D DRISHTI-PQC

See your crypto before quantum does.

A TLS and post-quantum readiness assessment platform for Punjab National Bank — built to make cryptographic posture visible, measurable, and audit-ready.

TLS / ML-KEM scanning | PQC readiness grading | RBI-mapped evidence | On-premises capable

BUILT BY
PNB · CISD-DR

ASSESSED AGAINST
RBI · NIST · ISO · CERT-In

DOCUMENT
Capabilities Overview

THE PROBLEM WE BUILT FOR

Quantum computers will break today's encryption. Banks need to know where they stand.

The cryptography that protects banking traffic today — RSA and elliptic-curve key exchange — is vulnerable to a sufficiently powerful quantum computer. Data captured now can be stored and decrypted later. Migration to post-quantum cryptography is no longer theoretical: the standards are published, and the regulators are watching.

2024	2030–35	Now
NIST finalised the first post-quantum standards (FIPS 203/204/205)	NIST timeline to deprecate & disallow RSA / ECC	"Harvest-now, decrypt-later" makes today's traffic a future liability

DRISHTI-PQC answers one question for every internet-facing asset: is this endpoint ready for the post-quantum era — and if not, how far off is it?

It does this the way a bank's own assurance team would want it done: every finding derived from what was actually observed on the wire, every grade showing its own arithmetic, and every result exportable as evidence mapped to the frameworks PNB is assessed against.

A note on language

Throughout this platform and its reports, capabilities are described as **"aligned to"** and **"assessed against"** recognised standards — never "certified" or "compliant." DRISHTI-PQC is an assessment instrument; formal certification rests with the accredited bodies that issue it.

THE PLATFORM AT A GLANCE

One workspace for cryptographic posture.

DRISHTI-PQC discovers a bank's internet-facing footprint, probes each asset's transport security, grades it, and tracks how it changes over time — organised into a single toolkit.

Asset discovery

Finds public subdomains across Certificate Transparency, multiple passive sources, and an optional subfinder pass — then sorts them into alive, stale and dead.

TLS / PQC scan

Probes each host for TLS 1.3, the hybrid post-quantum key exchange (X25519MLKEM768), cipher suites and HTTP/3 — and reports the exact named groups observed.

Posture grading

Turns observed facts into an SSL-Labs-style grade with fully visible math — no opaque scoring, every point accounted for.

Certificate health

Surfaces issuer, validity window, days-to-expiry, key strength and chain status, flagged red / amber / green.

DNS & email security

Checks DNS hygiene and the full email-authentication stack — SPF, DKIM, DMARC, MTA-STS, TLS-RPT and BIMI.

Change tracking

Records every scan forever and diffs them, so a grade drop, a new finding or an expiring certificate is caught the week it happens.

Per-bank workspaces, bank-wide rollup

Assets are organised into bank workspaces, each with its own posture dashboard — a certificate-grade breakdown, PQC-readiness split, a ranked migration worklist, and an evidence export. Filters stack (grade × PQC-readiness × reachability) so any view becomes an actionable list.

WHAT MAKES IT DIFFERENT

The grade shows its work.

Most scanners hand you a letter and ask you to trust it. DRISHTI-PQC shows the arithmetic behind every grade, so an auditor can reproduce it and a network owner can argue with it.

GRADE SCALE

Each asset's score is built from observed transport facts, not assumptions:

- `protocol support` — TLS 1.3 present, legacy versions absent
- `key exchange` — classical, or hybrid post-quantum (ML-KEM)
- `cipher strength` — forward secrecy, AEAD suites, key sizes
- `certificate` — validity, key strength, chain integrity
- `findings` — each observed weakness deducts a stated amount

The PQC-readiness signal is reported separately and exactly: the platform names the actual negotiated group (e.g. `X25519MLKEM768`) rather than inferring "quantum-safe" from a version number.

Observed only. Unreachable fields stay blank — never guessed

Severity never contradicts the grade

CVEs attached only where the observed condition implies them

The migration worklist

From the same data, DRISHTI-PQC produces a ranked "what to fix next" list: reachable assets that are not yet PQC-ready, ordered by exposure (TLS grade and score) and open findings. Every row states *why* it ranks where it does — turning posture into a defensible action plan.

Transparency is the product. A grade you can audit is a grade you can defend to a regulator.

USING THE PLATFORM

From a domain to an evidence pack in five steps.

1. **Discover the footprint**
   Enter a root domain in Asset Inventory and confirm authorisation. The platform unions Certificate Transparency, five passive sources and an optional subfinder pass, then probes reachability — showing live progress and an honest per-source breakdown.

2. **Save assets into a bank workspace**
   Promote discovered hosts into the relevant bank. Discovery, saving and scanning are deliberately separate, intentional actions — nothing is auto-chained.

3. **Scan for posture**
   Run a deep scan. Each host is probed for TLS version, key exchange (including ML-KEM), cipher suites, certificate facts, security headers and HTTP/3 — and graded with visible math.

4. **Read the dashboard, work the list**
   The workspace shows grade and PQC-readiness breakdowns as clickable filters, a ranked migration worklist, and a certificate-expiry view. Stack filters to isolate exactly the assets that need attention.

5. **Export the evidence**
   Export a per-feature Excel workbook — filtered to the current view if you wish — with findings, grades and standards citations in the footer, ready for an assurance file or a regulator's request.

Built for where banks actually run

DRISHTI-PQC deploys to the cloud or fully on-premises. Because some internal banking assets are only reachable from inside the network, the platform is designed to run from the right vantage point — an on-premises deployment sees what an external scanner cannot. Where a host can't be reached, the result is recorded honestly as unreachable, never fabricated.

STANDARDS ALIGNMENT

Assessed against the frameworks that matter to Indian banking.

Each capability is mapped to the specific regulatory and technical standard it supports. Citations are current as of June 2026.

RBI Master Direction on IT Governance

RBI/2023-24/107
DoS.CO.CSITEG/SEC.7/31.01.015/2023-24

Issued 7 November 2023, effective 1 April 2024. Across seven chapters and 32 paragraphs, it mandates IT & information-security risk management, vulnerability assessment, and assurance practices for regulated entities.

How DRISHTI-PQC aligns: continuous external-surface assessment, cryptographic risk identification, and audit-ready evidence support the Direction's IT/InfoSec risk-management and assurance expectations (Ch. IV–V).

NIST Post-Quantum Cryptography Standards

FIPS 203 · 204 · 205
effective 14 Aug 2024

FIPS 203 (ML-KEM, from CRYSTALS-Kyber) standardises post-quantum key encapsulation, replacing RSA/ECDH key exchange; FIPS 204 (ML-DSA) and 205 (SLH-DSA) cover signatures. NIST IR 8547 sets the 2030–2035 timeline to deprecate and disallow RSA/ECC.

How DRISHTI-PQC aligns: detects and names ML-KEM hybrid key exchange (X25519MLKEM768) on the wire, grades PQC readiness, and ranks migration — directly operationalising the FIPS 203 transition.

NIST Cybersecurity Framework 2.0

NIST CSWP 29
26 Feb 2024

The first major revision since 2014 adds a sixth *Govern* function and extends scope to all organisations. Voluntary and outcome-based; no certification is issued.

How DRISHTI-PQC aligns: maps to **Identify** (asset & crypto inventory), **Protect** (transport hardening) and **Detect** (change tracking) — the continuous-assessment outcomes CSF 2.0 describes.

ISO/IEC 27001:2022

ISMS · 93 Annex A controls

The international information-security management standard; the 2022 revision restructured Annex A into 93 controls across four themes. Certifiable through third-party audit.

How DRISHTI-PQC aligns: generates evidence supporting Annex A technological controls — cryptography, secure configuration and monitoring of network services.

CERT-In Directions, 2022

No. 20(3)/2022-CERT-In
28 Apr 2022 · s.70B(6), IT Act 2000

Mandates 6-hour cyber-incident reporting and 180-day ICT log retention within India for covered entities — the operational backdrop for security tooling deployed in Indian banking.

How DRISHTI-PQC aligns: retains every scan run indefinitely with timestamped change history, supporting the evidence-retention and reporting posture CERT-In expects.

Standard titles, reference numbers and dates verified against primary and authoritative sources, June 2026. DRISHTI-PQC supports alignment and evidence generation; it does not itself confer certification or a statement of compliance.

IN SUMMARY

Posture you can see. Evidence you can defend.

- **Visible grading math** — every score reproducible, nothing opaque.
- **Exact PQC reporting** — names the negotiated ML-KEM group, never infers it.
- **Honest by construction** — unreachable and unknown values stay blank, never fabricated.
- **Bank-wide posture** — per-asset detail rolls into a workspace dashboard and ranked worklist.
- **Standards-mapped evidence** — exports cite the frameworks PNB is assessed against.
- **Deploys where banks run** — cloud or fully on-premises, for assets external scanners can't see.

THE BOTTOM LINE

A transparent, trustworthy alternative to black-box scanners — purpose-built so Punjab National Bank can see its cryptographic posture, prioritise the post-quantum migration, and produce the evidence a regulator will accept.

D

DRISHTI-PQC

by Punjab National Bank · Cyber & Information Security Division — Disaster Recovery