC or hybrid algorithms for all systems and infrastructure. Decommission/Deprecate quantum-vulnerable cryptographic algorithms.
- Apply a layered risk-management approach for legacy systems that cannot migrate, using interim quantum-safe controls, segmentation, and planned decommissioning where possible.
- Operate PQC-only trust chains across internal environments.
- Ensure all digital signatures are executed exclusively using PQC algorithms.
- Require all vendors to demonstrate ongoing crypto-agility and continuous PQC enhancement.
- Maintain a register documenting vendor algorithm usage and future upgrade timelines.
- Establish long-term certification and audit programmes for external PQC solutions.
- Conduct independent third-party validation to ensure correct implementation and prevent fallback to vulnerable cryptography.
- Continuously monitor emerging PQC standards and developments that may influence security posture.
- Maintain sandboxes and testbeds for controlled evaluation of new cryptographic primitives, supported by the crypto-agility established earlier.

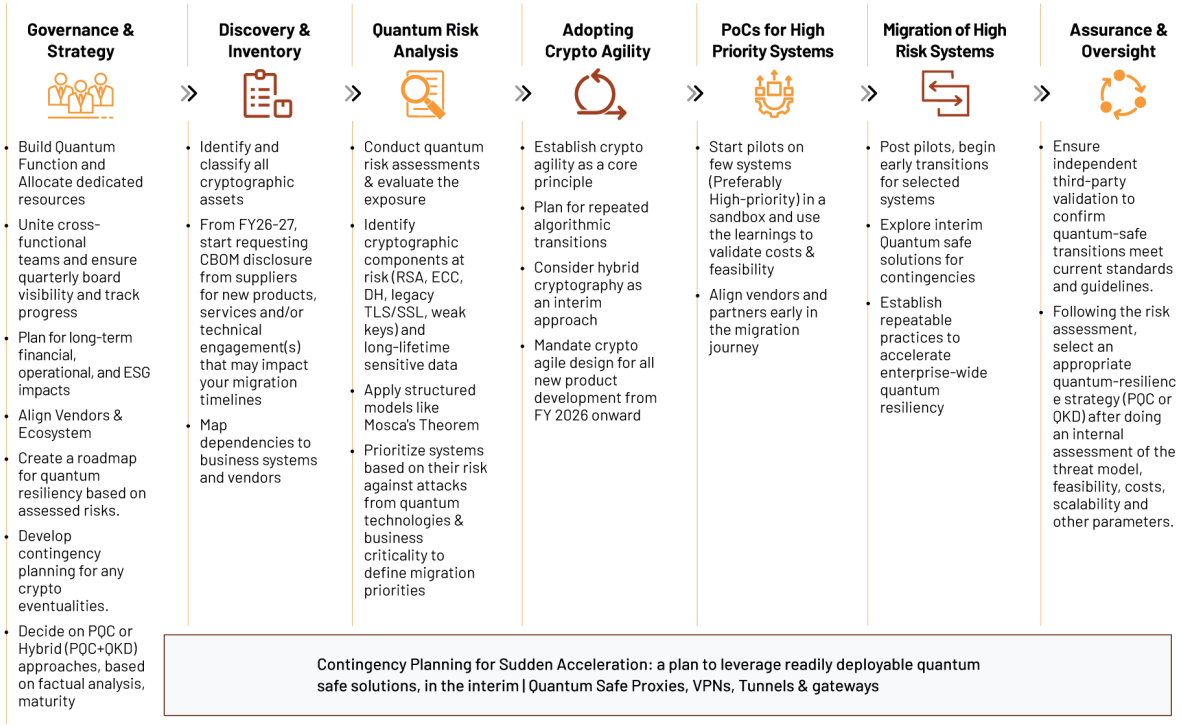
Migration Planning - Recommended Activities (Detailed)

The “At the glance” section of the timelines sets out the milestones for India’s enterprises to achieve quantum resiliency by 2033. This section provides detailed guidance on the activities required at each stage. The objective is to give organisations a structured set of actions that can be adapted to their sector, size, and risk profile, while ensuring consistency of approach across the economy.

Each milestone builds on the previous one. The first focuses on establishing governance and laying the groundwork for transition. The second moves into migration of high-priority systems and enforcement of supplier accountability. The third achieves full adoption of post-quantum cryptography and *institutionalises cryptographic agility as a practice*.

Milestone 1 – Building the Foundations - (CII: No later than 31 December 2027, Enterprises: No later than 31 December 2028)

By 31 December 2028, organisations are required to move from awareness to preparedness. The first milestone is about putting the building blocks in place: establishing governance, defining what quantum risk means in your context, based on risk and/or priorities, and developing organisational capabilities required for a smooth migration in the years ahead.



Governance & Strategy

- **Leadership commitment:** Boards and CEOs should setup a dedicated Quantum Function, typically reporting to the leadership. This function is responsible for steering the enterprise-wide Quantum Resiliency plan.
- **Resource Allocation:** Allocate necessary resources for quantum-safe migration. The resources for building Quantum Resiliency may be additional to the resources allocated for managing security.
- **Cross-functional ownership:** The Quantum Function should bring together representatives from IT, security, legal, risk, and core business units. This function becomes the steering forum for quantum resiliency, embedding it into the organisation's existing risk and governance frameworks.
- **Costs and sustainability:** Transitioning to PQC may require sustained financial and operational investment, as newer algorithms may require greater processing power and energy. These implications, including potential effects on ESG performance, should be incorporated into long-term technology and investment strategies.
- **Vendor & Ecosystem Alignment:** Identify and engage with key vendors/partners and take them along this migration journey.
- **Build a roadmap for quantum resiliency:** Once the Risk assessment and prioritisation is completed, build an internal roadmap for building Quantum Resiliency, aligned with the overall timelines published in this document or relevant sectoral regulators and nodal organisation for Cybersecurity (CERT-In).
- **Contingency Planning:** Prepare a contingency plan, which may involve leveraging readily deployable quantum-safe solutions (Proxies, Tunnels, VPNs, Gateways, etc.,) in the interim, should the quantum threat(s) realise before the planned migration timeline. The contingency planning should take into account the business continuity requirements and have a roll-back plan in case of any issues.

Discovery and Inventory - Cryptography Artefacts

- **Identify Cryptography:** Identify and catalogue all cryptographic artefacts (algorithms, keys, certificates, protocols, libraries, hardware modules, cloud services) across internal and external facing applications, products, and infrastructure and classify them by type, lifetime, and business criticality.
- **Procurement:** Communicate to the vendors that after FY2026-2027, they need to provide Cryptographic Bill of Materials (CBOM) and their quantum resiliency roadmap as part of every new product or service engagement.
- **Dependency Mapping:** Connect cryptographic artefact(s) to the business systems, vendors, and data flows in your organisation. This dependency map will form a baseline for any migration plan.

Quantum Risk Analysis

- **Comprehensive Risk Assessment:** Perform a comprehensive quantum risk assessment and identify systems prone to quantum attacks. Categorise assets based on business impact, data lifetime, risk profile, and other relevant parameters (cost of migration, supply chain details, lifecycle management data, risk tolerance, and other parameters relevant to your context). This step will help guide prioritisation for early migration
- **Evaluate exposure:** Identify cryptographic components vulnerable to quantum attacks (e.g., RSA, ECC, Diffie-Hellman, legacy TLS/SSL, or short key lengths) and highlight risks to long-lifetime sensitive data.
- **Apply structured methods:** Use frameworks such as Mosca's Theorem (comparing data lifetime plus migration time against the expected arrival of Cryptographically Relevant Quantum Computer capabilities) to identify urgent risks.
- **Set priorities:** Rank systems and datasets as High, Medium, or Low urgency, based on business impact and risk profile, creating a clear migration priority map for the organisation.

Defining & Adopting Crypto-Agility

- **Institutional principle:** Establish crypto-agility (The ability to change algorithms, protocols, and keys rapidly without business disruption) as a core capability, as you plan the migration.
- **Plan for repeated transitions:** Accept that this migration will not be the last cryptographic change. Future standards will evolve, and systems must be designed to accommodate these cycles. Investing in good crypto-agility practices will significantly save resources and time when the subsequent transitions are required.
- **Hybrid Cryptography:** Hybrid cryptography (classical + PQC) may be considered for adoption, as per industry and organisational policy, considering interoperability and security, vis-a-vis current state of PQC maturity and regulatory guidance.
- **New Product Developments:** Crypto-agility practices should be ingrained for new system/product/application created from FY2026-27, ensuring systems are backward compatible, without leading to downgrade attacks.

Pilot & PoCs of PQC/Hybrid PQC Algorithms and Solutions for high-priority systems

- **PoCs – High Priority Systems:** Begin with limited pilots in a few systems, preferably high-priority systems identified from Quantum Risk Analysis, in a sandbox environment.
- **Build Organisational Confidence:** Use these pilots to determine feasibility, do vendor alignment, path for migration, costs, and risks of PQC adoption at a small scale. These pilots will help organisations prepare a better migration plan.

Start Migration of High-Priority Systems

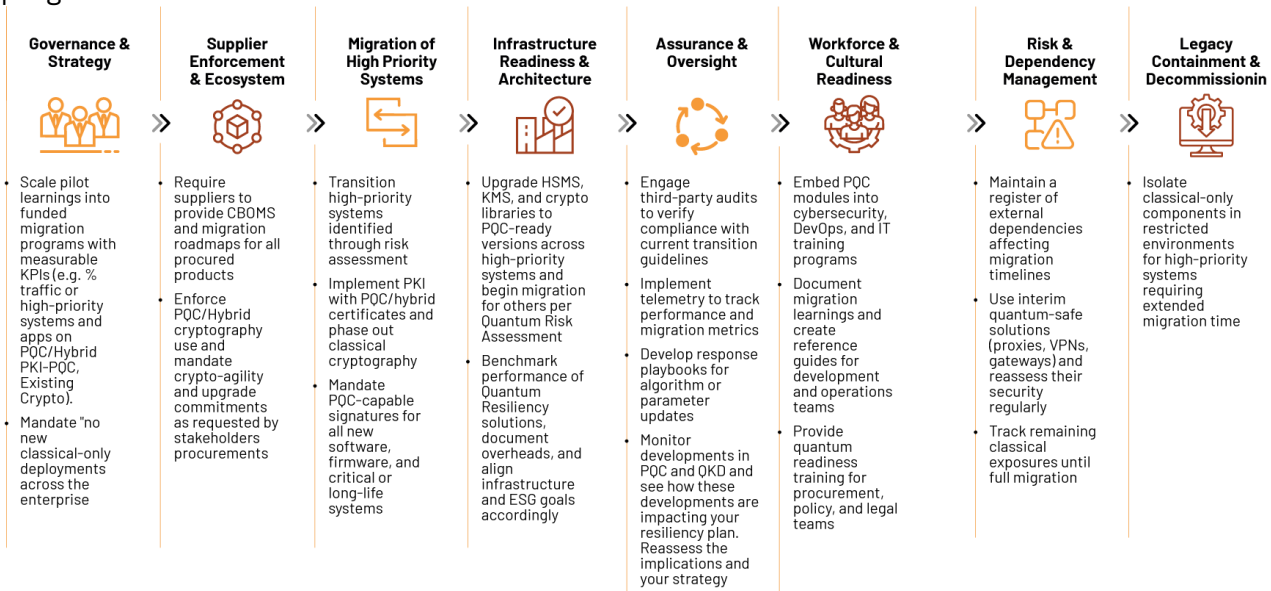
- **Early transitions/Interim Solutions:** Once the pilots are finished, start migrating a select set of high-priority systems identified in the Quantum Risk Analysis.
  o In case the transition is expected to take a longer time, explore interim solutions such as Quantum-Safe Proxies, VPNs, Tunnels & gateways for providing security till the migration is completed.
- **Capture lessons for scale:** Use the migration experience to document costs, operational challenges, and vendor dependencies, feeding these insights into the broader enterprise roadmap for migration.
- **Build foundation for accelerated adoption:** Ensure these early migrations establish repeatable practices and governance that will support larger-scale transitions in the next milestone.

Assurance & Oversight

- **Independent validation:** Use independent, third-party testing to confirm the transition is being done as per the guidelines in-force at the time.

Milestone 2 – Complete Migration of High Priority Systems

*(**CII**: No later than 31 December 2028, **Enterprises:** No later than 31 December 2030)*, organisations should move from pilots and preparation to complete migration of high-priority systems and focus on enforcing supplier accountability and ensuring board-level visibility of progress.



Governance & Strategy

- **Programme delivery:** Convert pilot learnings into funded migration programmes with clear KPIs (e.g., % of traffic on PQC or hybrid, % of critical applications on PQC-ready Public Key Infrastructure (PKI)).
- **Migration policy:** Enforce a "no new classical-only deployments" principle across the enterprise.

Supplier Enforcement & Ecosystem

- **CBOM compliance:** Require all suppliers to submit CBOMs and PQC roadmaps for the products you plan to procure from them.
- **Contract clauses:** Mandate all products use PQC/Hybrid Cryptography and ensure crypto-agility and upgrade commitments are requested by internal and external stakeholders in all procurements.

Migration of High Priority Systems

- **Priority migrations:** Complete transition for high priority systems, as identified in the risk assessment and prioritisation.
- **PKI modernisation:** Deploy PQC-capable PKI, enable dual-chain/hybrid certificates, and gradually phase out classical cryptography, certificates and keys.
- **Digital Signatures:** Mandate PQC-capable digital signatures for all new software and firmware, for high-priority systems and systems with long shelf life.

  o Adopt PQC-capable digital signatures for all new software and firmware, medium-risk systems.

Infrastructure Readiness & Architecture

- **Crypto platforms:** Complete upgrading HSMs, KMS, and crypto libraries to PQC-ready versions for all high priority systems and start the same migration for medium and low priority systems as determined during Quantum Risk Assessment.
- **Performance planning:** Conduct baseline tests, document PQC overheads. You may need to adjust infrastructure capacity & capabilities, ESG Goals as necessary.

Assurance & Oversight

- **Independent validation:** Use third-party testing to confirm the transition is being done as per the guidelines in-force at the time.
- **Continuous monitoring:** Deploy telemetry to monitor performance and other parameters resulting from the migration.
- **Crypto-Incident Preparedness:** Prepare cryptographic response playbooks for algorithmic update(s) or parameter changes.

Workforce & Cultural Readiness

- **Training integration:** Institutionalise PQC modules into cybersecurity, DevOps, and IT curricula.

- **Knowledge sharing:** Document lessons learned from Milestone 1 migration and build practice guides for development and operations team to refer to while building or maintaining products/posture.
- **Wider awareness:** Extend (non-technical) PQC readiness training to procurement, policy, and legal teams.

Risk & Dependency Management

- **Dependency mapping:** Maintain register of external dependencies including, but not limited to products, services, vendors and other factors that may affect your migration timelines.
- **Contingency planning:** Define contingency planning for sudden acceleration of Quantum Technologies that may impact security of pre-quantum cryptography. Plan to leverage readily deployable quantum-safe solutions, in the interim – Including but not limited to: Quantum-Safe Proxies, VPNs, Tunnels & gateways controls, untill the full migration is complete. Do continuous assessment of the security foundations and architecture of these interim solutions.
- **Residual risk:** Continue to document and track classical exposure until complete migration.

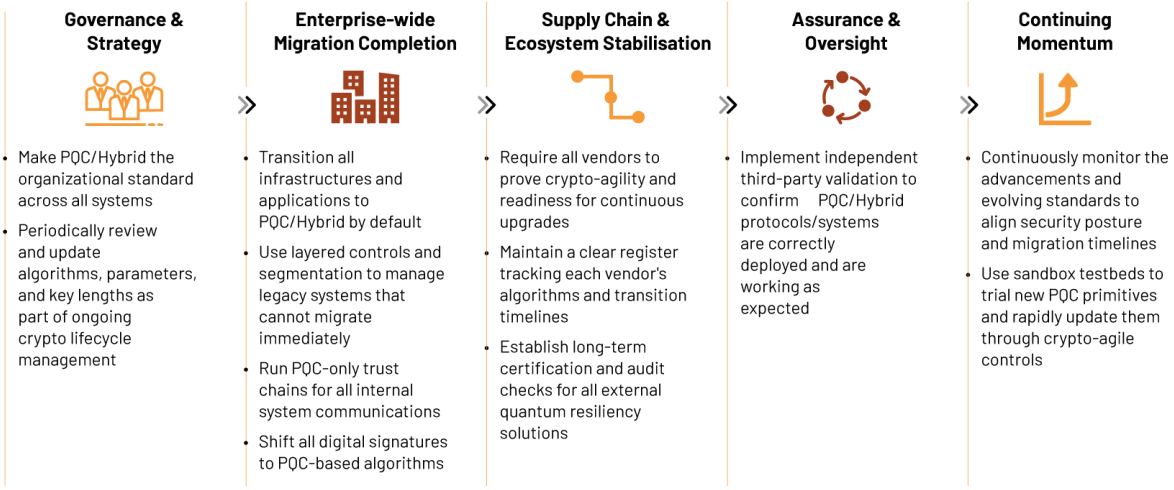
Legacy Containment & Decommissioning

- **Enclave control:** For high-priority systems that may need long time for migration, isolate classical-only components/systems, as much as possible, within restricted environments.

Milestone 3 – Full PQC Adoption

*(**CII:** No later than 31 December 2029, **Enterprises:** No later than 31 December 2033)*
No later than 31 December 2033, organisations should have achieved quantum resiliency at scale. PQC becomes the default, and cryptographic agility is institutionalised as a practice.

Governance & Strategy



- **PQC As a Standard:** Make full PQC adoption the organisational standard for all systems, and business processes.
- **Enhancement to existing Cryptographic Lifecycle Management:** Conduct periodic reviews of algorithms, parameters, and key lengths, in addition to the existing cryptographic lifecycle management framework(s).

Enterprise-wide Migration Completion

- **Full PQC by default:** Transition all systems and infrastructures to PQC/Hybrid algorithms.
- **Legacy Systems:** For assets that cannot be migrated to post-quantum cryptography, organisations should adopt a layered risk management approach that combines interim quantum-safe measures with long-term transformation plans, fused with segmentation practices. If possible, plan for a graceful degradation leading to decommissioning.
- **PQC Trust Chains:** Operate PQC-only trust chains for internal systems.
- **Digital Signatures:** Ensure all signatures are done through PQC algorithms.

Supply Chain & Ecosystem Stabilisation

- **Vendor PQC & Agility Readiness:** Require vendors to demonstrate Crypto-Agility and continual PQC Enhancement(s) and compliance.
- **Conformance register:** Maintain an authoritative register of vendor algorithm usage and timelines.
- **Long-term assurance:** Institute certification and audit programmes for external PQC solutions.

Assurance & Oversight

- **Independent validation:** Use third-party testing to confirm PQC protocols are implemented correctly and without fallback to vulnerable standards.

Continuing Momentum

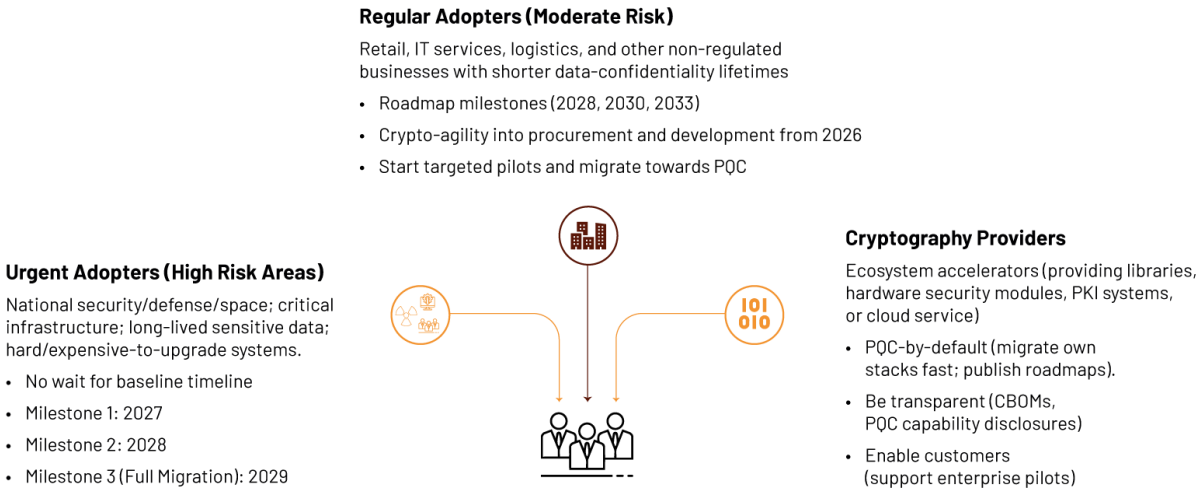
- **Algorithm monitoring:** Track emerging PQC standards, and other developments that may impact your security posture and the timelines.
- **Testbed validation:** Maintain sandbox environments for controlled trials of new primitives. Crypto-Agility will help you with the controlled trials and rapid re-deployment/updates.

PQC Personas

The urgency of migration to post-quantum cryptography is not uniform across all organisations. Different sectors, data types, and system lifetimes create distinct risk profiles. To help enterprises prioritise their response, this roadmap defines PQC Personas. These personas categorise organisations based on their exposure to quantum risk, the longevity of their systems, and the sensitivity of the data they safeguard.

The timelines and activities set out in this roadmap are intended as the baseline for Regular Adopters. Urgent Adopters, including Power Sector, Telecom Sector**,** ISRO, DRDO, ONGC, and other operators of critical information infrastructure (CII), must complete their transition significantly earlier, given the nature of the data and systems under their control. Cryptography providers and enablers, whose products and services shape the resilience of entire sectors, carry a parallel responsibility to accelerate their own adoption and support the wider ecosystem.

An enterprise may identify with more than one persona. Where this occurs, the persona with the highest risk must guide priorities and determine the pace of migration.



Persona 1 – Urgent Adopters (Organisations facing High Risks -> Accelerated Timelines)

Organisations that:

- Are qualified as Critical Information Infrastructure organisations.
- Manage long-lifetime data whose confidentiality must be preserved for decades, such as medical records, design blueprints, or strategic communications.
- Depend on systems that are difficult or costly to upgrade once deployed (satellite systems, industrial control systems, defence networks).

Implications

These CII enterprises must not wait for the regular timelines. Completion of migration of high and medium priority systems is essential, latest by 31 December 2028, and the full migration must be finished by 31 December 2029.

The organisation(s) fitting this persona should focus on embedding crypto-agility into procurement and development at the earliest, from 2026 onwards, establish Governance, complete crypto inventories rapidly, and transition pilots into production systems ahead of the Regular Adopters. Independent validation and sectoral oversight will be critical to ensure readiness. For these organisations, entire Quantum-Safe Migration - Milestones 1, 2 and 3 must be completed by 31 December 2027, 31 December 2028 and 31 December 2029 respectively.

Persona 2 – Regular Adopters (Organisations facing Moderate Risk Baseline Timelines)

Organisations that:

- Do not directly operate critical infrastructure or defence systems.
- Manage customer or enterprise data with shorter confidentiality lifetimes (e.g., retail, IT services, logistics, non-regulated businesses).
- Have more flexibility to replace or upgrade systems within their normal IT lifecycle.

Implications

For these organisations, the roadmap milestones 1, 2, and 3 (2028, 2030, 2033, respectively) provide a realistic baseline. The organisation(s) fitting this persona should focus on embedding crypto-agility into procurement and development from 2026 onwards, begin pilots for systems, preferably high-priority, and gradually migrate as PQC standards evolve. Delay beyond these milestones will increase costs, risk exposure and create dependencies that are difficult to unwind.

Persona 3 – Technology Providers and Enablers

Organisations that:

- Develop or maintain cryptographic libraries, hardware security modules, PKI systems, or cloud services that others depend upon.
- Supply products or services used widely across sectors, making their cryptographic choices critical for downstream customers.
- Influence the pace of migration across the economy through their standards, product roadmaps, and support for PQC adoption.

Implications

These entities must lead by example, migrate ahead of dependent stakeholders, publish migration roadmaps, and enable PQC features in their products by default. Vendor transparency through CBOMs, PQC capability disclosures, and active support for enterprise pilots is essential.

Applying PQC Personas

- Persona identification should be completed at the beginning of Milestone 1 – Building the Foundations.
- Organisations may belong to more than one persona. The highest-risk persona should set the pace of migration.
- Persona assignments are not static; they must be reviewed periodically as threats, technologies, and business risks evolve.
- Timelines in this roadmap reflect the expectations for Regular Adopters. Urgent Adopters, including critical infrastructure operators and strategic agencies, must transition ahead of these dates.

Crypto-Agility

The transition to post-quantum cryptography is not the end of the journey. It is the beginning of an era where cryptographic transitions may occur repeatedly, driven by new discoveries, evolving standards, and unforeseen vulnerabilities. Unlike most security controls, cryptography does not fail gradually. When algorithms are broken, they fail definitively and absolutely. In such a scenario, the ability of an enterprise to respond with speed and confidence will determine whether its operations remain trusted and resilient. This capability is what we define as crypto-agility.

Strategic Rationale

- **Current PQC algorithms may evolve/change:** The first generation of post-quantum algorithms are now being standardised. History shows that some algorithms will need replacement or revision as they are tested at scale. Enterprises that approach migration as a one-off upgrade will face recurring disruption.
- **Data lifetimes exceed algorithm lifetimes:** Confidential financial, healthcare, defence, and R&D data must remain protected for decades. If organisations cannot switch cryptographic protections quickly, long-lived data may be exposed.
- **Enterprise Resilience:** Every organisation, regardless of sector, carries direct responsibility for securing its own trust foundations. If cryptography is treated as static, each new cryptographic change requires costly "big bang" migrations. With agility, upgrades can be integrated into routine governance cycles, reducing cost, downtime, and systemic fragility.

Elements of Crypto-Agility

Building crypto-agility means embedding adaptability into governance, design, procurement, and operations:

Governance and Oversight

- Risks due to Cryptography must be treated as a lifecycle risk. Board shall be informed of the risks.
- Risk frameworks should explicitly account for cryptographic dependencies, lifecycle, and change readiness.

System and Architecture Design

- Applications and infrastructure should decouple cryptographic modules/functionalities from business logic.
- Agility requires extensibility (adding new algorithms), removability (retiring obsolete ones), and reversibility (rollback if failures occur).

Procurement and Vendor Alignment

- Require Cryptographic Bills of Materials (CBOMs) from all vendors.
- Contracts must obligate vendors to maintain PQC migration roadmaps and demonstrate agility in their solutions.

Operational Practice

- Conduct periodic algorithm and parameter reviews (every 9 to 12 months).
- Establish tested procedures for large-scale and automated certificate and key rotations, algorithm swaps, and interoperability testing.

Crypto-agility is the only sustainable way to manage the cryptographic transitions. Without it, future algorithmic changes may be disruptive, expensive, and potentially destabilising. With right Crypto-Agility practices, organisations can adapt smoothly, protect long-lived data, and maintain continuity of trust.

This section provides only a preview. A dedicated document on Guidelines for Crypto-Agility will be released as part of this series, offering detailed guidance for governance, architecture, procurement, and operational practices.

Challenges

The migration to post-quantum cryptography is not a routine upgrade; it is a foundational change to the trust model of digital systems. As enterprises operationalise this transition, several challenges are expected to emerge across governance, technology, and ecosystem coordination.

Diversity of Legacy Systems

- The scale and heterogeneity of legacy infrastructure across critical sectors will make the transition complex.
- Many systems were not designed with crypto-agility, and hard-coded algorithms or dependencies will require redesign or replacement.

Interoperability During Transition

- During the migration phase, systems will need to support both classical and quantum-safe algorithms, creating coexistence and interoperability challenges.
- This dual compatibility may increase system complexity and must be carefully managed to avoid downgrade or fallback risks.

Vendor and Ecosystem Readiness

- Enterprises rely heavily on third-party vendors for hardware, software, and cloud services; PQC readiness among these providers remains uneven.
- Delays in supplier compliance or absence of PQC capability declarations could impact overall migration timelines.

Performance and Operational Overheads

- Quantum-Safe algorithms may require greater computational resources, potentially affecting performance in latency-sensitive or high-volume environments.
- Performance testing, tuning, and infrastructure optimisation will be required to maintain operational efficiency.

Skills and Capacity Limitations

- The availability of professionals experienced in PQC integration, testing, and lifecycle management remains limited.
- Targeted capacity-building and continuous skill development will be critical for sustained progress.

Governance and Investment Continuity

- Migration requires long-term executive oversight, dedicated funding, and consistent programme management.
- Without sustained leadership attention, early pilot gains may not translate into enterprise-wide adoption.

Assurance and Validation

- PQC implementations must be independently validated to confirm algorithmic correctness and prevent fallback to vulnerable standards.
- Lack of common validation frameworks across sectors may lead to uneven assurance levels.

Sectoral and Cross-Domain Coordination

- India's digital infrastructure is deeply interconnected across financial, telecom, energy, and public-sector systems.
- Inconsistent migration schedules or implementation approaches across sectors could create interoperability and trust-chain challenges.

Addressing the Challenges

A coordinated and phased implementation, supported by vendor enablement, performance testing, capacity development, and independent assurance, will be essential. Embedding crypto-agility and continuous governance as enduring capabilities will help enterprises manage evolving standards, future algorithm changes, and long-term quantum risk.

Addressing these challenges demands a whole company, a whole industry and a whole country's approach.

A note on Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD)

As organisations prepare for the quantum era, two distinct technological approaches have emerged to secure data and communications.

- Post-Quantum Cryptography (PQC) and
- Quantum Key Distribution (QKD)

Both seek to mitigate the risks introduced by quantum computing, yet they differ significantly in their underlying principles and implementation models.

Post-Quantum Cryptography involves cryptographic algorithms that are designed to resist attacks from quantum computers while continuing to operate on existing digital infrastructure. These algorithms can be deployed through software and minimal hardware updates, integrated into current security protocols, and managed within established governance and assurance frameworks. PQC protects both data exchange and authentication processes, enabling secure communications and digital signatures without the need for new physical infrastructure. Because PQC aligns with current networking and computational models, it can be adopted at scale and updated as standards evolve.

Quantum Key Distribution (QKD), by contrast, uses quantum properties of light to generate/distribute symmetric keys between communicating parties. Its defining characteristic is that any attempt to intercept the quantum signal alters its state, providing a mechanism to detect eavesdropping. QKD, however, addresses only the distribution of keys and not the authentication of participants (devices) or the encryption of data itself. These functions still rely on classical or post-quantum cryptographic algorithms, which must remain secure for the system to be effective.

Over the past decade, several national and international programmes have advanced Quantum Key Distribution through laboratory demonstrations, pilots, and satellite-based experiments. Notable examples of QKD include the European Quantum Communication Infrastructure (EuroQCI) and China's Quantum Communication Network (CN-QCN), which have successfully demonstrated QKD over long distances, including intercontinental satellite links. These initiatives show that QKD may offer additional assurance for controlled, high-assurance environments where dedicated infrastructure and operational conditions can be maintained.

At the same time, independent guidance from national cybersecurity agencies such as the UK's NCSC, Australia's ACSC, BSI (Germany) and other countries and enterprises like Google (Google's Commitment to a Quantum-Safe Future: Why PQC is Google's Path Forward and not QKD), Cloudflare (You don't need quantum hardware for post-quantum security) have cautioned that QKD is not suited for any enterprise, including, defence and CII deployments. The assessments highlight practical constraints for large scale QKD deployments, which include: the need for dedicated optical channels or trusted nodes, sensitivity to environmental conditions, limited range without specialised repeaters, and interoperability challenges that can create vendor dependencies. These factors do not diminish QKD's scientific or strategic value but do place boundaries around its applicability in heterogeneous, internet-scale enterprise environments.

Considering these dynamics, PQC remains the most widely deployable and infrastructure-aligned pathway for organisations seeking quantum-resilient security across diverse systems and networks, including for CII and Defence. QKD may continue to evolve within research and national-security contexts, and its future capabilities may expand as underlying technologies mature.

Organisations should, therefore, make informed, evidence-based decisions for adopting either PQC or QKD or Hybrid Approaches to build quantum resiliency. It is also imperative that no matter which approach organisations take, they should maintain awareness of ongoing developments in both approaches (PQC or QKD).

Other Interim Quantum-Safe Technologies

In addition to approaches such as post-quantum cryptography, long-term cryptographic modernisation and Quantum Key Distribution, several interim technologies are being adopted to reduce exposure during the transition period. These solutions are typically deployed to protect data in motion, strengthen cryptographic controls at key boundaries, or address specific operational constraints where immediate system-wide upgrades are not feasible. The technologies outlined below represent commonly observed interim approaches and are not intended to be an exhaustive list. Their applicability and effectiveness depend on organisational context, system architecture, and risk profile, and they should be used as part of a broader, risk-based quantum-safe migration strategy rather than as standalone or permanent solutions.

Quantum Gateways

Quantum gateways are typically deployed at network periphery where traffic enters or leaves an organisation. Gateways work by terminating existing cryptographic sessions and re-establishing them using post-quantum or hybrid cryptographic mechanisms. Gateways allow organisations to protect sensitive data flow at the boundary without having to immediately modify internal applications or legacy systems. In practice, gateways are used to reduce exposure on external network as broader cryptographic upgrades are planned and rolled out across the environment.

Quantum VPNs

Quantum-Safe VPNs are an extension of traditional VPNs, with the key difference being the use of post-quantum or hybrid cryptographic methods during key exchange. The overall operating model remains similar, making them easier to deploy in existing environments. VPNs are commonly used for site-to-site links, remote access, and inter-data-centre connectivity, where data traverses untrusted networks. VPNs provide a practical way to address long-term confidentiality risks while full application-level migration to quantum-safe cryptography is underway.

Quantum Proxies and Tunnels

Quantum-Safe proxies and tunnels are used to wrap specific applications or communication paths with stronger cryptographic protection. Instead of changing the application itself, traffic is intercepted and secured at an intermediate layer using post-quantum or hybrid schemes before being forwarded onward. This approach is useful for selectively protecting high-risk services, APIs, or data flows, especially where systems are difficult to upgrade due to age, vendor constraints, or operational complexity.

Quantum & True Random Number Generators (QRNG & TRNG)

Quantum random number generators and True Random Number Generators provide high-quality randomness based on physical processes. This improves the strength of cryptographic key generation and other security-critical operations that depend on entropy. QRNGs do not, by themselves, make cryptographic systems quantum-safe, but they help strengthen the overall security of both classical and post-quantum implementations. They are typically integrated into hardware security modules, key management systems, or cryptographic services where strong entropy is required.

The reader must note that the above are only a few of many interim solutions for building Quantum Resiliency and do not represent all technologies available today for Quantum Resiliency. Technologies for building Quantum Resiliency will continue to evolve over coming months and years.

Technology Considerations for Quantum-Safe Migration Across CII

The impact of adopting quantum-safe migration technologies across Critical Information Infrastructure is shaped less by the cryptographic algorithms themselves and more by how these technologies interact with existing system architectures, operational constraints, and ecosystem dependencies. In practice, the same quantum-safe control can have very different consequences depending on where it is applied and how it aligns with system design and usage patterns.

Latency Sensitivity

The impact of quantum-safe cryptography is closely tied to how much latency a system can tolerate. Environments that operate comfortably within millisecond-level budgets can generally absorb post-quantum handshake overhead through software implementations and infrastructure scaling. Systems with microsecond-level or lower constraints, however, are highly sensitive to even small increases in processing time or jitter, making direct endpoint adoption difficult.

Handshake Frequency

Post-quantum overhead is primarily incurred during key exchange and authentication rather than during bulk data encryption. Systems that establish connections infrequently or maintain long-lived sessions experience relatively low impact from PQC adoption. In contrast, architectures that rely on frequent TLS renegotiation, mutual authentication, or short-lived sessions amplify the cost of post-quantum primitives.

User and Service Tolerance

The tolerance of users or dependent services to performance degradation shapes how aggressively quantum-safe technologies can be introduced. In many cases, modest increases in response time are not perceptible and have limited operational impact. In other contexts, even small delays can translate directly into service degradation, safety risk, or financial loss. Understanding these tolerance thresholds is essential to selecting appropriate migration paths & technology for building quantum resiliency.

Hardware Constraints

Many critical systems operate on long-lived hardware platforms with limited compute headroom and infrequent upgrade cycles. Embedded devices, field equipment, and certified systems may not support software-based PQC without significant redesign. Availability of PQC-capable HSMs, KMS platforms, and cryptographic accelerators also affects readiness. Where hardware limitations exist, interim controls are often required until the next refresh cycle.

Vendor Dependence

Quantum-Safe migration is often constrained by reliance on OEMs and third-party platforms. Even where algorithms are standardised, practical adoption depends on vendor implementation, firmware updates, interoperability testing, and backward compatibility. Roadmap transparency varies widely across vendors, influencing how quickly organisations can move from planning to execution. Strong vendor engagement and alignment are therefore critical enablers of migration.

Cross-Border Dependencies

Many critical systems depend on international standards, protocols, and counterparties. Cryptographic changes in these environments are constrained by cross-border interoperability requirements and alignment with global bodies. Even when internal systems are technically ready, external dependencies may delay end-to-end migration. Managing these constraints requires early engagement with international ecosystems and realistic expectations around achievable timelines.

Conclusion

The transition to post-quantum cryptography is a generational change in the foundations of digital security. It cannot be achieved in a single step, nor can it be left to government alone. Every enterprise that depends on digital trust has a direct responsibility to act, guided by the timelines and activities in this roadmap.

The milestones defined here provide the baseline for Regular Adopters, while Urgent Adopters, including national security agencies, critical infrastructure operators, and strategic enterprises, must move faster. Cryptography providers and enablers must lead from the front, ensuring that the technologies they deliver support and accelerate this transition.

But migration alone is not enough. If organisations approach PQC as a one-time transition/migration, they will face the same disruption again when algorithms evolve, parameters change, or vulnerabilities are uncovered. The true test of resilience lies in crypto-agility, the capacity to adapt cryptographic foundations continuously and without disruption. Agility turns a disruptive risk into a managed routine, protecting long-lived data, lowering future costs, and sustaining customer and partner trust.

This document establishes the strategic direction. The subsequent documents in this series will provide detailed guidance on crypto-agility, vendor engagement, assurance mechanisms, and sector-specific pathways. Together, these will equip India's enterprises to manage the PQC transition in an orderly way, and more importantly, to build the agility needed to keep pace with the cryptographic challenges of the decades ahead.

Further Support Needed

The continued implementation of this roadmap will benefit from sustained institutional guidance, policy alignment, and technical collaboration across government, industry, and research. Structured support and engagement from the National Quantum Mission (NQM) will help maintain consistency in guidance, interoperability, and capacity throughout the migration process.

Key areas of support include:

- **Supplementary guidance:** The sub-committee recommends that the detailed documentation on crypto-Agility frameworks, Quantum Risk Assessment and Prioritisation methodologies, and operational playbooks be released in due course. These references are critical in providing clarity and guidance for the ecosystem during the migration. Similar approaches are being followed by countries across the world.
- **Ecosystem collaboration:** Continued engagement with international partners in Europe, the United States, and Asia will help integrate global experience and strengthen India's quantum-safe readiness. Programmes like EuroQCI and NIST's international PQC outreach demonstrate the value of cross-border collaboration.
- **Preferential Market Access:** Subcommittee recommends that the "Public Procurement Order 2019 Cybersecurity Products (released by MeitY)" may be applied to products and solutions used for Quantum-Safe Migration. This will also ensure technology sovereignty in building Quantum Resiliency.
- **Development of PQC Algorithms & Capabilities in India:** The sub-committee recommends that the National Quantum Mission (NQM) facilitate the development and testing and standardisation of indigenous PQC Algorithms and participation of Indian companies, products, and services in the domestic market, provided these solutions conform to international standards and assurance requirements. This approach should be complemented by continued openness to credible global technologies that demonstrate interoperability and adherence to recognised best practices. There is a need to offer hand-holding and other support to help domestic companies develop, validate and commercialise Indian PQC algorithms and also to help them meet global standards and adoption.
- **Vendor participation:** Since many vendors operate outside the scope of existing sectoral regulators, the sub-committee recommends creating a policy framework that enables and encourages their active engagement with regulated entities. Such a framework would facilitate structured collaboration, ensure better alignment of products and services with regulatory expectations, and promote shared accountability across the ecosystem.
- **Capacity development:** To continue strengthening the national quantum-safe ecosystem, further work will be required to translate this roadmap into sustained operational and technical action. As these activities expand in scope and complexity, the National Quantum Mission (NQM) may consider enhancing the resources made available to this subcommittee to provide timely guidance and support for the wider ecosystem. Such reinforcement would help sustain momentum, ensure continuity in implementation, and maintain alignment across stakeholders as the ecosystem matures.

- **Sandboxes:** As India builds Quantum Resiliency, there is a growing demand for national sandboxes (Sector-specific and industry sandbox), from the solution providers and users of quantum-safe solutions. NQM and/or sectoral regulators may invest in providing sandboxes to provide support to and/or accelerate India's quantum resiliency journey.

Coordinated guidance, knowledge exchange, and an open yet standards-driven ecosystem will be key to ensuring that India's quantum-safe transition remains inclusive, resilient, and aligned with global best practices.

International Efforts in Quantum-Safe Migration

Please refer to: postquantum.in for the most up-to-date information on India's and international roadmaps.

National Efforts

United States (US)

- **Quantum Resiliency and enforcement:** NSM-10, OMB M-23-02, CNSA 2.0 and NIST IR 8547 together mandate cryptographic inventory, crypto-agility, budgeting, and migration across Federal and National Security Systems, explicitly addressing harvest-now-decrypt-later risk.
- **Standards-led global influence:** NIST's PQC standardisation (ML-KEM, ML-DSA, SLH-DSA) and CNSA 2.0 effectively set the global vendor and ecosystem baseline for quantum-safe products.

European Union (EU)

- **Coordinated PQC migration across 27 states:** The EU's Coordinated Implementation Roadmap aligns member states on phased PQC adoption, avoiding fragmentation in critical infrastructure and cross-border systems.
- **Quantum-secure communications at continental scale:** EuroQCI combines terrestrial fiber and space-based QKD, positioning Europe as the only region pursuing PQC + sovereign quantum networks in parallel.

United Kingdom (UK)

- **Early, explicit migration timelines:** NCSC timelines force early discovery, prioritization, and migration planning across government and CNI, rather than deferring action until standards mature.
- **Operational crypto-agility focus:** Strong emphasis on dependency mapping (PKI, vendors, HSMs) and crypto-agile architectures to reduce systemic migration risk.

Canada

- **Centralized federal roadmap:** ITSM.40.001 provides a single, government-wide PQC migration framework with clear ownership, milestones, and governance.
- **Enterprise readiness over pilots:** Focus on inventory, shared services, and PKI modernization —ensuring whole-of-government resilience, not siloed experimentation.

China

- China has demonstrated world leadership in quantum communications with operational space-based + fiber QKD networks, including intercontinental demonstrations, giving China real-world quantum-secure communications capability today.
- **Sovereign cryptography strategy:** National program to develop indigenous PQC algorithms and standards, reducing reliance on Western cryptographic primitives and standards bodies.

Japan

- **Government-wide PQC mandate:** Cabinet Secretariat guidance targets full government migration by 2035, with explicit attention to long-lived sensitive data.
- **Strong national crypto evaluation pipeline:** CRYPTREC provides structured evaluation and guidance, enabling controlled, trusted adoption of PQC algorithms.

South Korea

- **Integrated national quantum strategy:** PQC migration is embedded within the National Quantum Strategy, aligning defence, telecom, and government systems.
- **Operational hybrid deployments:** Active deployment of QKD + PQC hybrid networks across government and telecom infrastructure, moving beyond theory into production systems.

Australia

- **Hard deprecation signal:** ASD mandates cessation of traditional asymmetric cryptography by 2030, one of the strongest enforcement positions globally.
- **Risk-driven prioritization:** Focus on high-impact systems and long-confidentiality data, tightly coupled to national security policy via the ISM.

France

- **Security-assured PQC adoption:** ANSSI links PQC (often hybrid) adoption to formal certification and security visas, ensuring implementation quality.
- **Pragmatic hybrid approach:** Encourages hybrid classical-PQC schemes to balance near-term security with operational stability.

Germany

- **Early migration imperative:** BSI guidance frames PQC transition as unavoidable and urgent, pushing organisations to act before cryptographic failure.
- **Risk-management driven execution:** Emphasis on crypto-agility, system classification, and phased migration rather than wait-and-see.

Singapore

- **Operational readiness tooling:** Introduction of a Quantum-Safe Handbook and Quantum Readiness Index (QRI) turns policy into measurable action.
- **Whole-of-ecosystem approach:** Targets government, CII, and industry together to reduce weakest-link risk in national digital infrastructure.

Related Links

1. https://postquantum.in/
2. https://www.tec.gov.in/pdf/TR/Final%20technical%20report%20on%20migration%20to%20PQC%2028-03-25.pdf
3. https://www.ncsc.gov.uk/pdfs/guidance/pqc-migration-timelines.pdf
4. https://www.ncsc.gov.uk/pdfs/whitepaper/next-steps-preparing-for-post-quantum-cryptography.pdf
5. https://www.ncsc.gov.uk/pdfs/whitepaper/quantum-networking-technologies.pdf
6. https://www.bis.org/publ/bppdf/bispap158.pdf
7. https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
8. https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf
9. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf
10. https://csrc.nist.gov/pubs/ir/8547/ipd
11. https://postquantum.com/
12. https://www.cyber.gc.ca/sites/default/files/itsm.40.001-migration-post-quantum-cryptography-government-canada-e.pdf
13. https://arxiv.org/abs/2505.15917
14. https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/mas-quantum-advisory/mas-quantum-advisory.pdf
15. https://www.cyber.gov.au/business-and-government/cyber-security-frameworks/ism/cybersecurity-guidelines/guidelines-for-cryptography
16. https://www.gsma.com/newsroom/post-quantum-government-initiatives-by-country-and-region/
17. https://thequantuminsider.com/2025/03/14/china-established-quantum-secure-communication-links-with-south-africa/
18. https://blog.cloudflare.com/you-dont-need-quantum-hardware/
19. https://epjquantumtechnology.springeropen.com/articles/10.1140/epjqt/s40507-025-00350-5
20. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/when%20and%20how%20to%20prepare%20for%20post%20quantum%20cryptography/when-and-how-to-prepare-for-post-quantum-cryptography.pdf
21. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci
22. https://www.cert-in.org.in/
23. https://www.cyber.gov.au/business-government/secure-design/planning-for-post-quantum-cryptography
24. https://isomer-user-content.by.gov.sg/36/949031c3-6734-4d33-985e71331fa8ade4/Draft%20for%20Public%20Consultation%20-%20Quantum%20Readiness%20Index%20(Oct%202025).pdf
25. https://isomer-user-content.by.gov.sg/36/11227d39-4350-4ded-9046-d62f99f561ab/Draft%20for%20Public%20Consultation%20-%20Quantum-Safe%20Handbook%20(Oct%202025).pdf

28. https://bughunters.google.com/blog/4625466008862720/google-s-commitment-to-a-quantum-safe-future-why-pqc-is-google-s-path-forward-and-not-qkd
29. https://www.gsma.com/newsroom/post-quantum-government-initiatives-by-country-and-region/

Country-Specific Guidelines:

Please refer to: https://postquantum.in/observatory for most up-to-date information on several countries' guidelines.

United States:

1. NSM-10 and the Transition to Post-Quantum Cryptography (https://csrc.nist.gov/csrc/media/Presentations/2024/u-s-government-s-transition-to-pqc/images-media/presman-govt-transition-pqc2024.pdf
2. Promoting United States Leadership in Quantum Computing While Mitigating Risk to Vulnerable Cryptographic Systems (May 4, 2022) (https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf)
3. The Commercial National Security Algorithm Suite 2.0 (https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/1/CSI_CNSA_2.0_FAQ_.PDF)
4. Transition to Post-Quantum Cryptography Standards (https://csrc.nist.gov/pubs/ir/8547/ipd)

Europe (European Union):

1. A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography)
2. European Quantum Communication Infrastructure (EuroQCI) - (https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci)

United Kingdom:

1. Timelines for Migration to Post-Quantum Cryptography (NCSC UK) - (https://www.ncsc.gov.uk/guidance/timelines-for-migration-to-post-quantum-cryptography)

Canada:

1. Roadmap for the Migration to Post-Quantum Cryptography for the Government of Canada (ITSM.40.001) (https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm4000)
2. Preparing for Quantum-Resistant Cryptography – Government of Canada (https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/quantum-computing/preparing-quantum-resistant-cryptography.html)

China:

1. Satellite-based entanglement distribution over 10,000 km (China–South Africa QKD), Nature Quantum Information (https://www.nature.com/articles/s41534-025-01089-8)
2. Next-generation Commercial Cryptographic Algorithms Program (ICCS, China) (https://www.niccs.org.cn/niccs/Notice/pc/content/content_1937428197396713472.html)

Japan:

1. Interim Summary on Migration to Post-Quantum Cryptography for Government Systems (Cabinet Secretariat, Japan) (https://www.nisc.go.jp/pdf/policy/general/quantum_crypto_interim_summary.pdf)
2. CRYPTREC Report 2022 (Japan Cryptographic Evaluation Committee) (https://www.cryptrec.go.jp/en/report.html)

South Korea:

1. Korea's National Quantum Strategy (2023) (https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&bbsSeqNo=42&nttSeqNo=839)
2. Nationwide Quantum-Safe Network Deployment (Hybrid QKD + PQC) (https://www.idquantique.com/idq-korea-quantum-safe-network/)

Australia:

1. Australian Signals Directorate – Preparing for Post-Quantum Cryptography (https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/preparing-post-quantum-cryptography)

France:

1. ANSSI – Post-Quantum Cryptography: Recommendations and Perspectives (https://www.ssi.gouv.fr/en/publication/post-quantum-cryptography-recommendations-and-perspectives/)

Germany:

1. BSI – Quantum-Safe Cryptography and Migration to PQC (https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Kryptografie/Quantensichere-Kryptografie/quantensichere-kryptografie_node.html)

Singapore:

1. CSA Singapore – Quantum-Safe Handbook & Quantum Readiness Index (QRI) (https://www.csa.gov.sg/Newsroom/Press-Releases/2023/CSA-Launches-Quantum-Safe-Handbook)

Cross-cutting / Comparative:

1. GSMA – Post-Quantum Government Initiatives by Country and Region (https://www.gsma.com/newsroom/post-quantum-government-initiatives-by-country-and-region/)

विज्ञान एवं प्रौद्योगिकी विभाग
DEPARTMENT OF
SCIENCE & TECHNOLOGY

National Quantum Mission

Annexure D

List of Overall Contributors

Task Force Members

Dr. Rajkumar Upadhyay
CEO, C-DOT
Chairman, Task Force

Prof. Manindra Agrawal
Director, IIT Kanpur
Co-Chairman, Task Force

Sh. G. Narendra Nath
Joint Secretary, NSCS

Ms. Divya Sharma
Director, NSCS

Ms. Sheena Rani R
DS&DG(MED&CoS), DRDO

Dr. Rakesh Kaur
Adviser/Scientist G, O/o PSA

Sh. Kamal Kr. Agarwal
DDG (FA), TEC, DoT

Sh. Vinod Kumar
DDG (QT), TEC, DoT

Sh. Vinayak Godse
CEO, DSCI

Prof. Ajay Singh
Professor of Practice, RIMSR

Prof. Venu Gopal A
Director, CSIR-NPL

Sh. Saravade Nand Kumar
Former CEO, ReBIT

Task Force Members

Sh. Aashish Banati
Deputy Controller, CCA-MeitY

Sh. Sanjay Bahl
DG, CERT-In & CCA

Sh. Avneesh Pandey
ED, SEBI

Sh. Pravin Bhavsar
DGM, RBI

Dr. Anil Prabhakar
Professor, IIT Madras

Dr. Prem Laxman Das
HoD, SETS, Chennai

Sh. Sunil Gupta
Co-founder and CEO,
QNu Labs

Sh. Nilesh Dhande
CEO, Fortytwo42 Labs

Dr. J. B.V. Reddy
Head, Quantum Technology
Cell, NQM-DST

Sh. Anurag Mishra
Scientist D, NQM-DST

Dr. Swati Rawal Dang
Scientist D, NQM-DST

Sh. Joynarayan Mukherjee
Scientist C, NQM-DST

Sub-Groups Contributors

S. No	Name	Designation
1	Sh. Atul Kumar Gupta, Scientist G	C-DOT
2	Sh. Teja Chintalapati, Head – Innovation	DSCI
3	Sh. Dhanesh Goel, Director	TEC, DoT
4	Sh. A K Upadhyay, Scientist G	STQC-MeitY
5	Ms. Kamini Malhotra, Scientist G	SAG-DRDO
6	Sh. Prashant Chugh, Scientist F	C-DOT
7	Sh. Ravindra Barlingay, CEO	IITM CDOT Samgnya Technologies Foundation
8	Sh. Venkata Rama Raju Challe, Director (QT-I)	TEC, DoT
9	Dr. K K Soundra Pandian, Scientist E	CCA, MeitY
10	Sh. Gireesh Kumar N, CEO	AvinyaSQ Technologies Pvt Ltd
11	Dr. N. Subramanian, Executive Director	SETS, Chennai
12	Dr. V. Natarajan, Scientist E and HoD, Quantum Security Research Group	SETS, Chennai
13	Dr. Goutam Paul, Professor	ISI Kolkata
14	Dr. Rajan M A, Principal Scientist, Head, Cyber Security and Privacy Research	TCS
15	Sh. Rakesh Goyal, Director	TEC, DoT
16	Sh. B Srinivas Goud, Scientist E	NTRO
17	Ms. Astha Lakshmi J, Scientist E	NTRO
18	Dr. Satya Kesh Dubey, Sr Principal Scientist	CSIR-NPL
19	Sh. R C Sharma, Director	DoT
20	Sh. Dharmesh Makwana, Joint Advisor	TRAI

Sub-Groups Contributors

S. No	Name	Designation
21	Sh. Amul Madan, Sr. Consultant	TRAI
22	Sh. Rajiv Memani, President	CII
23	Sh. Swaminathan Iyer, Strategic Initiatives	Fortytwo42 Technology Innovations Pvt Ltd
24	Lt. Col. Mohit Judge, JCES	IDS, MoD
25	Sh. Sabyasachi Mandal, Senior Research Engineer	C-DOT
26	Sh. Ashok Kumar, DDG-SRI	DoT
27	Sh. Sailendra Kumar Verma	Bureau of Indian Standards
28	Dr. M. Sethumadhavan, Professor	Amrita Vishwa Vidyapeetham
29	Dr. K.V. Lakshmy, Associate Professor	Amrita Vishwa Vidyapeetham
30	Dr. Prabhakar Krishnan, Research Scientist	Amrita Vishwa Vidyapeetham
31	Dr. Vijay S. Rao, Researcher	LTIMindtree
32	Sh. Anand Shankar, Chief GM	Power Grid Corporation of India Limited
33	Ms. Mridusmita B Goswami, Assistant General Manager	SEBI
34	Sh. Ramesh Gurram, Chief Information Security	Bombay Stock Exchange
35	Ms. Madhavi Purandare, Joint General Manager	ICICI Bank
36	Sh. Harsha Saripalli, Assistant General Manager	Reserve Bank of India
37	Ms. Priya Sharma, Senior Associate – Strategy & Insights	DSCI
38	Sh. Mayank Wadhwa, Senior Associate - Cyber Security Technology	DSCI

Sub-Groups Contributors

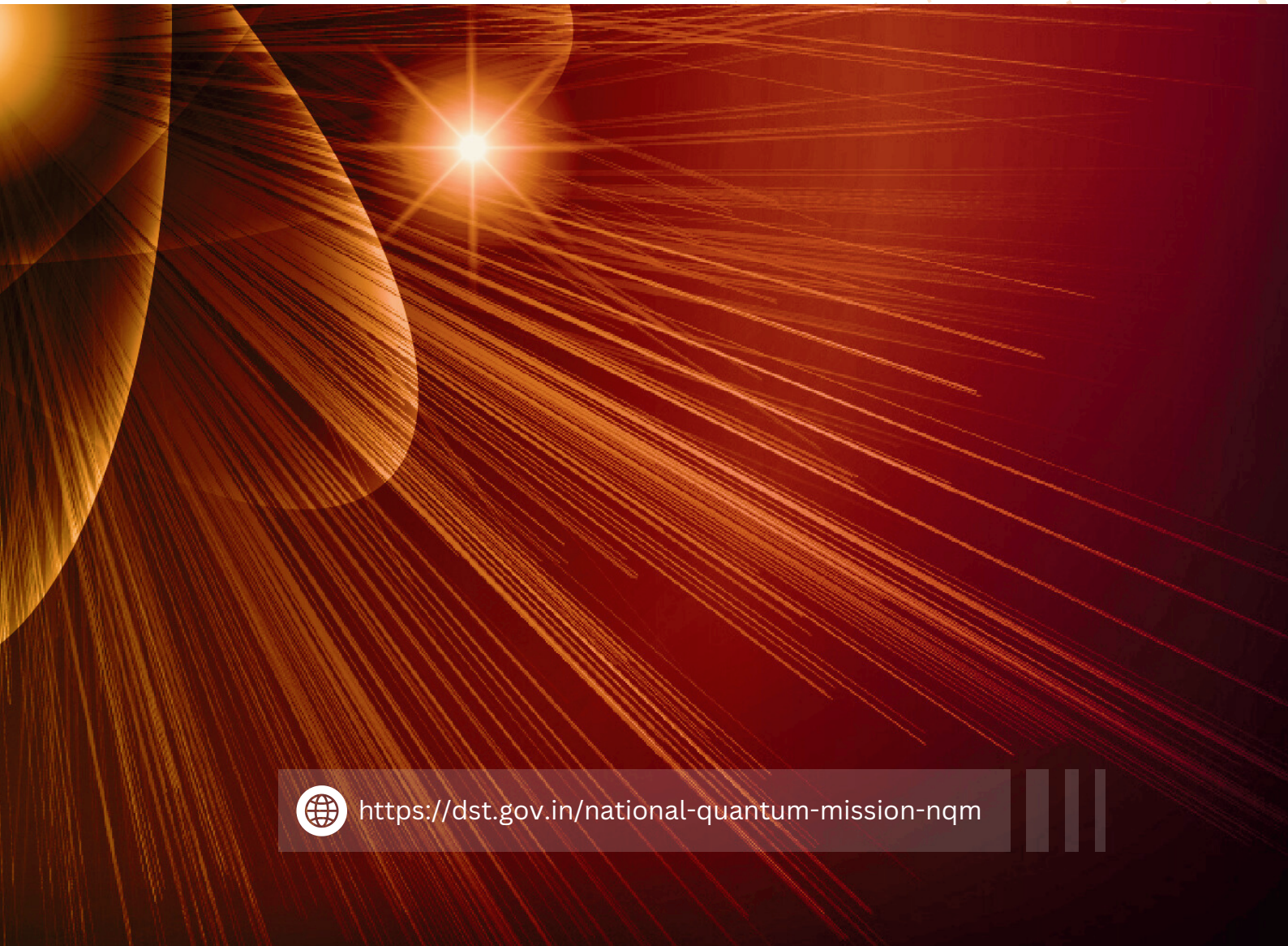
S. No	Name	Designation
39	Sh. Sridhar CV, Mission Director	Amaravati Quantum Valley
40	Col. Sai Shankar, Founder	QClairvoyance Quantum Labs Pvt Ltd
41	Sh. Dinesh Rajpal, General Manager	NETWEB Technologies
42	Dr. Vipin Rathi, Assistant Professor	University of Delhi
43	Sh. Rajesh Kumar Krishnan, Vice President	SVP-INNOVATION, QNu Labs
44	Ms. Poonam Kumari, ADET	TEC, DoT
45	Sh. Arka Mukherjee, Scientist E	C-DOT
46	Sh. Aditya Vyas	CEO, QMD Foundation, NQM
47	Dr. Jagrati Dwivedi	Technology Manager, QMD Foundation, NQM
48	Bhavya Chojar	Innovation, DSCI

विज्ञान एवं प्रौद्योगिकी विभाग
DEPARTMENT OF
SCIENCE & TECHNOLOGY
सत्यमेव जयते

National Quantum Mission

Department of Science & Technology

National Quantum Mission



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