MARCH 2026
APPLIED QUANTUM

THE APPLIED QUANTUM PQC MIGRATION FRAMEWORK

FINANCIAL SERVICES EXTENSION

Banking, Payments, and Capital Markets *— Industry-Specific Challenges and Framework Adaptations*

Version 1.1 — March 2026

Marin Ivezic

CEO, Applied Quantum

Author, PostQuantum.com

PQCFramework.com | PostQuantum.com | SecureQuantum.com | AppliedQuantum.com

"Start while it's a project, before it's a crisis."

COPYRIGHT AND LICENSE

DISCLAIMER

This extension is provided as professional guidance based on the author's and Applied Quantum's practitioner experience and publicly available standards, regulations, and industry research. It does not constitute legal, regulatory, financial, or compliance advice. Organizations should consult qualified legal counsel, auditors, and regulatory authorities for guidance specific to their jurisdiction, sector, and circumstances.

The regulatory timelines, vendor capabilities, algorithm parameters, and tool categories referenced in this document reflect the state of the PQC landscape as of March 2026. This landscape evolves rapidly. Readers should verify current status against primary sources (NIST, NSA, ETSI, national agencies, vendor documentation) before making implementation decisions.

References to specific vendors, products, or tools are for illustrative purposes and do not constitute endorsement.

NIST IR 8547, referenced throughout for deprecation and disallowance timelines, was an Initial Public Draft as of November 2024 with final publication expected in 2025–2026. Federal agencies and their contractors should reference the final published version when available.

ABOUT THIS DOCUMENT

Document type	Enterprise methodology and practitioner framework
Parent Document	The Applied Quantum PQC Migration Framework — Universal — v1.1 (March 2026)

Intended audience	CISOs, security architects, payment engineers, compliance officers, and program managers in banking, payments, and capital markets
Assumed knowledge	Familiarity with the Universal PQC Migration Framework and its 8-phase lifecycle; working knowledge of payment systems, card networks, and financial messaging standards
Scope	Industry-specific challenges and phase-by-phase framework adaptations for financial services. Not a standalone document — intended to be used alongside the Universal Framework.

HOW TO USE THIS EXTENSION

This document is a companion to the Applied Quantum PQC Migration Framework (Universal). It does not replace the Universal Framework but extends it with financial-services-specific guidance. For each topic, this extension identifies unique sector challenges and then maps specific adaptations to the relevant Universal Framework phase. Readers should have the Universal Framework open alongside this document and cross-reference its phase definitions, maturity indicators, and templates.

ACCOMPANYING RESOURCES

Every aspect of this framework — from executive business cases and cryptographic inventory methodologies to CBOM architecture, hybrid deployment patterns, and vendor governance — has been analyzed in detail on PostQuantum.com over the past 10+ years through practitioner-grounded articles, deep dives, and sector-specific analyses.

The best starting point is the curated Quantum Readiness Starting page: https://postquantum.com/quantum-readiness-starting/ — but readers should also use PostQuantum.com's Search function to surface additional relevant posts that may not be included in that curated list.

Key framework resources, templates, and supporting materials are also published on PQCFramework.com — a dedicated companion site for this framework, drawing on relevant content from PostQuantum.com.

TABLE OF CONTENTS

WHY FINANCIAL SERVICES REQUIRES A SECTOR EXTENSION

The Universal PQC Migration Framework provides a comprehensive 8-phase methodology applicable to any enterprise. Financial services institutions can and should follow that methodology. However, the financial services sector faces a distinct combination of constraints that make PQC migration more complex, more urgent, and more coordination-dependent than in most other industries. These constraints do not invalidate the Universal Framework — they sharpen, extend, and occasionally reorder its guidance.

This section identifies the characteristics that set financial services apart.

Unmatched Cryptographic Density

Financial services is arguably the most cryptography-dense sector in the economy. A single mobile banking session invokes approximately 320 cryptographic function calls before the user even initiates a transaction. A cross-border payment traverses 9+ independent parties and triggers over 30,000 unique cryptographic functions. The interbank payment stack — from customer authentication through SWIFT messaging to central bank RTGS settlement — involves dozens of distinct quantum-vulnerable cryptographic operations, each managed by a different entity with its own upgrade cycle. This density means that cryptographic inventory (Phase 1) and CBOM documentation (Phase 2) are orders of magnitude more complex in financial services than in a typical enterprise.

Multi-Party Coordination as the Binding Constraint

Most enterprises control their own cryptographic estate. Financial institutions do not. A card payment involves the cardholder's device, the merchant terminal, the acquirer, the card network, the issuing bank, one or more payment processors, a clearing house, a

correspondent bank, and a central bank settlement system. Each operates on independent upgrade cycles, with independent vendors, independent certification requirements, and independent risk appetites. Migrating one party's cryptography without coordinating with all counterparties is operationally meaningless — the chain is only as quantum-safe as its weakest link. This makes vendor and supply chain governance (Phase 7) not a supporting activity but a critical-path constraint that must start in Phase 0.

Harvest Now, Decrypt Later as an Active, Quantifiable Threat

Financial data has exceptionally long confidentiality requirements. Cross-border payment flows, correspondent banking records, trade finance documents, and regulatory filings may carry data that remains sensitive for decades. Nation-state adversaries are almost certainly harvesting encrypted financial traffic today for future quantum decryption. The Federal Reserve has explicitly acknowledged this risk in published research. This elevates HNDL from a theoretical concern to an operational imperative that should drive Phase 3 (Risk Scoring) prioritization toward external-facing interfaces and data-in-transit protections.

Hardened Infrastructure That Resists Change

Payment systems are built on purpose-engineered, heavily certified infrastructure: Hardware Security Modules (HSMs) validated to FIPS 140-2/140-3 and PCI PTS standards; smart cards with kilobytes of RAM running on 32-bit processors; message formats (ISO 8583) designed when every byte mattered; and settlement systems where a 200-millisecond latency increase could cascade into systemic risk. This infrastructure cannot be swapped out on a software release cycle — it requires hardware replacement, re-certification, and coordinated cutover across the ecosystem.

The Densest Regulatory Landscape of Any Sector

No other sector faces as many overlapping regulatory and standards bodies with direct or emerging PQC requirements: PCI DSS v4.0 (Requirement 12.3.3 for cryptographic inventories, effective March 2025), the G7 Cyber Expert Group quantum roadmap (January 2026), Europol's Quantum Safe Financial Forum prioritization framework (January 2026), BIS Papers No. 158, the EU Coordinated Implementation Roadmap (2030 deadline for critical financial infrastructure), HKMA's Quantum Preparedness Index (February 2026), MAS advisory guidance, UK NCSC phased targets, and the broader NIST IR 8547 deprecation timeline. Compliance officers need a financial-services-specific

regulatory mapping that the Universal Framework's general alignment table cannot provide.

Systemic Risk Amplification

A quantum-enabled attack on financial infrastructure is not merely an enterprise security incident — it is a systemic event. The Citi Institute's January 2026 analysis, drawing on Hudson Institute modeling, estimated that a quantum attack on a top-five U.S. bank's Fedwire access could cause $2.0–3.3 trillion in indirect economic losses and trigger a six-month recession through cascading liquidity failures. This systemic risk dimension changes the business case calculus in Phase 0 and justifies investment levels that would be difficult to defend in sectors without comparable cascading-failure dynamics.

INDUSTRY-SPECIFIC CHALLENGES

This section details the technical and operational challenges unique to financial services PQC migration. Each challenge is presented with its technical basis, real-world evidence, and the Universal Framework phases it most directly impacts. Section 3 then maps these challenges to specific framework adaptations.

CHALLENGE 1: PAYMENT MESSAGE FORMAT CONSTRAINTS

PQC signature sizes are structurally incompatible with legacy payment message formats. An ML-DSA-44 signature is 2,420 bytes; the ECDSA signature it replaces is 64 bytes — a 37.8× increase. ISO 8583, the binary format underpinning global card payment authorization, caps authentication data fields at approximately 256 bytes. An ML-DSA signature does not fit. ISO 20022, while more extensible, still presented problems in practice: BIS Project Leap Phase 2 found that PQC signatures in ISO 20022 Business Application Headers exceeded expected buffer sizes in TARGET2's message-handling logic.

The implications cascade across every switch, gateway, payment processor, middleware parser, logging system, database schema, and archive that assumes current field sizes. Payment processors that have spent decades optimizing ISO 8583 parsing logic — hardcoding field offsets to shave microseconds — will find those optimizations broken. The X9 Accredited Standards Committee has published a Post-Quantum Cryptography Financial Readiness Needs Assessment covering both ISO 8583 and ISO 20022, but the hard engineering of accommodating larger payloads across thousands of institutions remains ahead.

> **Framework Impact:** Phase 1 (Discovery) must include message format analysis as a distinct inventory track. Phase 3 (Risk Scoring) must weight message-format-constrained systems separately. Phase 5 (Pilots) must include message-format-specific testing with realistic payload sizes.

CHALLENGE 2: SMART CARD AND TERMINAL CONSTRAINTS

Nearly fourteen billion payment cards are in circulation worldwide, most running 32-bit processors at approximately 100 MHz with 48 KB of RAM and no hardware acceleration for PQC algorithms. Contactless transaction time budgets are under 300 milliseconds. Side-channel protection — essential for payment cards where physical attackers can probe power consumption — multiplies PQC execution time by 2× to 5.6×. Classic McEliece requires over 70 KB of RAM (more than the card's total memory). Only lattice-based algorithms (ML-KEM, ML-DSA) are even theoretically feasible on current hardware, and EMV commands' 256-byte data transfer limits require entirely new extended commands.

FS-ISAC's payment card guidance explicitly notes that it is not known whether EMV can accommodate quantum-safe certificates. New 28nm smart card chips (IDEMIA/GlobalFoundries, targeted for 2026 mass production) will provide more headroom, but the card and terminal replacement cycle is measured in years. Mastercard's Enhanced Contactless (Ecos) specification uses AES symmetric encryption for quantum resistance, sidestepping asymmetric PQC on constrained hardware — a pragmatic but partial solution that does not address offline data authentication.

> **Framework Impact:** Phase 4 (Roadmap) must incorporate hardware refresh cycles for cards and terminals as hard constraints on migration timelines. Phase 5 must include a triage strategy separating online (symmetric-safe) from offline (asymmetric-vulnerable) authentication.

CHALLENGE 3: THE PAYMENT HSM CERTIFICATION BOTTLENECK

Hardware Security Modules are the root of trust for every payment cryptographic operation. SWIFT mandates FIPS 140-2 Level 2+ certified HSMs; PCI compliance requires separate validation. As of early 2026, no HSM vendor has completed a FIPS 140-3 Level 3 CMVP validation that includes PQC algorithms within the validated module boundary. HSM vendors ship firmware with PQC support, but running PQC operations outside the FIPS-validated boundary creates a compliance gap that regulators and auditors may not accept.

Payment HSMs (Thales payShield, Utimaco Atalla, Futurex) have specific PQC upgrade timelines that organizations do not control. CMVP validation backlogs currently average 12–18 months. Until validated PQC HSM modules are available, institutions face a choice between running PQC in non-validated firmware mode (compliance risk) or waiting for validation (migration delay). Neither option is attractive.

> **Framework Impact:** Phase 6 (Infrastructure) must include HSM certification tracking as a gating dependency. Phase 7 (Vendor Governance) must establish structured engagement with HSM vendors specifically around FIPS/PCI certification timelines.

CHALLENGE 4: SETTLEMENT LATENCY AND PERFORMANCE

BIS Project Leap Phase 2 provided the first empirical evidence of PQC performance impact on real-world settlement infrastructure. Software-based PQC signature verification averaged 209.9 milliseconds compared to 28.1 milliseconds for RSA — a 7.5× slowdown. While hardware-accelerated implementations will narrow this gap, the 7.5× factor on a system that processes trillions of euros daily creates legitimate capacity planning concerns.

PQC's larger signatures and keys also increase bandwidth consumption across settlement networks. Certificate chains with ML-DSA could add tens of kilobytes per transaction. At peak throughput of thousands of transactions per second, this aggregates into substantial additional bandwidth and storage demands. RTGS systems, real-time payment networks (FedNow, TIPS, Faster Payments), and high-frequency trading venues all have tight latency budgets where PQC overhead must be engineered out, not absorbed.

> **Framework Impact:** Phase 6 (Infrastructure) must include settlement-system-specific performance benchmarking. Phase 5 (Pilots) should prioritize RTGS and real-time payment interfaces for early PQC testing.

CHALLENGE 5: CROSS-BORDER AND MULTI-NETWORK COORDINATION

A single cross-border payment can traverse the originating bank, its correspondent bank, SWIFT's messaging network, the receiving correspondent bank, the beneficiary bank, and one or more central bank RTGS systems — each with independent cryptographic implementations, PKI hierarchies, and upgrade cycles. Migrating one node to PQC while its counterparties remain on classical cryptography requires hybrid interoperability that none of these systems were designed for. BIS Project Leap discovered that a correctly PQC-signed liquidity transfer could not complete settlement because the corresponding digital certificate was missing from TARGET2's static reference data — the migration is not just an algorithm swap but an entire parallel PKI infrastructure.

SWIFT has announced that SwiftNet 8.0, targeted for 2027, will be PQC-enabled, with a 15-month migration window. Card networks (Visa, Mastercard) operate their own certificate authorities and will set their own PQC migration timelines. Domestic payment schemes (ACH, SEPA, Faster Payments) operate under national governance. International coordination across these independent timelines is the defining program management challenge for financial services PQC migration.

> **Framework Impact:** Phase 0 (Executive Mandate) must establish cross-industry coordination mechanisms from the outset. Phase 4 (Roadmap) must map external dependency timelines from SWIFT, card networks, and central banks as hard constraints.

CHALLENGE 6: OVERLAPPING REGULATORY AND STANDARDS REQUIREMENTS

Financial institutions face the most complex regulatory landscape of any sector for PQC migration. Relevant guidance and requirements come from multiple overlapping sources, often with inconsistent timelines and specificity levels. PCI DSS v4.0 Requirement 12.3.3 (effective March 2025) already mandates cryptographic cipher suite and protocol documentation and annual review for PCI-scoped entities. The G7 Cyber Expert Group roadmap (January 2026) targets 2030–2032 for critical financial system migration. The EU Coordinated Implementation Roadmap (June 2025) mandates national PQC strategies by end of 2026 and critical-sector quantum safety by end of 2030, explicitly naming financial services as a high-risk sector. HKMA announced a Quantum Preparedness Index in February 2026. MAS issued advisory guidance recommending cryptographic inventories. UK NCSC targets crypto discovery by 2028 and high-priority migration by 2031.

Crucially, no regulator has yet mandated specific PQC algorithms or implementation standards for financial institutions. PCI SSC has not published standalone PQC guidance. This creates a paradox: institutions face growing regulatory pressure to demonstrate quantum readiness but lack definitive compliance targets. The practical consequence is that framework Phase 0 business cases must build on regulatory trajectory rather than current mandates, and compliance officers must track multiple regulatory streams simultaneously.

CHALLENGE 7: TRUST NOW, FORGE LATER (TNFL) RISKS IN FINANCIAL SYSTEMS

While HNDL (Harvest Now, Decrypt Later) receives more attention, the Trust Now, Forge Later (TNFL) threat may be equally consequential for financial services. Digital signatures underpin the integrity of payment instructions, trade confirmations, regulatory filings, legal contracts, and audit trails. A cryptanalytically relevant quantum computer (CRQC) could forge digital signatures, enabling fabrication of payment orders, alteration of settlement records, or creation of fraudulent regulatory submissions — all with signatures that would pass current verification.

This is especially acute for financial instruments and records with long retention requirements. Court-admissible digital evidence, trade confirmations, and regulatory audit trails may need to remain verifiable for decades. If the signatures on these records become forgeable, the evidentiary foundation of financial transactions collapses. Phase 3 risk scoring must assess TNFL exposure on long-lived signed artifacts, not just HNDL exposure on encrypted data.

CHALLENGE 8: OPEN BANKING AND API ECOSYSTEM EXPOSURE

Open Banking regulations (PSD2 in Europe, analogous regimes in the UK, Australia, Brazil, and elsewhere) have created a vast API ecosystem through which financial data flows between banks, fintechs, aggregators, and third-party providers. These APIs rely on TLS for transport security and typically use OAuth 2.0, FAPI (Financial-grade API), and JWT/JWS for authorization and transaction signing — all of which depend on RSA or ECDSA for key exchange and digital signatures. The quantum vulnerability surface of Open Banking is both wide (thousands of API endpoints across the ecosystem) and fragmented (each participant controls only its own endpoints).

Open Banking APIs often carry sensitive financial data (account balances, transaction histories) and execute privileged operations (payment initiation, consent management). HNDL collection of Open Banking API traffic would expose the financial lives of millions of consumers. PQC migration for Open Banking requires coordinated action across regulators (who set the API standards), banks (who operate the endpoints), and fintechs (who consume them). This coordination layer does not currently exist.

CHALLENGE 9: DIGITAL ASSETS AND BLOCKCHAIN QUANTUM VULNERABILITY

Financial institutions with exposure to digital assets, central bank digital currencies (CBDCs), distributed ledger technology (DLT) for settlement (e.g., JP Morgan's Onyx, the European Central Bank's DLT settlement pilots), or tokenized securities face blockchain-specific quantum vulnerabilities. Most blockchains rely on ECDSA or EdDSA for transaction signing — directly breakable by Shor's algorithm. Unlike traditional payment systems where a compromised key can be revoked and reissued, blockchain transactions are immutable: a forged signature creates an irreversible transfer of value.

Institutional digital asset custody solutions, smart contracts, and on-chain settlement protocols all inherit this vulnerability. The migration path is complicated by blockchain governance constraints (protocol upgrades require consensus among decentralized participants) and the immutability of historical transactions (past signatures cannot be retroactively upgraded). Financial institutions with DLT exposure must include blockchain-specific risk assessment in Phase 3 and may need to engage with protocol governance bodies as part of Phase 7 vendor/supply chain activities.

CHALLENGE 10: TOKENIZATION AS INTERIM QUANTUM DEFENSE

Financial services makes extensive use of tokenization — replacing sensitive data (card PANs, account numbers, personal identifiers) with cryptographically irreversible tokens. Tokenized data has no value if harvested for future quantum decryption because the token-to-value mapping is protected by symmetric cryptography (AES), which is not vulnerable to Shor's algorithm. This makes tokenization a uniquely effective interim quantum defense for financial data at rest: it reduces the HNDL-exposed data surface immediately, without waiting for full PQC migration.

Institutions that have already deployed tokenization broadly (as many card issuers and payment processors have) should recognize this as a de facto head start on quantum resilience. The framework adaptation for Phase 5 should include a tokenization coverage assessment to identify which data stores are already quantum-defended through tokenization and which remain exposed. Expanding tokenization scope may be faster and cheaper than waiting for end-to-end PQC for certain data categories.

PHASE-BY-PHASE FRAMEWORK ADAPTATIONS FOR FINANCIAL SERVICES

This section walks through each Universal Framework phase and specifies the adaptations, additions, and re-prioritizations required for financial services. Organizations should implement these alongside — not instead of — the Universal Framework's phase guidance.

PHASE 0 — EXECUTIVE MANDATE & BUSINESS CASE

Additional Business Case Arguments

- **Systemic risk framing:** The business case should quantify potential systemic impact, referencing the Citi Institute/Hudson Institute $2.0–3.3 trillion cascading-loss scenario. This reframes quantum risk from an IT security issue to a financial stability concern that resonates with boards and regulators.
- **Regulatory trajectory:** Map the convergence of PCI DSS 12.3.3 (current mandate), G7 roadmap (2030–2032 target), EU roadmap (2030 critical-sector deadline), and national supervisory expectations. The argument is not "regulators require PQC today" but "the regulatory trajectory makes PQC investment inevitable — early movers face lower costs and less disruption."
- **HNDL as quantifiable exposure:** For institutions handling cross-border payments, sovereign wealth data, trade finance, or wealth management, calculate the volume of data currently in transit with confidentiality requirements extending past 2035. This produces a concrete "data-at-risk" metric that boards understand.
- **Insurance and counterparty expectations:** Insurers are beginning to inquire about quantum readiness in cyber policy renewals. Large counterparties (especially government-linked or defense-adjacent) may begin requiring quantum readiness attestations in RFP responses.

Governance Adaptation

Financial services PQC governance should include representation from payment operations, treasury, compliance/regulatory affairs, and digital channels — not just IT security. The steering committee must have the authority to coordinate across business lines that control different payment channels (cards, corporate banking, wealth management, digital assets). Consider establishing a dedicated "Quantum Readiness Working Group" under the existing Technology Risk Committee with a direct reporting line to the board risk committee.

PHASE 1 — DISCOVERY & INVENTORY

Expanded Scope: Payment-Specific Inventory Tracks

In addition to the Universal Framework's three parallel inventory tracks (static code analysis, runtime/configuration inspection, and passive network monitoring), financial services institutions should add the following sector-specific tracks:

- **Payment message format analysis:** Inventory every message format in use (ISO 8583, ISO 20022, FIX, SWIFT MT/MX, FpML, domestic scheme formats) and map field-level cryptographic dependencies. Identify fixed-size fields that cannot accommodate PQC payloads.
- **HSM estate mapping:** Inventory all payment HSMs by model, firmware version, FIPS/PCI certification status, and vendor-published PQC roadmap. Classify each HSM as PQC-ready, PQC-upgradeable (firmware update), or PQC-blocked (hardware replacement required).
- **Card and terminal estate:** Inventory card platform generations (chip type, RAM, supported algorithms), terminal firmware versions, and EMV kernel versions. Map offline vs. online authentication reliance by card program.
- **Third-party cryptographic interfaces:** Map every external cryptographic interface — SWIFT connections, card network links, clearing house integrations, correspondent banking channels, Open Banking APIs, digital asset custody interfaces. For each, identify the counterparty's PQC readiness (if known) and the protocol/algorithm in use.
- **Certificate authority hierarchy:** Map all CA hierarchies in which the institution participates — internal enterprise PKI, card network CAs, SWIFT PKI, domestic payment scheme CAs, Open Banking trust frameworks. These are PQC migration units that require coordinated root key rotation.

Risk-Driven Scoping for Financial Services

The Universal Framework recommends risk-driven scoping to avoid the “boil the ocean” trap. For financial services, the recommended initial scoping should prioritize: (1) external-facing payment APIs and SWIFT interfaces (highest HNDL exposure), (2) HSM-protected key material in settlement and clearing systems, (3) card network certificate chains, (4) correspondent banking encryption, and (5) customer-facing digital channels including Open Banking APIs. Internal service-mesh cryptography and data-at-rest encryption, while important, are lower priority because they are more readily controlled and less exposed to HNDL collection.

PHASE 2 — CBOM & DOCUMENTATION

Financial Services CBOM Complexity

The Minimum Viable CBOM model from the Universal Framework applies, but financial services institutions should expect their CBOMs to be substantially larger and more complex than in other sectors. The 30,000+ unique cryptographic functions across a cross-border payment chain means that the CBOM must span organizational boundaries — something the standard CBOM model does not address.

Practical recommendation: build the CBOM in concentric rings. Start with “what we control” (the institution’s own systems, HSMs, certificates, and code), then extend to “what we consume” (vendor-provided cryptographic implementations in payment HSMs, card platform SDKs, SWIFT Alliance software), and finally “what we depend on” (counterparty and network-level cryptography that we can document but not directly modify). The third ring is inherently incomplete, and that is acceptable — the goal is to make dependencies visible, not to achieve exhaustive documentation of counterparty internals.

PCI DSS 12.3.3 Alignment

PCI DSS v4.0 Requirement 12.3.3 already mandates that PCI-scoped entities document all cryptographic cipher suites and protocols in use, with annual review. A well-structured CBOM directly satisfies this requirement and extends it to PQC readiness assessment. Financial institutions should ensure their CBOM structure and metadata fields are sufficient to produce PCI 12.3.3 evidence artifacts as a standard output.

PHASE 3 — RISK SCORING & PRIORITIZATION

Adapted Risk Scoring Model

The Universal Framework's risk scoring model uses five dimensions: data sensitivity, cryptographic vulnerability, exposure to interception, migration difficulty, and regulatory/compliance urgency. For financial services, two additional dimensions should be added:

- **Systemic criticality:** Does this system's failure or compromise cascade to other institutions or market infrastructure? RTGS systems, clearing houses, and central counterparties score highest.
- **Multi-party dependency:** Does migrating this system require coordinated action with external parties? SWIFT interfaces, card network connections, and correspondent banking channels score highest because migration cannot be completed unilaterally.

Financial Services Priority Tiers

Priority	System Category	Rationale
Tier 1	SWIFT interfaces, RTGS/settlement connections, payment HSM key material, correspondent banking encryption	Highest HNDL exposure, systemic criticality, regulatory visibility. External-facing with long data confidentiality requirements.
Tier 2	Card network CA hierarchies, external payment APIs, Open Banking endpoints, digital asset custody	High HNDL and TNFL exposure. Multi-party coordination required. Consumer-facing reputational risk.
Tier 3	Core banking TLS mesh, internal API gateways, database encryption, application-level signing	Important but internally controlled. Can be migrated on institutional timeline without external dependencies.
Tier 4	Smart card/terminal offline authentication, legacy batch interfaces, archival systems	Hardware-constrained or low-urgency. Dependent on vendor hardware refresh cycles. Plan now, execute on hardware availability.

PHASE 4 — ROADMAP & GOVERNANCE

External Dependency Mapping

The financial services roadmap must incorporate external timelines that the institution does not control:

- **SWIFT SwiftNet 8.0:** Targeted for 2027 with PQC enablement and a 15-month migration window.
- **Card network PQC timelines:** Visa and Mastercard CA migration timelines (not yet publicly committed as of March 2026). EMV specification updates for PQC certificate handling.
- **HSM vendor certification:** FIPS 140-3 Level 3 CMVP validation with PQC algorithms within the validated boundary. Track Thales, Utimaco, Futurex, and Entrust timelines.
- **Smart card silicon availability:** IDEMIA/GlobalFoundries 28nm PQC-capable chips (targeted 2026). Infineon equivalents.
- **Central bank RTGS upgrades:** TARGET2, Fedwire, BOE RTGS modernization timelines for PQC adoption.
- **Domestic payment scheme upgrades:** ACH, SEPA, Faster Payments scheme-level PQC adoption decisions.
- **Regulatory enforcement milestones:** PCI SSC standalone PQC guidance (expected but not yet published), EU 2030 critical-sector deadline, national supervisor examination cycles.

These external dependencies should be visualized on a single timeline map and reviewed quarterly. Where external timelines slip, the institution's roadmap must adapt — but "waiting for vendors" is not a strategy. Internal preparation (Phases 0–3) should proceed regardless of external readiness.

Recommended Year-1 Plan Adaptations

The Universal Framework's quarter-by-quarter Year-1 plan should be adapted for financial services as follows:

- **Q1:** Establish governance with cross-business-line representation. Begin PCI 12.3.3 aligned cryptographic inventory on PCI-scoped systems. Initiate HSM vendor engagement (Phase 7 early start). Commission SWIFT readiness assessment.
- **Q2:** Expand inventory to payment message format analysis and card/terminal estate. Begin CBOM construction for Tier 1 systems. Join industry coordination

forums (FS-ISAC Quantum Working Group, Europol QSFF, national supervisor forums).

- **Q3:** Complete Tier 1 risk scoring. Produce initial Quantum Readiness Assessment for board and regulatory consumption. Begin Tier 1 pilot design (SWIFT interface or external payment API using hybrid ML-KEM + X25519 for TLS key exchange).
- **Q4:** Execute first Tier 1 pilot in test environment. Establish external dependency timeline map. Produce Year-2 roadmap with budget request.

PHASE 5 — PILOTS & MIGRATION EXECUTION

Financial Services Pilot Targets

The Universal Framework recommends selecting pilot targets that are high-value, technically representative, and bounded in scope. For financial services, the following pilot targets are recommended in order of priority:

- **External payment API with hybrid TLS:** Enable hybrid ML-KEM-768 + X25519 key exchange on a non-critical external payment API. Measure handshake latency, throughput impact, and client compatibility. This is the lowest-risk, highest-learning pilot.
- **SWIFT test environment:** If SWIFT sandbox/test infrastructure supports PQC, pilot PQC message signing in the non-production SWIFT environment to understand message size impacts and certificate distribution requirements.
- **Internal service-mesh PQC:** Enable PQC in the internal TLS mesh between core banking microservices. This provides production-scale performance data without external coordination risk.
- **HSM PQC key generation:** If HSM firmware supports PQC key generation (even outside the FIPS-validated boundary), pilot PQC key generation and storage to validate operational key management procedures.

Tokenization Coverage Assessment

Before designing migration pilots for data-at-rest protection, conduct a tokenization coverage assessment. Data stores already protected by tokenization (card PANs, account numbers, personal identifiers) are de facto quantum-defended against HNDL for those data elements. The assessment should identify: which data categories are currently tokenized, which tokenization implementations rely on format-preserving encryption (FPE) — since FPE may have quantum-specific weaknesses depending on its construction — and which sensitive data categories remain untokenized and exposed to HNDL.

The Hybrid Architecture Reality

Hybrid cryptography (running classical and PQC algorithms in parallel) is universally recommended for the transition period. However, BIS Project Leap revealed that hybridization in settlement systems was not envisaged in the original cryptographic design and requires substantial system evolution. Financial institutions should expect that hybrid deployments will be significantly more complex than simple algorithm addition — they require duplicate PKI infrastructure, extended certificate handling, modified verification logic, and expanded message formats. Plan for hybrid as an architectural change, not a configuration toggle.

PHASE 6 — INFRASTRUCTURE MODERNIZATION & PERFORMANCE

Payment HSM Modernization Strategy

Payment HSMs deserve their own modernization track within Phase 6, separate from the general HSM/KMS guidance in the Universal Framework. The strategy should address:

- **Firmware-upgradeable vs. hardware-replacement HSMs:** Classify the HSM estate. Newer HSMs (Thales payShield 10K with post-2024 firmware, Utimaco CryptoServer with PQC addon) may be firmware-upgradeable. Older units require hardware replacement with attendant procurement, certification, and deployment lead times of 12–24 months.
- **FIPS/PCI certification gap management:** Document the compliance risk of running PQC algorithms outside the FIPS-validated boundary. Prepare risk acceptance memos for internal audit and regulator discussions. Monitor CMVP validation queues for PQC-inclusive submissions.
- **Key ceremony adaptation:** PQC key generation may require updated key ceremony procedures, particularly for HSM root keys. Plan and rehearse PQC key ceremonies in test environments before production execution.
- **Dual-key management:** During the hybrid period, HSMs must manage both classical and PQC key material simultaneously. This doubles key storage requirements and complicates key lifecycle management (generation, backup, rotation, destruction).

Settlement System Performance Benchmarking

Financial institutions participating in RTGS or real-time payment systems should conduct PQC performance benchmarking specific to settlement workflows:

- **Signature verification throughput:** Benchmark ML-DSA verification rates on production-equivalent hardware at peak transaction volumes. The 7.5× slowdown observed in Project Leap should be revalidated with hardware acceleration.
- **Certificate chain validation:** Test full PQC certificate chain validation including OCSP/CRL checks with enlarged PQC certificates. Measure end-to-end latency.
- **Network bandwidth impact:** Model the bandwidth increase from larger PQC signatures and certificates at peak volumes across settlement network links.

PHASE 7 — VENDOR & SUPPLY CHAIN GOVERNANCE

Financial Services Vendor Classification

The Universal Framework classifies vendors by PQC impact. Financial services requires a finer-grained classification that reflects the multi-party nature of the payment system:

Vendor Category	Examples	Engagement Approach
Network operators	SWIFT, Visa, Mastercard, domestic payment schemes, central bank RTGS operators	Strategic engagement at C-suite level. Participate in industry forums and pilot programs. Align institutional roadmap to published network timelines.
Crypto infrastructure	HSM vendors (Thales, Utimaco, Futurex, Entrust), PKI/CA providers, key management platforms	Quarterly PQC roadmap reviews. FIPS/PCI certification tracking. Early access to PQC firmware for lab testing.
Platform vendors	Core banking vendors (Temenos, FIS, Finastra), card management systems, payment gateways	PQC readiness questionnaires. Contractual PQC upgrade commitments. CBOM exchange requirements.
Fintech ecosystem	Open Banking providers, aggregators, TPPs, digital wallet platforms	Coordinate through Open Banking trust framework governance. PQC requirements in TPP onboarding criteria.
Digital asset infra	Custody providers, blockchain protocol teams, DLT platform operators	Monitor protocol-level PQC upgrade plans. Assess custody provider quantum readiness. Evaluate PQC-native chain alternatives.

Industry Coordination Forums

Financial institutions should actively participate in sector-specific PQC coordination bodies:

- **Europol Quantum Safe Financial Forum (QSFF):** Produces practical prioritization scoring frameworks. Published a uniquely actionable priority matrix combining quantum risk scores and migration time scores (January 2026).
- **FS-ISAC Quantum Working Groups:** Sector-specific threat intelligence and migration guidance, including payment card industry quantum impact analysis.
- **BIS Innovation Hub:** Coordinates central bank PQC experiments (Project Leap and successors). Participation provides early insight into RTGS migration timelines.
- **X9 / ISO TC 68:** Standards development for PQC in financial messaging (ISO 8583, ISO 20022 PQC accommodation).
- **National supervisory forums:** Many national regulators are establishing quantum readiness working groups. Presence ensures the institution shapes regulatory expectations rather than merely reacting.

FINANCIAL SERVICES REGULATORY ALIGNMENT MAP

The following table maps key regulatory and standards requirements to framework phases, providing a compliance planning reference for financial services institutions.

Regulatory Body / Standard	Key Requirement	Timeline	Framework Phase(s)
PCI DSS v4.0 Req 12.3.3	Document and annually review all cryptographic cipher suites and protocols	Effective March 2025	Phase 1 (Inventory), Phase 2 (CBOM)
G7 Cyber Expert Group	Phased quantum readiness activities for financial authorities and institutions	2030–2032 target	Phase 0 (Business Case), Phase 4 (Roadmap)
EU Coordinated Roadmap	National PQC strategies; critical sectors quantum-safe	Strategies by end 2026; high-risk by end 2030	Phase 0 through Phase 5
NIST IR 8547	Deprecate RSA/ECC at 112-bit after 2030; disallow after 2035	2030 deprecation, 2035 disallowance	Phase 3 (Scoring), Phase 4 (Roadmap)
UK NCSC	Crypto discovery by 2028; high-priority migration by 2031; full transition by 2035	2028 / 2031 / 2035	Phase 1 through Phase 5
HKMA Quantum Preparedness Index	Banking sector readiness scoring	Announced Feb 2026	Cross-cutting: Maturity Model

MAS Advisory	Cryptographic asset inventories and migration strategies recommended	Active (Circular MAS/TCRS/2024/01)	Phase 1 (Inventory), Phase 4 (Roadmap)
Europol QSFF	Prioritization scoring framework: quantum risk × migration time	Published Jan 2026	Phase 3 (Risk Scoring)
BIS Papers No. 158	Central bank perspective on quantum threats to financial infrastructure	Published Jul 2025	Phase 0 (Business Case)
SWIFT SwiftNet 8.0	PQC-enabled messaging infrastructure	Targeted 2027; 15-month migration	Phase 5 (Pilots), Phase 7 (Vendor)

FINANCIAL SERVICES MATURITY MODEL SUPPLEMENT

The Universal Framework's 5-level maturity model applies. The following table provides financial-services-specific indicators for each level, enabling institutions to benchmark themselves against sector-appropriate expectations.

Level	Universal Indicator	Financial Services Indicator
1 — Aware	Quantum risk acknowledged; no formal program	PCI 12.3.3 compliance may be ad hoc. No inventory of payment HSMs or card platforms. No engagement with SWIFT, card networks, or regulators on quantum readiness.
2 — Assessed	Cryptographic inventory underway; initial risk assessment completed	PCI 12.3.3 satisfied with structured cryptographic documentation. HSM estate mapped with firmware/certification status. SWIFT and card network PQC readiness assessed. Initial QRA produced for board and regulators.
3 — Planning	Multi-year roadmap established; pilots designed; governance operational	External dependency timeline map maintained. Year-1 plan in execution. HSM vendor PQC roadmap reviews quarterly. Industry forum participation active. Tokenization coverage assessed. Regulatory alignment map current.
4 — Migrating	Pilots in production; wave-based migration underway; metrics reported	Hybrid PQC deployed on Tier 1 systems (SWIFT, external APIs). HSM PQC operations in validated or risk-accepted mode. Card/terminal migration plan aligned to silicon availability. CBOM integrated into PCI compliance workflow.
5 — Resilient	Crypto-agility achieved; algorithm transitions routine; continuous monitoring	All payment channels quantum-safe or hybrid. Payment HSMs FIPS-validated with PQC. Card platforms PQC-capable for offline auth. Full CBOM exchange with Tier 1 vendors. Crypto-agility enables algorithm rotation without program-level effort.

FINANCIAL SERVICES KPI SUPPLEMENT

The Universal Framework defines board-level, operational, and evidence-dossier KPIs. The following additional KPIs are recommended for financial services:

Board-Level KPIs (Quarterly)

- **Payment HSM PQC readiness:** Percentage of payment HSMs with PQC-capable firmware installed / total payment HSM estate.
- **External interface quantum exposure:** Number of external-facing payment interfaces (SWIFT, card network, Open Banking APIs) operating without any PQC protection / total external interfaces.
- **Regulatory readiness score:** Composite score based on compliance with PCI 12.3.3, alignment to G7/EU/national roadmap milestones, and ability to respond to regulator quantum readiness inquiries.
- **HNDL data-at-risk volume:** Estimated volume of data in transit across external payment interfaces with confidentiality requirements exceeding 10 years that is not yet PQC-protected.

Operational KPIs (Monthly)

- **Vendor PQC roadmap alignment:** Number of critical payment vendors (HSM, core banking, card platform, messaging) with confirmed PQC roadmaps / total critical payment vendors.
- **Message format PQC readiness:** Number of payment message formats analyzed for PQC payload accommodation / total formats in use.
- **Tokenization coverage:** Percentage of high-sensitivity data categories protected by tokenization (providing interim HNDL defense).

RECOMMENDED IMMEDIATE ACTIONS

For financial institutions at Maturity Level 1 (Aware) or Level 2 (Assessed), the following actions can begin immediately and do not depend on external vendor readiness:

#	Action	Timeline	Framework Phase
1	Satisfy PCI DSS 12.3.3 with a structured cryptographic inventory that doubles as the input for CBOM and QRA	0–3 months	Phase 1 / Phase 2
2	Map the complete payment HSM estate by model, firmware, and PQC readiness status; initiate vendor engagement on PQC firmware and certification timelines	0–3 months	Phase 1 / Phase 7
3	Assess SWIFT interface readiness for SwiftNet 8.0 PQC requirements; register for SWIFT PQC pilot programs if available	0–6 months	Phase 5 / Phase 7
4	Conduct tokenization coverage assessment to identify data categories already quantum-defended and prioritize remaining exposed data	0–3 months	Phase 5
5	Establish a Quantum Readiness Working Group with representation from IT security, payment operations, treasury, compliance, and digital channels	0–1 month	Phase 0
6	Join at least one industry PQC coordination forum (Europol QSFF, FS-ISAC Quantum Working Group, BIS Innovation Hub)	0–3 months	Phase 0 / Phase 7
7	Produce an initial Quantum Readiness Assessment suitable for board risk committee and regulatory inquiry response	3–6 months	Phase 3
8	Enable hybrid PQC (ML-KEM-768 + X25519) on at least one non-critical external API endpoint to gain operational experience	3–9 months	Phase 5

FURTHER READING

The following PostQuantum.com articles provide detailed analysis supporting this extension:

- **Payments and the Race to Quantum Safety —** postquantum.com/post-quantum/payments-quantum-pqc/ — Seven payments-specific PQC challenges with detailed technical analysis and emerging approaches.
- **The Cryptographic Iceberg Inside a Mobile Banking Transaction —** postquantum.com/post-quantum/cryptography-cbom-mobile-banking/ — Layer-by-layer reconstruction of the ~320 cryptographic function calls in a single mobile banking session across 9 parties and 30,000+ unique functions.
- **Cryptographic Stack in Modern Interbank Payment Systems —** postquantum.com/post-quantum/cryptography-interbank-payment/ — End-to-end cryptographic mapping from customer authentication through SWIFT messaging to central bank settlement.
- **Hybrid Cryptography for the Post-Quantum Era —** postquantum.com/post-quantum/hybrid-cryptography-pqc/ — Hybrid schemes in TLS, SSH, IPsec; standards alignment; pilot design.
- **Infrastructure Challenges of Dropping In PQC —** postquantum.com/post-quantum/infrastructure-challenges-pqc/ — How PQC stresses real infrastructure: handshakes, cert chains, CPU/memory, middleboxes.
- **Rethinking CBOM —** postquantum.com/post-quantum/rethinking-cbom/ — Challenges the completeness model; proposes the Minimum Viable CBOM approach.
- **120,000 Tasks: Why PQC Migration Is Enormous —** postquantum.com/post-quantum/quantum-security-pqc-program-plan/ — Why credibly planned programs reach six-figure task counts.
- **Evaluating Tokenization in the Context of Quantum Readiness —** postquantum.com/post-quantum/tokenization-quantum-readiness/ — Tokenization as scope-reducer and blast-radius limiter.

ABOUT

ABOUT THE AUTHOR

Marin Ivezic is a former Fortune Global 500 CISO/CTO, the Editor-in-Chief of PostQuantum.com, and the founder and CEO of Applied Quantum. He previously held cybersecurity partner and practice lead roles — including regional and global leadership positions — at IBM, Accenture, PwC, and KPMG. He is also the former CEO of Cyber Agency and the founder of Cryptosec, a cryptography advisory and engineering firm.

Marin has been involved in quantum technologies for over 25 years, having advised governments on the quantum threat since the early 2000s. He previously founded Boston Photonics and PQ Defense. He has led real-world quantum readiness programs for telecoms, financial institutions, and critical infrastructure operators — including programs exceeding 120,000 discrete migration tasks.

PostQuantum.com, his personal blog, reaches over 1 million monthly readers and is recognized as the premier quantum security publication for CISOs, CTOs, and security architects worldwide.

ABOUT APPLIED QUANTUM

Applied Quantum (AppliedQuantum.com) is a research-driven professional services firm focused entirely on quantum technologies and post-quantum security. Its dedicated security practice, Secure Quantum (SecureQuantum.com), focuses on quantum security advisory and PQC migration. Services span Quantum Security & PQC Migration, Quantum Strategy & Sovereignty, Quantum Engineering & Implementation, and Quantum Commercialization.

If you need help: Applied Quantum provides advisory, program design, and hands-on migration execution support. Contact: contact@appliedquantum.com