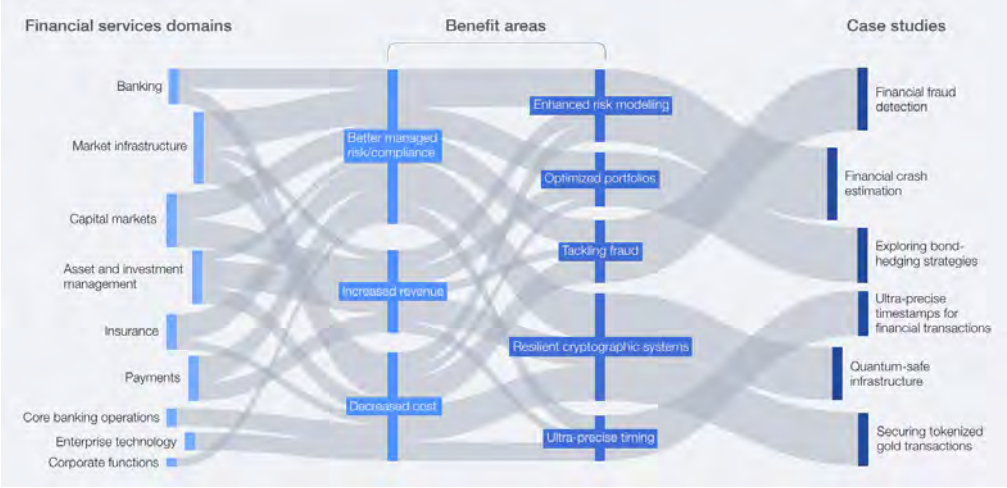
Q→NU

Banking & Financial Services (BFSI) Quantum Threat Intelligence Report

Critical Threat Landscape

Immediate Quantum Risks (2024-2025):

- **92% of BFSI leaders worry about quantum risks** and "harvest now, decrypt later" attacks. (Source: Deloitte Insights)
- **NIST standardised new quantum-resistant algorithms in August 2024** and have defined the i**mplementation window between 2025** (Aggressive) to **2030 (Pessimistic)**
- **NIST's transition roadmap** clearly states that **RSA-based key establishment** (and digital signatures at 112-bit strength) is slated to be **deprecated after 2030** and **disallowed after 2035. (Source: appviewx)**
- The **National Quantum Mission (NQM)** is **establishing a task force to help banks adopt quantum-safe technologies** for cybersecurity, financial modelling, and data analysis **(Source: Reserve Bank Innovation Hub)**
- **Q-Day** when quantum computers break classical security—will cause major losses and compliance breaches, making early Quantum Communication adoption crucial. **The $1B market in 2023 is growing rapidly at a 22–25% CAGR.**
- The U.S. views quantum computing as a national security priority, with advisor Jake Sullivan naming it a key technology the government aims to safeguard over the next decade. **(AOShearman)**
- Total Quantum Communication is projected to reach **$10.5B–$14.9B** by 2035 with a CAGR of 22–25% **(McKinsey, June 2025)**. India's BFSI cybersecurity market is expected to reach $3.5B by 2027. **(Source: Research and Markets)**
- SEBI's CSCRF addresses emerging threats like quantum-computing **("harvest-now, decrypt-later")** with guidance on cryptographic inventory and post-quantum readiness. It sets a unified framework for India's financial stability, requiring Regulated Entities to meet five resilience goals and submit annual Cyber Capability Index reports. **(RBI, Apr 2025)**
- India launched the first Digital Threat Report 2024 for BFSI, highlighting the urgency of an integrated approach.



Mapping of financial services domains to benefits and case studies **(source: WEF, July 2025)**

RBI Tightens Cyber & Data Sovereignty Norms – Mandates '.bank.in' domains by Oct 31, 2025 **(Source: RBI Circular, 2025)**; it also mandated data localisation, cybersecurity audits, and operational resilience under ORMF to protect India's digital sovereignty of sensitive financial data and bolstering public trust in India's rapidly evolving digital financial landscape. **(RBI, Apr 2025)**

65% of financial organisations reported experiencing a ransomware attack in 2024, up from 34% in 2021. [Source: **Cognizant**]

Quantum technologies are reshaping finance from fraud detection to encryption and risk forecasting.

In 2025, MeitY launched "Transitioning to Quantum Cyber Readiness" whitepaper calling upon strategic sectors to identify vulnerable areas in national security infrastructure and financial transactions. [Source: **PIB**]

Business Impact

- **Revenue at Risk:** ₹2.3 trillion Indian banking sector vulnerable to quantum attacks
- **Customer Trust:** Complete compromise of encrypted customer data and transactions
- **Regulatory Penalties:** Non-compliance fines estimated at ₹500-1000 crores per major bank
- **Competitive Disadvantage:** Early adopters gain 40% advantage in quantum-safe operations

Timeline Urgency

- **Q-Day Prediction:** 2025-2032 for cryptographically relevant quantum computers; though some analyses suggest it could be as early as 2025.
- **Preparation Window:** 5-7 years to migrate the entire BFSI infrastructure
- **Regulatory Deadline:** 2024-2026 for quantum-safe compliance mandates

Key Statistics

- **87%** of Indian banks still use quantum-vulnerable RSA/ECC encryption
- **₹45 billion** daily UPI transactions at risk of quantum decryption
- **23%** increase in BFSI cyber incidents in 2024 vs 2023

Immediate Actions Required

- **Quantum Risk Assessment**: Audit all encryption systems within 90 days. Identify all data and systems that rely on current encryption protocols, such as RSA, ECC. Evaluate the quantum vulnerability of your organisation.
- **Pilot Deployment:** Start quantum-safe protocols for critical systems, i.e. start transitioning to PQC (post quantum cryptography) NOW, as the process takes 5-7 years for an enterprise and delaying action allows adversaries to collect encrypted data now for future decryption.
- **Regulatory Alignment:** Prepare for upcoming RBI quantum security guidelines. Also, check the new guidelines from NIST and other regulatory bodies of countries.
- **Vendor Evaluation:** Assess the quantum readiness of your vendors and service providers. Select the RIGHT quantum security partners before market saturation.

Other Sources:

- World Economic Forum Quantum Security Report (2024)
- CERT-In Comprehensive Cyber Security Audit Policy Guidelines
- CERT-In Digital Threat Report 2024

Q→NU
Proactively™
Quantum

Tomorrow's Quantum Security, Today

Scan for more details

Registered Office:

QuNu Labs Private Limited, Centenary Building, 2nd Floor, East Wing, #28 MG Road Bengaluru - 560025

CIN: U72900KA2016PTC096629

India USA Australia Global