JUNE 2026
APPLIED QUANTUM

THE APPLIED QUANTUM PQC MIGRATION FRAMEWORK

FINANCIAL SERVICES EXTENSION

Banking, Capital Markets, Insurance, and Digital Assets *— Industry-Specific Challenges and Framework Adaptations*

Version 2.1 — June 2026

Marin Ivezic
CEO, Applied Quantum
Author, PostQuantum.com

PQCFramework.com | PQCMigrationBrief.com | PostQuantum.com | SecureQuantum.com | AppliedQuantum.com | QuantumReady.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 June 2026. These references may become outdated quickly. Readers should verify current status against primary sources before making implementation decisions.

References to specific vendors, products, or tools are for illustrative purposes and do not constitute endorsement. The PQC tooling market is evolving rapidly; products mentioned may have changed in capability, licensing, or availability since publication. Organizations should conduct their own evaluation based on their specific requirements, regulatory environment, and procurement constraints.

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

ABOUT THIS DOCUMENT

Document type	Enterprise methodology and practitioner framework
Parent Document	The Applied Quantum PQC Migration Framework — Universal — v2.1 (June 2026)

Intended audience	CISOs, security architects, compliance officers, risk managers, and program managers in banking, capital markets, insurance, asset management, and digital assets
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. For payments-specific guidance (card networks, RTGS, SWIFT, payment HSMs, POS terminals), see the companion Payments Extension. For digital asset and blockchain-specific guidance, see the companion Digital Assets Extension. Not a standalone document, intended to be used alongside the Universal Framework.

VERSION HISTORY

Version 1.1 (March 2026): Initial publication as a companion to the Universal Framework v1.1. Covered banking, payments, and capital markets with 10 industry-specific challenges, phase-by-phase adaptations, regulatory alignment map, maturity model supplement, KPI supplement, and recommended immediate actions.

Version 2.0 (June 2026): Major update aligned with Universal Framework v2.0. Scope refined to banking, capital markets, insurance, and digital assets (payments separated to dedicated extension). Added: v2.0 alignment (two-track model, FIPS validation gap, MTC position), CNSA 2.0 voluntary adoption, capital markets and insurance challenges, updated regulatory section (G7 CEG, Europol QSFF, FS-ISAC, DORA, HKMA), and updated immediate actions.

Version 2.1 (June 2026): Aligned with Universal Framework v2.1. Six new alignment subsections: hybrid/composite signatures as the Track B default; algorithm-specific vulnerability weighting (ECC is not a safe harbor); the identity stack in Track B (passkeys, open banking token signing, federation); SP 800-208 deploy-now code and firmware signing; securing the CBOM and program artifacts; verification, decommissioning, and program closure. Corrections: Universal dimension count in Phase 3; MTC wording aligned with the Universal position. Companion book cross-references added.

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.

WHAT'S NEW IN V2.1

Version 2.1 of the Financial Services Extension is a targeted alignment release tracking Universal Framework v2.1 (June 2026):

Alignment with Universal Framework v2.1. Six new alignment subsections map the v2.1 positions that require sector adaptation to financial services: hybrid and composite signatures as the Track B default; algorithm-specific vulnerability weighting and why ECC is not a safe harbor; the identity stack (customer passkeys, open banking token signing, federation) within Track B; SP 800-208 stateful hash-based signatures as the deploy-now action for code and firmware signing; protection of the CBOM and program artifacts as high-value targets; and migration verification, decommissioning, and program closure. The remaining Universal v2.1 additions are sector-neutral and apply as written; the alignment section introduction lists them and the governing cross-references.

Editorial corrections. The Universal Framework dimension count in Phase 3 risk scoring was corrected, and the Merkle Tree Certificates wording was aligned with the Universal Framework position. A cross-reference to the companion book, *Quantum Ready*, was added.

WHAT'S NEW IN V2.0

Version 2.0 of the Financial Services Extension reflects three developments since the March 2026 release:

Alignment with Universal Framework v2.0. The parent framework introduced a two-track migration model (key exchange and signatures as parallel tracks), a deployment environment classification (addressing the FIPS 140-3 validation gap), and a definitive position on Merkle Tree Certificates for public Web PKI. This extension maps each of these to financial services contexts.

Payments separation. Payments-specific content (card networks, RTGS systems, payment HSMs, POS terminals, ISO 8583/20022 message format constraints) has been moved to a dedicated Payments Extension. This extension retains guidance relevant to all financial services sub-sectors and cross-references the Payments Extension where appropriate.

Regulatory acceleration. The G7 Cyber Expert Group published its six-phase financial sector roadmap (January 2026), Europol's QSFF and FS-ISAC jointly published a prioritization methodology (January 2026), HKMA announced in February 2026 that it will develop a Quantum Preparedness Index to assess banking-sector PQC readiness, and DORA's crypto-agility requirements took effect. These are integrated into the regulatory alignment section and Phase 0 business case.

Scope additions include capital markets trading infrastructure, insurance and asset management considerations, digital asset quantum vulnerability, and CNSA 2.0 voluntary adoption by financial services organizations.

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 Getting Started with Quantum Security and PQC Migration page: https://postquantum.com/starting-pqc-quantum-security/, 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.

This extension, like the framework it accompanies, is the execution methodology. For the complete treatment (the reasoning behind each phase, extended case examples, and guidance for leading the program from the first board conversation through closure), see the companion book, *Quantum Ready* (QuantumReady.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 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 moves HNDL from a theoretical concern to an operational one 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 sector.

The Densest Regulatory Environment 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.

Financial Services Structural Advantages for PQC Migration

Financial services faces severe PQC migration challenges, but it also possesses structural advantages that most other sectors lack. Organizations should recognize and use these advantages in their program design.

Three Lines of Defense Model

Most regulated financial institutions already operate a three lines of defense governance model (business units as first line, risk management and compliance as second line, internal audit as third line). The Universal Framework's governance structure maps directly into this model: the PQC program management function sits in the first line, the CISO and risk management provide oversight as the second line, and internal audit provides independent assurance as the third line. Unlike organizations that must build governance structures from scratch for PQC migration, financial institutions can integrate quantum readiness into existing governance frameworks.

Existing Risk Appetite and Tolerance Frameworks

Financial institutions maintain formal risk appetite statements approved by the board, with quantified risk tolerances and escalation triggers. PQC migration risk can be expressed within this existing framework. Organizations should define a quantum risk appetite statement, track it alongside market, credit, and operational risk, and report it through the same board risk committee process.

Concentrated HSM Vendor Market

The general-purpose and payment HSM market is dominated by three vendors: Thales (payShield and Luna product lines, a leading share of the global market), Utimaco (CryptoServer, u.trust, and Atalla), and Entrust (nShield). Most financial institutions use one or two of these vendors, which simplifies Phase 7 vendor governance.

Utimaco has a strategic partnership with Keyfactor (which acquired InfoSec Global and CipherInsights). The Keyfactor AgileSec Analytics platform integrates directly with Utimaco's u.trust HSM Se-Series, providing automated cryptographic discovery,

inventory, and vulnerability analysis. Financial institutions that already operate Utimaco HSMs may have access to cryptographic discovery capabilities through their existing vendor relationship that they have not yet activated. Similarly, Thales offers visibility through its CipherTrust platform for data-at-rest encryption inventory. Before procuring standalone discovery tooling (Phase 1), check what your current HSM vendor already provides.

Regulatory Examination Experience

Financial institutions undergo regular regulatory examinations and have developed organizational muscle for producing evidence, responding to examiner inquiries, and managing multi-year compliance programs (Basel III/IV, DORA, PCI DSS, SOX, AML/KYC). This experience directly transfers to PQC migration: the evidence-based approach the framework requires (CBOM documentation, risk scoring artifacts, pilot reports, maturity assessments) aligns with the audit-ready culture that regulated financial institutions already maintain.

FS-ISAC as a Coordination and Learning Channel

FS-ISAC's Post Quantum Computing Working Group, chaired by Wells Fargo's Peter Bordow, has published technical guides, a global coordination timeline (January 2026), and is working with the Europol QSFF and the Canadian CFDIR on cross-border coordination. Participation connects the migration team with peers facing identical challenges and reduces the risk of each institution solving the same problems independently. Financial institutions should join the FS-ISAC PQC Working Group as a Phase 0 action.

Mature Third-Party Risk Management (TPRM)

Banks operate some of the most sophisticated vendor due diligence programs in any industry, with structured questionnaire frameworks, on-site assessment capabilities, and contract clause libraries developed over decades of regulatory scrutiny. The framework's Phase 7 (Vendor and Supply Chain Governance) maps directly into existing TPRM processes. The vendor PQC readiness questionnaire in the Universal Framework can be incorporated into existing vendor assessment cycles rather than creating a separate process. Most other sectors must build this vendor governance capability from scratch for PQC migration; banks already have the infrastructure and organizational muscle.

Change Advisory Board Discipline

Banks run formal change advisory boards (CABs) with change freezes around quarter-end, year-end, and regulatory reporting periods. PQC pilots fit naturally into this structure. The rollback requirements in Phase 5 align with existing change management practices: banks already maintain rollback procedures, test in staging environments that mirror production, and schedule deployments in controlled maintenance windows. This

discipline reduces pilot risk and accelerates the path from pilot to production deployment.

Existing Cryptographic Key Management Teams

Most Tier-1 and Tier-2 banks maintain dedicated key management functions within their security operations. These teams manage HSM estates, certificate lifecycles, and encryption key rotation schedules. They have institutional knowledge of the cryptographic estate that accelerates Phase 1 discovery: they know where the HSMs are, what applications use them, and which key ceremonies are performed annually. This knowledge base is a head start that organizations in less-regulated sectors typically lack.

Multi-Year Strategic Planning Alignment

Banks plan technology investments in 3-to-5-year strategic cycles. PQC migration maps naturally into the strategic technology roadmap alongside core banking modernization, cloud migration, and digital transformation. The Phase 0 business case can be positioned within the existing strategic planning process rather than competing as a standalone initiative. Organizations that align PQC migration with scheduled core banking platform upgrades, cloud migration waves, or PKI modernization projects can share costs and reduce the incremental budget required.

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.

The challenges below address broader financial services issues first (regulatory environment, trust infrastructure, core banking, lending, corporate banking, wealth management, and digital banking), followed by payment-infrastructure challenges (summarized here; covered in full depth in the companion Payments Extension), followed by sector-specific considerations for capital markets, insurance, post-trade infrastructure, compliance, and emerging areas.

Challenge 1: Overlapping Regulatory and Standards Requirements

Financial institutions face the most complex regulatory environment 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.

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 2: 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 3: Core Banking Platform Dependency

Core banking systems are the operational backbone of every bank. Major platforms (Temenos T24/Transact, FIS Modern Banking Platform, Finastra Fusion, TCS BaNCS, Infosys Finacle, and numerous regional and legacy platforms) embed cryptographic operations throughout: customer authentication, transaction authorization, inter-system messaging, database encryption, and API security. PQC migration for core banking depends on the vendor's PQC roadmap, and banks have minimal ability to accelerate that timeline.

Banks running multiple core banking platforms across regions or product lines face multiplicative complexity. A global bank operating Temenos in Europe, FIS in North America, and a legacy in-house platform in Asia must coordinate three separate PQC migration streams with three different vendor roadmaps. Phase 7 vendor governance must identify core banking vendors as Strategic Blocking vendors from the outset, and executive-level engagement on PQC roadmap commitments should begin during Phase 0.

Challenge 4: Mortgage and Long-Term Lending Data

Mortgage records carry 30-year data sensitivity lifetimes at minimum. A 30-year fixed-rate mortgage originated in 2026 contains personally identifiable information, property valuations, income documentation, and credit assessments that remain sensitive until at least 2056. Encrypted mortgage documents, title records, and deed registrations transmitted today are HNDL targets with some of the longest sensitivity windows in any sector.

Mortgage servicing platforms frequently use legacy cryptographic implementations that predate current best practices. Many servicers operate on mainframe or mid-range systems with embedded cryptographic routines that are difficult to inventory. Phase 1 discovery should include mortgage origination systems, document management platforms, e-signature services used for mortgage closings, and electronic recording systems used to file deeds and liens.

Digital signatures on mortgage documents (electronic promissory notes, deeds of trust, assignments) create TNFL exposure: a forged signature on a mortgage assignment could transfer ownership of a loan portfolio.

Challenge 5: Corporate and Investment Banking Cryptographic Exposure

M&A advisory generates extremely sensitive data: deal terms, valuations, bidder strategies, and non-public financial information. Virtual data rooms used in M&A due diligence rely on TLS for transport and frequently use document-level encryption. HNDL exposure for M&A data is acute because the information retains material non-public status for years and may be of interest to nation-state economic intelligence programs.

Trade finance documents (letters of credit, bills of lading, warehouse receipts) carry legal weight: a forged letter of credit could authorize the release of goods worth millions. TNFL risk for trade finance is immediate and financial. Treasury management systems managing corporate cash positions, FX hedges, and intercompany lending use SWIFT messaging and host-to-host connections with cryptographic authentication that often run on dedicated infrastructure with long replacement cycles.

Challenge 6: Wealth Management and Private Banking Client Data

Ultra-high-net-worth individuals, family offices, and institutional clients expect the highest levels of confidentiality. Client communication channels in private banking (secure messaging, document sharing, video conferencing) all depend on TLS and carry data that remains sensitive for the lifetime of the client and beyond. Trust and estate

administration involves digital signatures on legal documents with multi-decade validity. Powers of attorney, trust amendments, and beneficiary designations signed today create TNFL exposure that extends until the trust terminates.

Challenge 7: 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, where the quantum-vulnerable dependencies sit in TLS key establishment, certificate-based authentication, and RSA/ECDSA-based JWS or certificate 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 8: Payment Message Format Constraints (See Payments Extension)

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. For detailed treatment of message format constraints, HSM certification, and settlement latency, see the companion Payments Extension, which covers the buffer issues observed in T2's message-handling logic in detail.

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 9: Smart Card and Terminal Constraints (See Payments Extension)

Almost twenty 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 10: The Payment HSM Certification Bottleneck (See Payments Extension)

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 June 2026, no payment HSM product has completed a FIPS

140-3 Level 3 CMVP validation that includes PQC algorithms within the validated module boundary. For general-purpose HSMs, organizations should verify CMVP validation status at the specific product and firmware level rather than relying on vendor marketing claims of PQC support. 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 11: Settlement Latency and Performance (See Payments Extension)

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 12: Cross-Border and Multi-Network Coordination (See Payments Extension)

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 T2's (successor to TARGET2 since March 2023) static reference data. The migration is not just an algorithm swap but an entire parallel PKI infrastructure.

SWIFT has announced that SwiftNet 8.0 is being designed as PQC-enabled, with industry communications indicating a target introduction around 2027 and a migration window on the order of 12 to 18 months. 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 13: Capital Markets Trading Infrastructure

Trading platforms, order management systems, and market data feeds depend on low-latency authenticated messaging. The FIX protocol (Financial Information eXchange) uses digital signatures for trade confirmations and order authentication. Market data feeds from exchanges use signed timestamps for regulatory compliance (MiFID II transaction reporting, SEC Rule 613 CAT). TNFL is the primary threat: a quantum adversary could forge trade confirmations or alter timestamps on market data, undermining regulatory compliance and settlement integrity.

Migration requires coordination with exchanges, clearing houses (CCP), and central securities depositories (CSD) because signature verification happens at multiple points in the trade lifecycle. Organizations should inventory all FIX connections and market data

signature dependencies during Phase 1 and include trading infrastructure in Track B of their two-track migration plan.

Challenge 14: Insurance and Long-Tail Data Sensitivity

Insurance carriers hold data with exceptionally long sensitivity lifetimes: policy records (30+ years for life insurance), actuarial datasets, claims histories, reinsurance treaty documentation, and medical underwriting data. HNDL exposure for this data exceeds most other financial sub-sectors because the sensitivity window extends decades beyond the typical 7-10 year financial record retention.

Reinsurance data exchange between carriers, brokers, and reinsurers involves multi-party cryptographic dependencies similar to the payment chain. The ACORD (Association for Cooperative Operations Research and Development) data standards used in insurance do not yet address PQC. Insurance regulators (NAIC in the US, EIOPA in the EU, PRA in the UK) have not published PQC-specific guidance but are expected to follow the G7 CEG roadmap.

Insurance organizations should prioritize HNDL protection for policy and claims databases during Phase 3 risk scoring, and engage reinsurance partners on PQC readiness during Phase 7 vendor governance.

Challenge 15: Securities, Custody, and Post-Trade Infrastructure

Post-trade infrastructure depends on authenticated messaging between counterparties, custodians, central counterparties (CCPs), and central securities depositories (CSDs). Securities lending and repo transactions, collateral management, corporate actions processing, and settlement confirmation all rely on digital signatures that are vulnerable to TNFL. A forged settlement instruction or custody transfer confirmation could redirect securities worth billions.

Custodian banks face a specific challenge: they hold assets on behalf of institutional clients and must authenticate instructions from those clients. The authentication chain includes the asset manager's instruction, the custodian's confirmation, the CSD's settlement, and the CCP's clearing. Each link uses independent cryptographic infrastructure. Migration requires coordination across the entire post-trade chain, with the same N-party synchronization challenge that characterizes payments.

Challenge 16: Regulatory Reporting and Compliance Data Integrity

Financial institutions submit digitally signed regulatory filings to dozens of authorities: call reports to the OCC/FDIC, stress test submissions to the Federal Reserve, transaction reports under MiFID II and EMIR, Suspicious Activity Reports to FinCEN, and XBRL-tagged financial statements to the SEC. TNFL risk for regulatory filings is systemic: if a quantum adversary could forge a bank's signature on a regulatory submission, they could file fraudulent data that triggers regulatory action or market disruption.

KYC/AML data presents a distinct challenge. Customer identity verification records, beneficial ownership documentation, and transaction monitoring data are subject to retention requirements of 5-7 years minimum. HNDL exposure for KYC/AML data could enable identity fraud or undermine sanctions compliance.

Challenge 17: Cloud Banking and Multi-Cloud Cryptographic Dependencies

Banks migrating to cloud face a double transition: cloud adoption introduces new cryptographic dependencies (cloud KMS, managed encryption services, cloud-native certificate management) at the same time PQC migration requires upgrading the algorithms those services use. AWS KMS, Azure Key Vault, and Google Cloud KMS each have their own PQC roadmaps and validation timelines. A bank using multiple cloud providers must track three independent PQC roadmaps for key management alone.

Cloud-hosted workloads also introduce shared responsibility questions: who is responsible for PQC migration of encryption at rest in a managed database service? The cloud provider controls the encryption implementation, but the bank owns the data and the compliance obligation. Phase 7 should include cloud service providers as a distinct vendor category with specific PQC readiness assessment criteria for managed cryptographic services.

Challenge 18: Financial Crime Prevention and Fraud Detection Data

Transaction monitoring systems, fraud detection platforms, and financial crime case management systems process and store highly sensitive data: suspicious activity patterns, investigation details, intelligence from law enforcement, and cross-border information sharing through FIU networks. This data is encrypted in transit and at rest, creating HNDL exposure that could compromise ongoing investigations if decrypted by a future quantum adversary.

Sanctions screening systems that match transactions against watchlists (OFAC, EU, UN) transmit data between banks and screening providers. The confidentiality of screening

results (which transactions were flagged, which were cleared) is itself sensitive. Financial crime data retention requirements (typically 5-7 years minimum, often longer for ongoing cases) create a defined HNDL exposure window that should inform Phase 3 risk scoring.

Challenge 19: Digital Assets and Blockchain Quantum Vulnerability (See Digital Assets Extension)

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 20: 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.

ALIGNMENT WITH UNIVERSAL FRAMEWORK V2.1

The Universal Framework v2.0 introduced the structural foundations below. v2.1 added positions and sections with further financial services implications; those are covered in the subsections that follow the v2.0 foundations. The remaining Universal v2.1 additions (the data-at-rest decision framework in Activity 5.6, the AI-assisted migration position in 5.7 with its Phase 1 tool category, cloud and SaaS shared responsibility in 7.7, the Accelerated Execution Profile in 4.7, the risk-weighted coverage KPI, algorithm sovereignty and standards fragmentation, crisis communications, the skills matrix, and Appendices G and H) apply to financial institutions as written, with two notes. Supervisory record-retention regimes supply the confidentiality-horizon inputs the data-at-rest decision framework requires, so the Activity 5.6 strategy choice is made per retention class, not per system. And the counterparty coordination pattern in Activity 7.6 is the general case of the interbank, correspondent, and market-infrastructure coordination this extension already covers; where the two overlap, this extension's guidance governs.

Two-Track Migration Model in Financial Services

The Universal Framework v2.0 introduces an explicit two-track migration model. For financial services, the two tracks map as follows:

Track A (Confidentiality / Key Exchange): External-facing TLS on internet banking, mobile APIs, and Open Banking endpoints. Interbank messaging encryption (SWIFT, correspondent banking channels). Customer data in transit across all digital channels. This track addresses HNDL, which is the most immediately exploitable threat given the long sensitivity lifetime of financial data.

Track B (Integrity / Signatures / PKI): Trading infrastructure authentication (FIX protocol signatures, trade confirmations). Regulatory filing signatures and audit trail integrity. Code signing for banking applications and firmware. PKI root certificates with 10-20 year

validity periods. This track addresses TNFL, which could enable forged payment instructions, altered settlement records, or fraudulent regulatory submissions.

Most financial institutions should start Track A immediately (hybrid key exchange on customer-facing and interbank channels) and launch Track B within 90 days (PKI lifetime assessment, trading infrastructure signature inventory, code signing review). Both tracks should run as parallel workstreams with separate milestones.

FIPS Validation Gap Impact

Financial services operates predominantly in FIPS-aware or FIPS-required environments. The current absence of FIPS 140-3 validated PQC modules (earliest expected mid-2027) directly constrains production deployment timelines. Financial institutions should classify their systems using the Universal Framework's environment classification and sequence their migration accordingly: begin pilots in unrestricted environments (development, staging) now, deploy to FIPS-aware systems with documented risk acceptance, and plan FIPS-required production deployment for the period following module validation.

The FIPS 140-2 sunset on September 21, 2026 creates additional urgency: financial institutions must plan their FIPS 140-3 migration alongside their PQC migration, and the two timelines intersect at the HSM layer.

Merkle Tree Certificates for Customer-Facing Infrastructure

For public-facing web banking and API infrastructure, Merkle Tree Certificates (MTCs), backed by Google, Cloudflare, and Let's Encrypt, are the emerging preferred path for post-quantum authentication in Chrome-trusted public Web PKI. Chrome has indicated it has no immediate plan to add traditional PQC X.509 certificates to the Chrome Root Store. Financial institutions should invest in ACME-based certificate automation now, both to prepare for MTCs and to comply with the CA/Browser Forum's trajectory toward 47-day maximum validity for publicly trusted TLS certificates by March 2029. Internal banking PKI (interbank mTLS, HSM certificate chains, internal service mesh) will continue on X.509 with PQC algorithms.

CNSA 2.0 Voluntary Adoption

An increasing number of financial institutions are adopting CNSA 2.0 algorithm requirements (ML-KEM-1024, ML-DSA-87 at NIST Security Level 5) as their internal standard, even though CNSA 2.0 is designed for national security systems. The rationale: financial institutions that serve government clients need CNSA 2.0 compliance for those

relationships, and maintaining two separate algorithm standards (one for government, one for commercial) adds operational complexity. Adopting CNSA 2.0 as the single standard simplifies compliance across both contexts.

Note that CNSA 2.0 excludes SLH-DSA, which means financial institutions adopting this standard are committing to lattice-based algorithms for general-purpose digital signatures (though CNSA 2.0 retains stateful hash-based signatures, LMS and XMSS, for software and firmware code signing). This is a defensible choice for institutions that prioritize interoperability with government clients, but it forecloses the SLH-DSA conservative fallback.

Hybrid and Composite Signatures: The Default for Track B

Universal v2.1 takes the position that composite or dual signatures (classical plus PQC) are the default for Track B wherever toolchains support them, with solo ML-DSA treated as a recorded risk decision. For financial services the case is strongest exactly where Track B matters most: regulatory filings, trade confirmations, e-signed legal documents, and audit trails must remain verifiable for years or decades, and a composite signature preserves verifiability even if one component algorithm is later broken or an implementation flaw surfaces in first-generation PQC deployments. The Phase 5 pilot list in this extension already operationalizes the position: the internal code signing pilot dual-signs with ML-DSA-65 alongside existing ECDSA/RSA. Where signature size is the binding constraint, that is largely a payment message problem; see the Payments Extension for sequencing guidance under ISO 8583 and ISO 20022 field limits. Institutions that deploy solo ML-DSA in any Track B system should document it as a risk decision per the Universal position.

Algorithm Weighting: ECC Is Not a Safe Harbor

Universal v2.1 introduces algorithm-specific vulnerability weighting in Phase 3: quantum attack cost scales with key size, not classical strength, so 256-bit ECC keys are at least as exposed as RSA-2048 and considerably more exposed than RSA-3072. This cuts against a common sequencing intuition in financial services. Open Banking token signing on ES256, ECDSA across FIX and trading infrastructure, and modern P-256-standardized API estates are not safer than the RSA-legacy core banking platforms behind them: on a pure attack-cost basis they sit at least one tier higher. Institutions should not let “modern crypto” serve as a proxy for “quantum-safe” in Phase 3 scoring, and should record algorithm family and key size for every CBOM entry so the weighting can be applied mechanically rather than by impression. Digital asset signing keys, almost universally on 256-bit curves, are the extreme case; see the Digital Assets Extension.

The Identity Stack in Track B

Universal v2.1 brings the identity stack explicitly into Track B scope. For financial services the surface is broad and growing: customer authentication is moving onto passkeys (FIDO credentials on P-256) across retail banking, Open Banking rests on OAuth/OIDC/FAPI token signing with ES256 or PS256 JWS, institutional and workforce access runs on SAML federation and certificate-based smart card logon (including trading floor PKI), and e-signature platforms anchor document workflows. These are long-lived signing keys and enrolled credentials, not ephemeral session material. Two actions follow: carve an identity slice in the Phase 1 inventory and Phase 2 CBOM (identity providers, token signing keys, federation trust chains, authenticator policies), and add the credential migration question (how enrolled passkeys, certificates, and device-bound credentials will be re-enrolled or migrated when signature algorithms change) to Phase 7 vendor governance for identity and authentication vendors. Short-lived access tokens are low priority; the signing keys and root-of-trust credentials behind them are standard Track B targets.

SP 800-208: The Deploy-Now Signature Migration

Universal v2.1 foregrounds stateful hash-based signatures (LMS and XMSS, NIST SP 800-208) as the component of Track B that deploys now. They are standardized, conservative, and, as the CNSA 2.0 subsection above notes, retained under CNSA 2.0 specifically for software and firmware code signing, which means institutions voluntarily adopting CNSA 2.0 are already committed to them for that use. The deploy-now action for financial services: move application release signing and firmware signing pipelines to SP 800-208 signatures, dual-signed with classical during transition, operated from HSM-backed signing infrastructure. The state-management constraint that makes these schemes unsuitable for general-purpose signing is satisfied by the controlled, ceremonial signing environments banks already operate. Banking application release pipelines and branch device firmware are the natural first targets; for terminal and ATM fleet firmware specifics, see the Payments Extension.

Securing the CBOM and Program Artifacts

Universal v2.1 adds Activity 2.5: the CBOM and migration program artifacts are themselves high-value targets. A financial institution's CBOM maps every cryptographic weakness, the HSM estate, the long-retention data stores, and the unmigrated interfaces: a target-selection document for any adversary, from financially motivated groups to nation-state economic intelligence. The sector-specific exposure is examination culture: regulators, internal and external auditors, QSAs, and counterparty

due diligence teams all generate standing requests for exactly this material. Apply Activity 2.5's controls through the three lines of defense: examiners and counterparties receive point-in-time extracts scoped to their inquiry rather than standing access to the queryable inventory, the second line owns the access policy, the third line audits adherence to it, and the CBOM repository joins the SOC's high-sensitivity exfiltration watch list.

Verification, Decommissioning, and Program Closure

Universal v2.1 adds a Migration Verification & Program Closure section defining what "done" means: observed cryptographic negotiation on the wire rather than configuration-file assertions, negative testing that classical-only connections are actually refused once policy requires it, and an evidence standard for retiring systems and keys. For financial services this is examination material. Verification records (observed handshakes, negative test results, decommissioning logs with key destruction certificates) are precisely the artifacts supervisory examinations and DORA ICT risk documentation will ask for, and they are far stronger evidence than attestations. Decommissioning must include trust-store cleanup across branch, ATM, and client-side estates, because a key is only retired when nothing trusts it. Closure means handover into business as usual through the three lines: second-line standing ownership of cryptographic risk reporting, with algorithm transitions becoming routine change management rather than program-level events.

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.

Three Lines of Defense Integration

The Universal Framework's governance model maps directly into the three lines of defense structure used by most regulated financial institutions. The first line (business units and technology operations) owns PQC migration execution within their domains. The second line (risk management, CISO function, compliance) provides independent oversight of migration progress, risk acceptance decisions, and regulatory alignment. The third line (internal audit) provides independent assurance that the migration program is operating as designed and producing reliable evidence. This mapping means financial institutions do not need to create parallel governance structures for PQC migration; they need to integrate quantum readiness into the existing risk governance architecture, which is faster and more sustainable.

The board risk committee should receive quarterly PQC migration reporting as a standing agenda item, using the same risk appetite and tolerance framework applied to other technology risks. Quantum risk metrics (CBOM coverage, migration progress, vendor readiness) should be incorporated into the enterprise risk dashboard rather than reported through a separate channel.

Phase 1 — Discovery & Inventory

Expanded Scope: Financial Services 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. The first four apply across all financial services sub-sectors; the remaining tracks are payments-specific (see the Payments Extension for detailed guidance):

- **Core banking and enterprise application cryptography:** Inventory cryptographic dependencies in core banking platforms, loan origination systems, treasury management, wealth management, and trading platforms. For each, identify whether cryptographic operations are vendor-controlled or institution-configurable.
- **Customer-facing digital channel cryptography:** Inventory TLS configurations, certificate pinning, and authentication cryptography across internet banking, mobile banking, wealth management portals, and corporate banking platforms. These are the primary Track A (key exchange) targets.

- **Regulatory submission and document signing infrastructure:** Inventory all systems producing digitally signed regulatory filings, trade confirmations, audit reports, mortgage documents, and legal contracts. Include e-signature platforms. These are Track B (signature) targets.
- **Long-retention data stores:** Identify all encrypted data stores with retention periods exceeding 10 years: mortgage records, insurance policy records, trust and estate files, M&A archives, compliance records, and KYC/AML data. Highest HNDL priority for data-at-rest.
    - **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) customer-facing digital channels (internet banking, mobile banking, wealth management portals) as the broadest HNDL exposure surface, (2) interbank messaging and correspondent banking encryption, (3) HSM-protected key material across trading, treasury, and settlement systems, (4) regulatory submission and document signing infrastructure (Track B targets), and (5) long-retention data stores (mortgage records, policy records, M&A archives, compliance data). For payment-specific scoping priorities, see the Payments Extension. 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.

Discovery Tooling Advantage: Existing HSM Vendor Relationships

Financial institutions should assess whether their current HSM vendor offers integrated cryptographic discovery capabilities before procuring separate discovery tools. Utimaco's partnership with Keyfactor (AgileSec Analytics) provides automated discovery of cryptographic assets and their management status directly from the HSM management plane. Thales offers comparable visibility through its CipherTrust platform for data-at-rest encryption inventory. These vendor-provided capabilities may cover a significant portion of the Phase 1 discovery scope at lower cost and faster deployment than standalone discovery tools, because the HSM vendor already has deep integration with the institution's cryptographic infrastructure.

This does not eliminate the need for network-level and code-level discovery (the Universal Framework's Layers 1-3), but it may provide a faster start on Layer 4 (embedded/third-party) and infrastructure-layer cryptographic inventory.

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. PCI DSS 12.3.3 creates a documentation and review obligation, not a PQC remediation mandate; its value for PQC migration is that it provides an existing compliance-backed mechanism for building and maintaining a cryptographic inventory. 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 scores each CBOM entry across four dimensions: data sensitivity and exposure window (HNDL risk), TNFL risk, regulatory pressure, and migration feasibility. 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	Internet banking and mobile banking TLS endpoints, corporate banking host-to-host connections, interbank messaging channels (including SWIFT), settlement system connections, and HSM-protected key material	Highest HNDL exposure, systemic criticality, regulatory visibility. External-facing with long data confidentiality requirements.
Tier 2	Open Banking API endpoints, trading platform authentication, regulatory submission signing infrastructure, card network CA hierarchies, external payment APIs, digital asset custody (see Digital Assets Extension)	High HNDL and TNFL exposure. Multi-party coordination required. Consumer-facing reputational risk.
Tier 3	Core banking platform TLS, wealth management portals, internal API gateways, mortgage servicing platform encryption,	Important but internally controlled. Can be migrated on institutional timeline without external dependencies.

	database encryption, application-level code signing	
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:** Target introduction around 2027 with PQC enablement and a migration window on the order of 12 to 18 months.
- **Card network PQC timelines:** Visa and Mastercard CA migration timelines (not yet publicly committed as of June 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:

- **Internet banking or external API with hybrid TLS:** Enable hybrid ML-KEM-768 + X25519 key exchange on a non-critical internet banking endpoint or external 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.

Non-Payment Pilot Targets

Beyond the payment-specific pilots listed above (which are covered in detail in the Payments Extension), financial institutions should consider the following pilot targets for broader banking and capital markets:

Internet banking TLS endpoints: Enable hybrid key exchange (X25519+ML-KEM-768) on the institution's primary online banking portal. Client-side support is universal (all major browsers default to PQC). This is the lowest-friction pilot target because the institution

controls the server configuration and the clients are already PQC-capable. Measure hybrid negotiation rates, handshake latency impact, and middlebox/WAF compatibility.

Mobile banking API endpoints: Enable hybrid key exchange on the mobile banking API gateway. Mobile app certificate pinning configurations may need updating. Test against all supported app versions and mobile platforms.

Corporate banking host-to-host connections: Treasury management system connections, cash management platforms, and corporate banking portals that use dedicated TLS channels. These connections are typically lower-volume and higher-value, making them suitable for early hybrid deployment with careful monitoring.

Internal code signing for banking applications: Pilot dual-signing (ML-DSA-65 alongside existing ECDSA/RSA) for one internal banking application's release pipeline. This validates the code signing toolchain without affecting production verification.

Document signing for regulatory submissions: Pilot PQC signatures on one category of regulatory filing in a test/sandbox environment, in coordination with the relevant regulator if available.

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 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. The table below groups vendors by their role in the financial services infrastructure. For payments-specific vendor engagement guidance (card networks, RTGS operators, payment gateway providers), see the Payments Extension:

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

Key Regulatory and Industry Coordination Developments

Financial services faces the densest regulatory environment of any sector for PQC migration. The following developments shape migration planning and timelines. PCI DSS v4.0 Requirement 12.3.3 (effective March 2025) already mandates cryptographic cipher suite and protocol documentation. The G7 Cyber Expert Group published a six-phase roadmap targeting 2030-2032 for critical financial systems (January 2026). NIST IR 8547 proposes deprecating RSA and ECC at 112-bit security after 2030 and disallowing all quantum-vulnerable asymmetric cryptography after 2035. The EU Coordinated Implementation Roadmap requires national PQC strategies by end of 2026 and critical-sector quantum safety by end of 2030. Beyond these, several coordination bodies and regulators have published financial-services-specific guidance:

Europol QSFF Prioritization Framework (January 2026): Published jointly with FS-ISAC and the CFDIR Quantum-Readiness Working Group. Provides an operational prioritization methodology for financial services PQC migration, balancing quantum risk against migration time. This is the closest external framework to this extension's Phase 3 risk scoring methodology. Financial institutions should cross-reference their Phase 3 outputs with the Europol methodology for regulatory defensibility.

FS-ISAC Global Coordination Timeline (January 2026): Calls for industry-aligned action plans and coordinated global transition milestones. Wells Fargo's Peter Bordow (FS-ISAC PQC Workgroup Chair) and Banco Santander's Jaime Gomez Garcia (QSFF) are driving cross-sector coordination that financial institutions should participate in.

HKMA Quantum Preparedness Index (February 2026): The first banking regulator to score sector-wide PQC readiness. Financial institutions operating in Hong Kong should expect examination questions based on this index. Other APAC regulators are likely to follow.

DORA (effective January 2025): The Digital Operational Resilience Act requires state-of-the-art cryptography and ICT risk management that includes emerging technology threats. While DORA does not name PQC explicitly, its requirement for "state of the art" cryptography, explicit crypto-agility obligations, and risk-based ICT management standards create what amounts to an indirect PQC mandate: organizations that fail to plan for PQC when the quantum threat is documented and NIST standards are published will struggle to demonstrate compliance with DORA's own provisions.

BIS Quantum Roadmap for Banking (2025): BIS Papers No. 158 provides a quantum risk assessment framework for banking supervisors. Central banks are using this framework to shape examination expectations.

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	Target around 2027; 12-to-18-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. Actions 1-4 apply broadly across financial services; actions 5-8 include payments-specific items covered in detail in the Payments Extension:

#	Action	Timeline	Framework Phase
1	Launch a structured cryptographic inventory across internet banking, core banking, and trading platforms. For PCI-scoped entities, align with Requirement 12.3.3 so the same inventory satisfies PQC readiness and PCI compliance	0–3 months	Phase 1 / Phase 2
2	Map the complete HSM estate (general-purpose and payment HSMs) by model, firmware version, and PQC readiness status. Check whether your HSM vendor offers integrated discovery capabilities (Utimaco/Keyfactor, Thales/CipherTrust). 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, risk management, compliance, treasury, retail banking, corporate banking, capital markets, 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 internet banking or 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 —** https://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 —** https://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 —** https://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 —** https://postquantum.com/post-quantum/hybrid-cryptography-pqc/ — Hybrid schemes in TLS, SSH, IPsec; standards alignment; pilot design.
- **Infrastructure Challenges of Dropping In PQC —** https://postquantum.com/post-quantum/infrastructure-challenges-pqc/ — How PQC stresses real infrastructure: handshakes, cert chains, CPU/memory, middleboxes.
- **Rethinking CBOM —** https://postquantum.com/post-quantum/rethinking-cbom/ — Challenges the completeness model; proposes the Minimum Viable CBOM approach.
- **120,000 Tasks: Why PQC Migration Is Enormous —** https://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 —** https://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.

QUANTUM READY: THE COMPANION BOOK

Quantum Ready (QuantumReady.com) is the book-length companion to this framework, written by the same author. Where this document is deliberately methodology-grade (prerequisites, activities, outputs, decision logic). The book provides the complete treatment: the reasoning behind each phase, extended case examples from real migration programs, sector narratives, and guidance for leading the program from the first board conversation through closure. The two are maintained in alignment: the framework is updated as the field moves, and the book supplies the depth that a methodology document omits by design.

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