Your PQC Risk Assessment Report

Generated on February 19, 2026

France PQC Migration Timeline

Medium Risk

Your organization in the Finance & Banking sector has a quantum risk score of 53/100 (medium). You are currently using 4 quantum-vulnerable cryptographic algorithms that require migration to post-quantum alternatives. Given your high data sensitivity, "Harvest Now, Decrypt Later" attacks represent an immediate threat to long-lived data. Your migration has already begun, which significantly reduces your risk.

Risk Breakdown

Quantum Exposure 79/100

Migration Complexity 49/100

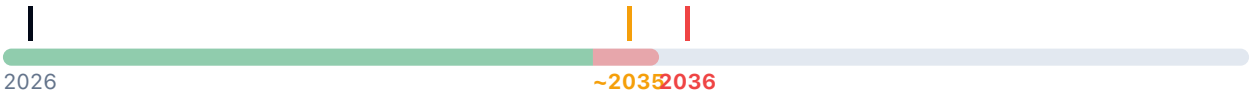
Regulatory Pressure 28/100

Organizational Readiness 40/100

Executive Summary

Your Finance & Banking organization faces a medium quantum risk (53/100). 4 algorithms require migration: 4 moderate migrations. Data persists 1 year beyond the estimated quantum threat horizon, making HNDL attacks an active concern. Migration is underway, reducing overall risk.

HNDL Risk Window



Safe zone At risk

Your data persists 1 year beyond the estimated quantum threat horizon. HNDL attacks are an active concern.

Current	Vulnerable?	PQC Replacement	Effort	Scope	Notes
ECDSA P-256	⚠ Yes	ML-DSA-44	medium	Moderate	Broken by Shor's algorithm. Used widely in TLS and code signing.
RSA-2048	⚠ Yes	ML-KEM-768 / ML-DSA-65	medium	Moderate	Broken by Shor's algorithm. NIST targets deprecation by 2030.
RSA-4096	⚠ Yes	ML-KEM-1024 / ML-DSA-87	medium	Moderate	Broken by Shor's algorithm. Larger key provides no quantum resistance.
ECDSA P-384	⚠ Yes	ML-DSA-65	medium	Moderate	Broken by Shor's algorithm.

Compliance Impact

PCI DSS

No PQC mandate yet

Deadline: No explicit PQC timeline yet
Payment card industry will follow NIST guidance. Monitor for updates.

SWIFT CSP

No PQC mandate yet

Deadline: Annual
Annual security attestation required for SWIFT network participants.

Recommended Actions

1. Migrate 4 quantum-vulnerable algorithms to PQC equivalents.
   IMMEDIATE MEDIUM EFFORT

2. Migrate TLS endpoints to hybrid PQC key exchange (ML-KEM + X25519).
   IMMEDIATE MEDIUM EFFORT

3. Implement hybrid PQC encryption for data-at-rest to guard against HNDL attacks.
   IMMEDIATE HIGH EFFORT

4. Evaluate PQC-ready libraries and tools for your technology stack.
   SHORT-TERM LOW EFFORT

5. Build PQC awareness across engineering and leadership teams.
   LONG-TERM LOW EFFORT

Finance & Banking Threat Landscape

Threat ID	Criticality	Description	Crypto at Risk	PQC Replacement
CRYPTO-001	Critical	Bitcoin ECDSA transaction hijacking: Approximately $718B in quantum-vulnerable P2PK addresses with exposed public keys (price-dependent estimate). Early P2PK addresses including Satoshi's estimated 1.1M BTC are permanently vulnerable as public keys are exposed on-chain. P2PKH addresses are protected until first spend.	secp256k1 ECDSA	P2QRH BIP proposal, Lamport signatures, hash-based migration
CRYPTO-002	Critical	Ethereum Foundation PQC initiative: Dedicated post-quantum security team established January 2026 with $2M in research prizes. Active development of account abstraction and Verkle tree migration paths. All Ethereum accounts that have transacted expose public keys making them quantum-vulnerable via secp256k1 ECDSA and BLS12-381.	secp256k1 ECDSA, BLS12-381, keccak256 address derivation	Account Abstraction (EIP-4337), Verkle Trees, quantum-resistant signature schemes
CRYPTO-003	Critical	Blockchain HNDL permanence risk: Federal Reserve research confirms distributed ledger networks face permanent data privacy risks from harvest-now-decrypt-later attacks even with future PQC deployment. On-chain transaction data is immutable — encrypted data harvested today remains permanently exposed once CRQCs arrive.	RSA-2048, ECDSA, ECDH in blockchain protocols, BLS signatures	ML-KEM-1024, ML-DSA-87, SLH-DSA, validator PQC authentication
CRYPTO-004	Critical	Cryptocurrency custody HSM quantum vulnerability: Institutional custody solutions managing billions in digital assets rely on secp256k1 ECDSA keys stored in HSMs. NIST PQC standardization	secp256k1 ECDSA custody keys, RSA/ECDH key wrapping, HSM root keys	ML-KEM-1024, ML-DSA-87, PQC-enabled custody HSMs

		identifies ECDSA as quantum-vulnerable. Custody HSM vendors face multi-year FIPS 140-3 recertification timelines for PQC-enabled modules, creating a gap between threat emergence and mitigation availability.		
FIN-001	Critical	BIS Project Leap quantum-safe payment integration: Central banks implementing quantum-safe wholesale CBDC settlement. Phase 2 launched July 2025 with Bank of Italy, France, Germany, Nexi, and SWIFT testing hybrid PQC on TARGET2 real-time gross settlement for cross-border transactions worth trillions daily.	Wholesale CBDC infrastructure, cross-border settlement, RSA-2048, ECDSA, TLS legacy	ML-KEM-1024, ML-DSA-87, hybrid TLS 1.3, HQC
FIN-002	Critical	Harvest Now Decrypt Later (HNDL) attacks targeting long-lived financial data including transaction records and settlement logs. Federal Reserve research confirms cryptocurrency networks face permanent data privacy risks from HNDL even with future PQC deployment. Financial records retained for regulatory compliance spanning decades are prime targets.	RSA-2048, ECDSA, ECDH, ECC-256/384	ML-KEM-1024, ML-DSA-87, SLH-DSA, AES-256
FIN-003	High	G7 Cyber Expert Group PQC roadmap: January 2026 statement coordinated by U.S. Treasury and Bank of England establishes G7-wide framework for financial sector quantum-safe migration. Calls for cryptographic inventory, vendor roadmap alignment, and coordinated transition planning across G7 financial systems.	G7 financial infrastructure, cross-border payment systems, correspondent banking TLS	ML-KEM, ML-DSA, hybrid implementations, coordinated G7 PQC standards
FIN-004	Critical	HSM backup key extraction vulnerability: Master encryption keys wrapped with RSA in HSM backup archives become recoverable with quantum computers, exposing entire key	RSA key wrapping in HSM backups, ECDH key agreement, archived master keys	ML-KEM-1024 per NIST SP 800-227, AES-256-GCM key wrapping

		hierarchies protecting decades of financial data. NIST SP 800-227 (September 2025) provides formal KEM guidance for transitioning key wrapping to quantum-safe mechanisms.		
FIN-005	High	FS-ISAC PQC migration urgency warning: Financial Services Information Sharing and Analysis Center (September 2025) warns that financial sector organizations have not defined or allocated resources for quantum-resistant migration, compressing transition into unrealistically short timeframes. Without immediate action, roadmap collapse by 2030 compliance deadlines is likely.	RSA, ECC, TLS 1.2/1.3 key exchange, PKI certificates across financial infrastructure	ML-KEM, ML-DSA, hybrid implementations, immediate cryptographic inventory
INS-001	High	NAIC Insurance Data Security Model Law (MDL-668) quantum exposure: Adopted 2017 and enacted in 25+ states, requires encryption of nonpublic information in transit and at rest. Actuarial models, claims history spanning decades, and underwriting algorithms represent long-lived sensitive data prime for HNDL attacks.	RSA/ECDSA protecting policyholder data, TLS for claims processing, database encryption	ML-KEM for key exchange, AES-256-GCM, ML-DSA for document signing
INS-002	High	New York DFS cybersecurity regulation (23 NYCRR 500) quantum gap: Requires risk assessment and encryption for financial services including insurance companies. Life insurance and annuity records with 50+ year retention periods are prime HNDL targets. Regulation does not yet address post-quantum cryptography.	Database encryption, policyholder data TLS, claims management systems	PQC-enabled encryption, hybrid TLS 1.3, ML-KEM key management
INS-003	High	Systemic cyber risk to insurance sector: Geneva Association research identifies systemic cyber risk including quantum threats to insurance industry managing	Actuarial model encryption, reinsurance platform crypto, policyholder PII protection	AES-256 with ML-KEM key exchange, ML-DSA for contract signing, crypto-agile platforms

		multi-decade policy data. Life insurance and pension records retain sensitivity for 50+ years. Reinsurance treaties with multi-year duration vulnerable to data manipulation.		
LEG-001	Critical	eIDAS long-term signature vulnerability: EU Regulation 910/2014 Article 25(2) grants qualified electronic signatures legal equivalence to handwritten signatures across 27 EU member states. Property deeds, constitutional documents, and notarial acts require 50-100+ year validity. Quantum signature forgery would retroactively invalidate millions of legally binding documents.	RSA-2048/4096, ECDSA P-256/P-384, SHA-256 in AdES formats (XAdES, PAdES, CAdES)	ML-DSA-65/87, SLH-DSA for long-term archival signatures, XMSS
LEG-002	High	eIDAS 2.0 Digital Identity Wallet quantum risk: Regulation 2024/1183 (entered force May 20, 2024) amends eIDAS to mandate European Digital Identity Wallets for all EU member states. Wallets must support qualified electronic attestations of attributes. Cryptographic protocols underpinning wallet-to-verifier authentication rely on RSA/ECDSA.	ECDSA P-256, RSA-2048, ECDH in wallet authentication, X.509 certificates	ML-DSA-65/87, ML-KEM-768/1024, hybrid signature schemes
LEG-003	High	Qualified timestamp quantum forgery risk: ETSI EN 319 422 governs qualified time-stamp authorities under the eIDAS framework using RFC 3161 time-stamp protocol. Timestamps cryptographically prove document existence at specific moments for legal evidence and IP filings. Quantum-capable adversaries could forge timestamps to backdate contracts or fabricate audit trails.	RSA-2048/4096, ECDSA P-256/P-384 in RFC 3161 timestamp tokens, SHA-256	ML-DSA-65/87, SLH-DSA for long-term timestamp integrity
LEG-004	High	Court electronic evidence	RSA/ECDSA	PQC re-signing

		repudiation risk: As quantum computing advances, defense attorneys may challenge the integrity of digitally signed electronic evidence, arguing signatures could have been forged. This introduces reasonable doubt for any evidence authenticated solely with quantum-vulnerable cryptography. Courts will need to establish new standards for digital evidence admissibility in the post-quantum era.	signatures on court filings, evidence chain of custody, forensic reports	with archival timestamps, SLH-DSA for evidence integrity
PCI-001	Critical	EMV offline authentication quantum vulnerability: EMVCo specifications use RSA as the only approved asymmetric algorithm for offline card authentication (CDA/DDA). Approximately 14.7 billion EMV chip cards in circulation globally (end 2024). Quantum forgery of RSA signatures enables counterfeit card acceptance at any offline-capable terminal.	RSA-1024/2048 in EMV CDA/DDA offline authentication, card personalization keys	ML-DSA hybrid offline authentication, FN-DSA for constrained chip environments
PCI-002	High	PCI DSS 4.0.1 cryptographic gap: PCI DSS requires 'strong cryptography' for cardholder data protection but does not yet mandate post-quantum algorithms. Organizations meeting current PCI compliance may still be quantum-vulnerable. Cryptographic inventory requirements (Req 3/4) do not address PQC readiness assessment.	TLS protecting payment data, RSA/ECDSA certificates, HSM key wrapping for card data	PQC-enabled payment HSMs, hybrid TLS 1.3, ML-KEM for key exchange
PCI-003	High	PIN block encryption quantum vulnerability: Triple-DES DUKPT base derivation keys protecting PIN blocks at millions of payment terminals face quantum compromise. AES-256 DUKPT provides quantum-resistant	3DES DUKPT base derivation keys, RSA key injection, PIN encryption	AES-256 DUKPT, ML-KEM key injection, quantum-safe PIN encryption

	symmetric alternative but terminal hardware replacement required at massive scale.