SEPTEMBER 2026

APPLIED QUANTUM

THE APPLIED QUANTUM PQC MIGRATION FRAMEWORK

FINANCIAL SERVICES EXTENSION

Banking, capital markets and insurance – *sector-specific challenges and framework adaptations*

Version 3.0 – September 2026

Marin Ivezic

CEO, Applied Quantum

Author, PostQuantum.com

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

COPYRIGHT AND LICENSE

DISCLAIMER

This framework 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 PQC as of September 2026. These references may become outdated quickly. Readers should verify current status against primary sources before making implementation decisions; movement between editions is published through the PQC Migration Brief.

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

NIST IR 8547, referenced throughout for deprecation and disallowance timelines, remains an Initial Public Draft at the date of this edition; the deprecation and disallowance dates it proposes are cited as anchors and re-checked at each release. Federal agencies and their contractors should reference the final version when it publishes.

ABOUT THIS DOCUMENT

Document type	Enterprise methodology and practitioner framework
Parent document	The Applied Quantum PQC Migration Framework – Universal – v3.0 (September 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 v3.0 and its 8-phase lifecycle; working knowledge of banking, capital markets and insurance technology estates, financial messaging and market infrastructure, and supervisory examination
Scope	Industry-specific challenges and phase-by-phase framework adaptations for financial services (banking, capital markets,

	insurance). For payments-specific guidance (card networks, RTGS, SWIFT scheme mechanics, 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.
Status	Version 3.0 - published September 2026

VERSION HISTORY

Version	Date	Changes
2.0	June 2026	Major version. Three methodological changes: (1) two-track migration model separating key exchange (HNDL) and signature/PKI (TNFL) as parallel tracks; (2) PKI architecture fork with definitive position on Merkle Tree Certificates for public Web PKI; (3) FIPS 140-3 validation gap as hard deployment constraint with environment classification. New Program Foundation sections: SOC Implementation (five detection use cases, four incident response playbooks, five tabletop exercises, three-horizon quantum CTI model), GRC Implementation (17-indicator cascading KRI framework, risk appetite statements, regulatory intelligence process, audit and assurance, GRC-SOC handoff). Expanded Program Foundations: Governance (program leadership, board oversight, three lines of defense), Crypto-Agility (five-dimensional operational discipline with four-year implementation roadmap), Skills & Team Structure (team sizing, build/borrow/buy framework, crypto champion program). Also added: cost estimation methodology, NIST CSWP 39 crypto-agility alignment, 2026–2030 regulatory deadline convergence analysis, multinational hybrid navigation framework, deployment ecosystem status data, algorithm pipeline update (9 additional signature candidates, FN-DSA/HQC status, CNSA 2.0 requirements), objection-handling appendix (Appendix F). All sector extensions updated to v2.0.
2.1	June 2026	Targeted update. Activity 3.3 sequencing harmonized with the two-track model; explicit position on hybrid/composite signatures; algorithm-specific vulnerability weighting added to Phase 3 risk scoring (ECC/RSA quantum resource analysis); SP 800-208 hash-based signatures foregrounded as the deploy-now component of Track B. New: Activity 2.5 (Secure the CBOM and Program Artifacts), Migration Verification &

Version	Date	Changes
		Program Closure section, identity and authentication stack in Track B scope. Added: reference program economics (0.2c), confidentiality-horizon method (1.1), evidence dossier as litigation defense, M&A due diligence, procurement model-language references, additional common failures and benefit arguments. Web PQC adoption datapoint corrected to F5 Labs mid-2025 attribution. Companion book (Quantum Ready) cross-references added. Also added: data-at-rest decision framework (5.6); AI-assisted migration position (5.7) with a Phase 1 tool category; counterparty coordination (7.6); cloud shared responsibility and SaaS (7.7); Accelerated Execution Profile (4.7); risk-weighted coverage KPI; algorithm sovereignty and standards fragmentation; crisis communications and industry information sharing (GRC); skills matrix; role-based reading paths and right-sizing profiles; Appendix G (framework crosswalk); Appendix H (protocol coverage matrix).
3.0	September 2026	Major version, published with Universal v3.0. Crypto-agility as the program's method read for financial institutions: the agility objective stated for the sector (a bank is crypto-agile when it can change the algorithm on its own edge, issuers and signing services on a planned date and can name the date on which each shared interface will follow its network), the agility criterion and a rehearsal per wave on the customer-facing edge, the internal issuers and the signing services, scheduled outside the change advisory board's freezes, "migrated with agility debt" as the expected recorded state for the vendor-locked core platform and the network-set shared interfaces, and closure at zero unaccepted agility debt with the four verification dispositions. The banking version of the shared-machinery argument with the AI-security mandate, which the Universal cites (Phase 0), and the dual-outcome framing in the supervisor's terms. Qualified signatures and seals in onboarding, lending and custody documentation, with the keyholder-liability question stated (alignment section). HNDL restated as inference from demonstrated capability and the Federal Reserve attribution corrected to the staff working paper FEDS 2025-093, cited under its own disclaimer. The validation subsection rewritten to the per-product rule (CMVP certificates #5247, April 2026, and #5497, August 2026, each with its qualifications), correcting the June 2026 statement; the systemic-loss figures re-attributed to the Hudson Institute's

Version	Date	Changes
		2023 analysis as relayed in the Project Leap Phase 2 report, and the Project Leap findings and the Swift release dates stated to the source texts; the Merkle Tree Certificates subsection aligned to the Universal (Chrome Quantum-resistant Root Store Q3 2027; Let's Encrypt June 3, 2026; SC-081v3 lifetimes). "Attest, do not send" as the rule for examiners, QSAs and counterparties. Three new alignment subsections (the agility criterion and rehearsal; evidence grades and the coverage denominator; vendor dates and questions). Phase adaptations mirror the v3.0 method: dual-outcome charter and named Crypto-Agility and Cryptographic Record owners (Phase 0); the three lines by function; evidence grades, the enumerated denominator and an identity-stack track (Phase 1); the minimum record with the Profile as informative carriage (Phase 2); the two sector dimensions restated as factors inside Dimensions 2 and 3 with the arithmetic, model-risk treatment, delivery state, the agility-debt register and the Profile's fs:* fields with the CCF Financial Services extension cross-referenced (Phase 3); firmness grades on every external date, two results per gate record and the Re-Baseline Protocol (Phase 4); the rehearsal per wave and the wave-exit criterion (Phase 5); the four-field HSM and KMS register with entropy references, payment HSMs grouped (Phase 6); questionnaire order, contractual crypto-agility with FINMA Guidance 05/2026 as the example, the acceptance test and the one-afternoon test (Phase 7). Regulatory content restructured under E1: three named instruments in the prose (PCI DSS 12.3.3; DORA with Delegated Regulation (EU) 2024/1774 Article 6; FINMA Guidance 05/2026); the map rebuilt at four columns with status and enforcement-tier columns, the HKMA index dated to its July 27, 2026 publication and FINMA added, both without scores, and the jurisdiction roster replaced by the Global PQC Migration Clock pointer. Commercial vendor and product names moved to Tool and Vendor References. Payments content grouped and pointed to the Payments Extension throughout. Maturity supplement on the Universal's 0 to 5 scale with a signature-track indicator per level; four agility KPIs; ten immediate actions. Requirements register generated as Appendix J. About block aligned to the Universal.

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 banking, capital markets and insurance. For each topic, this extension identifies unique sector challenges and then maps specific adaptations to the relevant Universal Framework phase; the Universal's Financial Services note (Sector Adaptation Notes) is the binding summary, and its Payments note, expanded in the Payments Extension, carries scheme, terminal and payment-HSM constraints. Readers should have the Universal Framework open alongside this document and cross-reference its phase definitions, maturity indicators, and templates.

WHAT'S NEW IN V3.0

Version 3.0 of the Financial Services Extension publishes with Universal Framework v3.0 (September 2026). Crypto-agility is the program's organizing method and measured end state, and this extension states the ruling for the sector: a bank is crypto-agile when it can change the algorithm on its own customer-facing edge, its own issuers and its own signing services on a planned date, and can name the date on which each shared interbank and scheme interface will follow its network; the agility criterion and the rehearsal per wave run on those layers, "migrated with agility debt" is the expected recorded state for the vendor-locked core platform and the network-set interfaces, and closure requires zero unaccepted agility debt under the four verification dispositions. Regulatory content states the mechanism and three named instruments; the sector bodies are in the map with status and enforcement tier, and the jurisdiction roster is in the Universal's Regulatory Timeline Context and on the Global PQC Migration Clock page.

Content the Universal cites, and two positions stated for the sector. The banking version of the shared-machinery argument with the AI-security mandate is written in Phase 0, as the Universal's Activity 0.2b says it is: one inventory, one vendor register and one legacy-remediation backlog for both obligations, funded once under the readiness heading, with the dual outcome stated in the supervisor's terms (readiness is what the supervisor scores; crypto-agility is what supervisory outsourcing guidance now asks contracts to contain). Qualified signatures and seals in onboarding, lending and custody documentation are treated in a new alignment subsection that applies the Universal's Qualified Trust Services position to the three document classes and states the keyholder-liability question where a statutory presumption of validity meets a forgeable algorithm. Challenge 2 records that supervisory instruments acknowledge the forgery risk without measuring it, and the supplements report the signature track on its own line.

Corrections made in the open. Harvest-now-decrypt-later is stated as inference from demonstrated capability, never as observed harvesting; the June 2026 sentence that the Federal Reserve had "explicitly acknowledged" the risk is corrected to the staff working paper it rests on (Mascelli and Rodden, FEDS 2025-093, September 2025), quoted at its own strength and cited under the paper's disclaimer that the views are the authors'. The June 2026 statement that no FIPS 140-3 validated PQC module existed, with validation expected in mid-2027 at the earliest, was wrong when published: CMVP certificate #5247 (the Go Cryptographic Module, FIPS 140-3 Level 1 software, April 27, 2026) lists ML-KEM key generation and encapsulation-decapsulation at ML-KEM-768 and ML-KEM-1024 among its approved algorithms, and CMVP certificate #5497 (the Crypto4A QASM Cryptographic Module, FIPS 140-3 Level 3 hardware, August 19, 2026) lists ML-KEM, ML-DSA, SLH-DSA and LMS inside the approved boundary, with two qualifications that travel with every citation (the module does not establish SSPs using an approved KEM, and HSS is vendor-affirmed rather than CAVP-tested); validation is decided per product, per operation and per certificate. The systemic-loss figures are attributed to the Hudson Institute's April 2023 "Prosperity at Risk" analysis as relayed in

the BIS Project Leap Phase 2 report (the June edition attributed them to a Citi Institute analysis; the six-month-recession framing is the study's own and an earlier form of this correction wrongly called it an addition); the Project Leap Phase 2 findings are stated to the report's text (the June edition described the missing certificate as a failure and the message-size finding as a buffer overrun); and the Swift statements replace the June edition's "around 2027" and "12 to 18 months" (Alliance Release 8.0 planned for end July 2027, Release 7.9 needed first by the majority of the community, SwiftNet 8.0 in 2027). The HKMA Quantum Preparedness Index is dated to its first publication on July 27, 2026 (the June edition dated the February 2026 announcement). The Universal's three inventory tracks are named as the Universal names them (the June edition listed discovery layers in their place). The named bank DLT platform in Challenge 19 is replaced by the class it belonged to.

Alignment section, adaptations and supplements. The alignment section is rebuilt on v3.0, its FIPS subsection rewritten to the per-product rule and retitled, its Merkle Tree Certificates subsection aligned to the Universal's PKI Architecture Evolution (Chrome Quantum-resistant Root Store targeted Q3 2027; Let's Encrypt's June 3, 2026 decision; no ML-DSA roots in the major trust stores; the SC-081v3 lifetimes), its closure subsection rewritten to the four dispositions, and three subsections added (the agility criterion and rehearsal; evidence grades and the coverage denominator; vendor dates and questions). The phase adaptations mirror the v3.0 method where this extension already adapts the element: named Crypto-Agility and Cryptographic Record owners and the three lines by function (Phase 0); evidence grades, the enumerated denominator and an identity-stack track, with the payments tracks grouped (Phase 1); the minimum record with the Applied Quantum CBOM Profile as informative carriage (Phase 2); the sector's two dimensions restated as factors inside Dimensions 2 and 3 with the Universal's arithmetic, model-risk treatment under the institution's model risk management function, delivery state, the agility-debt register and the Profile's fs:* fields with the Cryptographic Concentration Framework's Financial Services extension cross-referenced (Phase 3); firmness grades on every external date, two results per gate record and the Re-Baseline Protocol (Phase 4); the rehearsal per wave and the wave-exit criterion, with the pilots regrouped banking first (Phase 5); the four-field HSM and KMS register with entropy references leading Phase 6 and payment HSMs grouped behind it; the questionnaire order, contractual crypto-agility with FINMA Guidance 05/2026 (July 9, 2026) as the one supervisory example, the acceptance-test rehearsal, the certificate-authority questions and the one-afternoon test (Phase 7). The regulatory map is rebuilt at four columns as a dated snapshot with status and enforcement-tier columns, with FINMA added and the MAS row not carried; the maturity supplement is re-based on the Universal's 0 to 5 scale with a signature-track indicator per level; the KPI supplement gains a TNFL exposure line and the four agility KPIs; ten immediate actions include naming the agility owner and scheduling the first rehearsal. Commercial vendor and product names move to Tool and Vendor References; Further Reading adds the July 2026 HNDL analysis, the HKMA and FINMA analyses and the Global PQC Migration Clock; Appendix J lists the extension's own requirements.

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.

TOOL AND VENDOR REFERENCES

This framework references specific tools, products, and vendors as illustrative examples to help practitioners understand the categories of capability available. A mention does not constitute an endorsement, recommendation, or assessment of fitness for any particular environment. 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.

The body of this edition names categories and capability requirements. Commercial vendors appear in the body only where a dated public fact is itself the evidence (an announcement, a measurement, a published roadmap), and the counterparties a reader deals with regardless of choice (SWIFT, the card schemes, RTGS operators, FS-ISAC, the regulators) are named as public facts. The references below carry the names the body relied on in the June 2026 edition, as named there and verified September 2026 where a date is given, and are maintained on PQCFramework.org between editions.

General-purpose and payment HSMs (sector characteristics; Challenge 10; Phase 4; Phase 6; Phase 7): the June 2026 edition named Thales (payShield and Luna product lines), Utimaco (CryptoServer, u.trust and Atalla) and Entrust (nShield) as the three vendors supplying most of the estate, and Futurex among the payment HSM suppliers. Thales Luna HSM firmware 7.9 (July 2025) added native ML-KEM and ML-DSA, with FIPS 140-3 Level 3 validation of that firmware in progress at release. Utimaco Quantum Protect (April 2025) is an application package for the u.trust General Purpose HSM Se-Series, activated in the field without a hardware exchange, carrying ML-KEM, ML-DSA, LMS/HSS and XMSS/XMSS-MT; older Utimaco models outside the Se-Series are a hardware question. The payment HSM product lines (Thales payShield, Utimaco Atalla, Futurex) carry their own PQC firmware and PCI certification timelines, unverified at this edition; the Payments Extension carries them. Validation is read per product from the CMVP list, never from a product name.

Discovery capability reachable through the HSM vendor (sector characteristics; Phase 1): the June 2026 edition named the Utimaco partnership with Keyfactor (which acquired InfoSec Global and CipherInsights), whose AgileSec Analytics platform integrates with the u.trust HSM Se-Series, and Thales CipherTrust for data-at-rest encryption inventory. Dedicated cryptographic discovery platforms are listed in the Universal's Tool and Vendor References and analyzed on PostQuantum.com.

Core banking platforms (Challenge 3; Phase 7): the June 2026 edition named Temenos T24/Transact, FIS Modern Banking Platform, Finastra Fusion, TCS BaNCS and Infosys Finacle as the major platforms, beside numerous regional and legacy platforms. The list describes the installed base this extension was written against; it is not an assessment of any vendor's PQC readiness, which is established per product through the questionnaire in Phase 7 and graded for firmness.

Cloud key management (Challenge 17; Phase 6): AWS KMS, Azure Key Vault and Google Cloud KMS publish their own PQC key-type roadmaps; check the current status per service and region, and record the provider as a dependency boundary in the Activity 6.2 register.

Smart card silicon (Challenge 9; Phase 4): the June 2026 edition named IDEMIA with GlobalFoundries (28 nm chips targeted for 2026 mass production) and Infineon equivalents; the Payments Extension carries the current status.

Validated modules (alignment section; Challenge 10): CMVP certificate #5247 (the Go Cryptographic Module, Geomys LLC, a FIPS 140-3 Level 1 software module validated April 27, 2026) lists ML-KEM key generation and encapsulation-decapsulation at ML-KEM-768 and ML-KEM-1024 only, with no ML-DSA; CMVP certificate #5497 (the QASM Cryptographic Module, Crypto4A Technologies, a FIPS 140-3 Level 3 hardware module validated August 19, 2026) lists ML-KEM, ML-DSA, SLH-DSA and LMS as approved algorithms, with the qualifications stated in the validation subsection. Some validated modules list PQC only among their non-approved services, and a listing of that kind does not count; payment HSMs, which also carry a PCI PTS HSM approval, are checked one product at a time. Consult the CMVP validated-modules and Modules in Process lists for the current state.

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.org, a dedicated companion site for this framework, drawing on relevant content from PostQuantum.com.

Two sibling Applied Quantum properties carry work this framework cites rather than repeats. The Applied Quantum CBOM Profile, the property taxonomy layered on CycloneDX that Phase 2 cites by minimum version, publishes at CBOMProfile.org. The Cryptographic Concentration Framework, which measures cryptographic concentration beneath the vendor layer and consumes a Profile-conforming CBOM, publishes at CCFramework.org. Both are open under CC BY 4.0 and follow this framework's sector taxonomy.

This framework 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). Quantum Academy (QuantumAcademy.com), founded by the author, offers trainings and certifications on the topics this framework covers, for the roles and training levels described in Skills & Team Structure.

The PQC Migration Brief (pqcmigrationbrief.com) carries corrections, standards and regulatory movement between editions, and the current jurisdiction roster is maintained on the Global PQC Migration Clock page on PostQuantum.com; the framework itself remains free and ungated.

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. The Universal Framework applies in full. These constraints sharpen, extend and in places reorder its guidance.

Six constraints set the sector apart, and the structural advantages that offset them close this section.

Unmatched Cryptographic Density

Financial services is the most cryptography-dense sector in the economy. In one internal discovery exercise on a limited set of representative components at a point in time (The Cryptographic Iceberg Inside a Mobile Banking Transaction, Further Reading), a single mobile banking session invoked approximately 320 cryptographic function calls before the user initiated a transaction, and a single mobile banking payment, followed end to end from the device through the bank's API gateway, the card network or interbank messaging, clearing and central bank settlement, touched nine independent parties and upward of 30,000 unique cryptographic functions.

The figures are an illustration of order of magnitude, not an industry benchmark or a representative average. 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. The cryptographic inventory in Phase 1 and the CBOM built in Phase 2 are therefore 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 party has its own upgrade cycle, vendors, certification requirements and risk appetite. Migrating one party's cryptography without coordinating with its counterparties protects the paths that party controls (its own edge, its own issuers and signing services, its side of each link) and leaves every shared path at the level of its least-migrated link. The exposure reduces on the paths covered, and the chain is not protected until the counterparties follow. Vendor and supply chain governance (Phase 7) is therefore a critical-path constraint that must start in Phase 0.

Harvest Now, Decrypt Later as an Active Planning Risk

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. HNDL is treated as an active planning risk on inference from demonstrated capability (means, motive, opportunity, precedent; Universal, Two-Track Migration Model), never on observed harvesting. A passive collector leaves no trace in the victim's network.

Financial traffic meets every ground of that inference. The flows are high-volume, and the data keeps its value for longer than any credible CRQC estimate. The routes cross backbone links and submarine cable stations that actors with interception capability hold. Where an authority's statement is cited, it is quoted at the strength the authority used. A Federal Reserve Board staff working paper (Mascelli, J., and M. Rodden (2025), "Harvest Now Decrypt Later": Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks, Finance and Economics Discussion Series 2025-093, Board of Governors of the Federal Reserve System, https://doi.org/10.17016/FEDS.2025.093) describes HNDL as "a present, active, and in some circumstances unavoidable data privacy risk".

The paper states that the views are the authors' and not those of the Board of Governors, the Federal Reserve Bank of Chicago or the Federal Reserve System, and this extension cites it as staff research on that basis. On that inference, Phase 3 prioritizes external-facing interfaces and data-in-transit protections. The reasoning for why the harvest cannot be detected, written for the funding conversation, is in the July 2026 PostQuantum.com analysis.

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 answers to as many overlapping bodies with direct or emerging PQC expectations. The Universal's Regulatory & Standards Alignment Map defines three deadline archetypes. The sector meets every one of them. A requirement type recurs across schemes and standards: PCI DSS v4.0 Requirement 12.3.3 has required a documented, annually reviewed inventory of cipher suites and protocols of PCI-scoped entities since March 31, 2025.

A sector regime binds through supervision: in the EU, DORA and its ICT risk management standards require a policy on cryptographic controls with provisions for changing cryptographic technology as cryptanalysis develops. Supervisory expectations now come with dates: FINMA Guidance 05/2026 of July 9, 2026 recommends that Swiss institutions draw up a post-quantum roadmap by mid-2027 at the latest. Two further sources apply: the cross-sector anchors the Universal is built against (NIST IR 8547, the EU coordinated roadmap) and the coordination bodies whose publications supervisors read.

The sector-body instruments are listed with their status and enforcement tier in this extension's Regulatory Alignment Map. The jurisdiction roster is in the Universal's Regulatory Timeline Context and, kept current, on the Global PQC Migration Clock page.

Systemic Risk Amplification

A quantum-enabled attack on financial infrastructure is a systemic event. The Hudson Institute's April 2023 analysis (Butler and Herman, "Prosperity at Risk"), as relayed in the Project Leap Phase 2 report, ran a quantum-enabled attack on Fedwire alone through the resulting six-month recession and put the effect at 10 to 17 percent of US real GDP, with $2 to $3.3 trillion in indirect losses measured as GDP at risk. Those are conditional estimates under the study's scenarios, not a forecast, and the Phase 0 business case carries them as such.

The June 2026 edition attributed the figures to the Citi Institute's January 2026 analysis. The attribution is corrected to Butler and Herman. An earlier form of this correction said the six-month-recession framing was added here as well. That was wrong and is withdrawn: the framing is the study's own, stated in its abstract. The cascading-failure exposure changes the Phase 0 business case and justifies investment levels that sectors without it would find hard to defend.

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, and the Universal states the mapping by function (Activity 0.3; GRC Implementation, Decision Rights and the Three Lines). The program is first-line management and delivers: the QRPM, the CISO directing the program, and the business and technology teams that migrate their estates, whatever their titles. The risk function is second line and challenges what the first line delivers: the scoring model and its runs, the gate decisions and the closure decision.

Internal audit is third line and provides independent assurance. The board approves the risk appetite and receives the KPI pack. Financial institutions can place quantum readiness inside a governance model their supervisors already examine, scaffolding most other sectors lack in that form, provided the CISO's function is recorded as first line for this program and the second-line challenge is owned by a function that does not execute the migration.

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

A small number of vendors supply most of the general-purpose and payment HSM estate, and most financial institutions use one or two of them, which simplifies Phase 7 engagement and concentrates the dependency. Whether two institutions' alternatives, or two product lines under two names, run one firmware family is a Cryptographic Concentration Framework question (CCF layer 4, key custody platform), cross-referenced from the Activity 6.2 register and not recomputed in this extension. Product, firmware and certification references are in the front-matter Tool and Vendor References with an as-of date.

Several HSM vendors also supply, directly or through a partner, cryptographic discovery and inventory capability reachable from the HSM management plane. An institution may already hold it under an existing contract without having activated it. Before procuring standalone discovery tooling (Phase 1), check what the current HSM vendor

provides, and grade what it finds with the evidence tiers of Activity 1.2 like any other source.

Regulatory Examination Experience

Financial institutions undergo regular regulatory examinations and are practiced at producing evidence, responding to examiner inquiries, and managing multi-year compliance programs (Basel III/IV, DORA, PCI DSS, SOX, AML/KYC). That experience transfers directly to PQC migration: the evidence the framework requires (CBOM documentation, risk scoring artifacts, pilot reports, maturity assessments) is of the kind regulated financial institutions already produce and retain for examination.

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. Banks run the vendor PQC readiness questionnaire in the Universal Framework inside the existing vendor assessment cycle. No separate process is needed. Few other sectors run vendor governance at this depth; banks already have the infrastructure and the practiced teams, and the framework's questionnaire enters that cycle rather than creating one.

Change Advisory Board Discipline

Banks run formal change advisory boards (CABs) and freeze changes 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 is presented inside the existing strategic planning process. 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. The Framework Adaptations section later in this extension maps each challenge to the phases it changes.

The challenges below run in three groups: the broader financial services issues first (the regulatory environment, trust infrastructure, lending, wealth management, and core, corporate and digital banking); then the payment-infrastructure challenges, summarized here and covered in full in the companion Payments Extension; then the 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. Guidance and requirements come from multiple overlapping sources, which between them set three kinds of deadline (Universal, Deadline Archetypes): plan-by, procure-by and migrate-by. The recurring requirement type is the cryptographic inventory in all but name: PCI DSS v4.0 Requirement 12.3.3 (required after March 31, 2025) obliges PCI-scoped entities to document and annually review the cipher suites and protocols in use.

The EU sector regime is DORA (Regulation (EU) 2022/2554, in application since January 17, 2025) with its ICT risk management standards (Commission Delegated Regulation (EU) 2024/1774), whose Article 6 requires a policy on encryption and cryptographic controls that includes provisions for updating or changing cryptographic technology on the basis of developments in cryptanalysis, and Article 7 the key-management rules beneath it.

Supervisors now publish dates. FINMA Guidance 05/2026 (July 9, 2026), a supervisory communication under existing operational-risk and resilience rules, recommends a post-quantum roadmap by mid-2027 at the latest, a cryptographic inventory, HNDL protection for critical data, the involvement of external service providers and the

transition to crypto-agility. The Universal's anchors apply on top: the EU coordinated roadmap's end-2030 date for high-risk use cases names the financial sector, and NIST IR 8547's 2030 and 2035 dates are the reference most instruments cite.

Readiness indices and sector surveys (this extension's Regulatory Alignment Map; Universal Appendix G) are the newest instrument type: a supervisor that publishes one has stated the scale on which it scores the plan.

No regulator mandates specific PQC algorithms or implementation standards for financial institutions. PCI SSC had published no PQC guidance of its own at the June 2026 edition (re-checked at each release). Several supervisors now publish dates, so the targets are no longer undefined: a plan-by date (a roadmap by mid-2027 in one jurisdiction), migrate-by anchors (end-2030 for high-risk use cases under the EU roadmap; 2030 and 2035 under NIST IR 8547) and, through the readiness indices, a stated scale for the plan.

Phase 0 business cases are therefore built on the deadline archetypes and the enforcement tiers that bind the institution. The algorithm choice is made under this framework's positions (hybrid ML-KEM-768 with X25519 for key establishment; composite or dual signatures for Track B), and compliance officers monitor the sector bodies through the Regulatory Horizon Report (Universal, GRC Implementation). No supervisor has said it will issue an algorithm mandate to wait for.

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 signed artifacts with long verification periods as well as HNDL exposure on encrypted data.

Supervisory instruments acknowledge the forgery risk without measuring it. The sector's readiness indices and surveys stage institutions across awareness, planning, pilots and preparedness, and the guidance that names electronic signatures and non-repudiation as a long-term protection requirement scores the plan on one scale, with no separate

signature dimension. An institution reporting on the supervisor's scale can therefore score well while its Track B exposure is unmeasured.

The two tracks are kept separate in every number. The Trust KPI and the TNFL exposure entries in the KPI supplement report the signature track on its own; the maturity supplement shows a signature indicator at each level; and the Quantum Readiness Assessment maps its Track B findings onto whichever supervisory stage the institution reports. The forgery exposure stays visible in the figures the supervisor sees.

Challenge 3: Core Banking Platform Dependency

Core banking systems are the operational backbone of every bank. The major core banking platforms and the many regional and legacy systems beside them 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. Platform names as the June 2026 edition listed them are in the front-matter Tool and Vendor References with an as-of date.

Banks running multiple core banking platforms across regions or product lines face multiplicative complexity. A global bank running one platform on each of three continents must coordinate a separate PQC migration stream per platform, against a different vendor roadmap for each, with every date graded for firmness (Activity 7.5). Phase 7 vendor governance must identify core banking vendors as Strategic Blocking vendors from the outset.

Executive-level engagement on PQC roadmap commitments should begin during Phase 0. The two agility questions of Activity 7.2 (algorithm change by configuration; verifiers and trust stores updatable in the field) are asked of every core platform before its roadmap dates are discussed. A platform whose algorithms change only with a new release turns every future algorithm change into a vendor release.

Challenge 4: Mortgage and Long-Term Lending Data

A 30-year fixed-rate mortgage originated in 2026 carries several record classes with different clocks: personally identifiable information, property valuations, income documentation and credit assessments. The loan term is one input to their confidentiality horizons and not a substitute for them. The horizon of each class comes from the obligation that binds that class, per Activity 1.1, and the five clocks the Universal separates stay separate here: the continuing confidentiality need, the retention obligation, any legal preservation period, the signing authority's period of authority and the verifier's service life.

Credit assessments and income documentation are bound by data-protection and banking-secrecy duties that can outlast the loan or expire before it ends. A property

valuation stays confidential on a schedule of its own, and a title record is public in some jurisdictions from the day it is filed. Phase 1 therefore records a horizon per record class rather than one date for the file. The retention regime is evidence toward that horizon and does not set it.

Several of these classes will run past 2056 on their own obligations. Encrypted mortgage documents, title records and deed registrations transmitted today are HNDL targets with some of the longest sensitivity windows in any sector. Dimension 1 reads the confidentiality need alone.

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) have 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 Network Exposure

Open Banking regulations (PSD2 in Europe, analogous regimes in the UK, Australia, Brazil, and elsewhere) have created a vast API network 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. The quantum-vulnerable dependencies are TLS key establishment, authentication by certificate, and JWS or certificate signatures on RSA/ECDSA. The quantum vulnerability surface of Open Banking is both wide (thousands of API endpoints across the network) 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 finances 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, carries at most 999 bytes in a variable-length field in the base standard, and scheme and switch implementation specifications narrow the fields further (Field 55, the ICC system-related data, is commonly limited to 255 bytes of EMV data, and the authentication data fields are smaller).

An ML-DSA signature does not fit in any single field. ISO 20022 is more extensible. Even there, BIS Project Leap Phase 2 could not carry a post-quantum signature in the Business Application Header of a T2 message by configuration: the network service providers shipped updated modules, the central banks reconfigured their connectors, and a separate verification component was built because the existing verification software accepts one signature algorithm at that level.

The RSA signature in that header was 256 bytes. The Dilithium signature that replaced it measured 3,293 bytes, a 12.9× increase by this framework's arithmetic (the standardized ML-DSA-65 signature is 3,309 bytes per FIPS 204). The June 2026 edition described that finding as a buffer overrun. It is corrected here to the report's text, as in the Payments Extension. For detailed treatment of message format constraints, HSM certification, and settlement latency, see the companion Payments Extension.

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 tight and set per scheme and per kernel test requirement, which an issuer reads for its own deployment. 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). Of the standardized algorithms, the lattice schemes (ML-KEM, ML-DSA) are the candidates for current card hardware on memory and execution-time grounds (Universal, Appendix A), with SLH-DSA's signatures, from 7,856 bytes upward (FIPS 205), outside the contactless data budget; whether a given chip can run them is measured per product, not assumed. 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 silicon announced for 2026 mass production by the major chip suppliers (Tool and Vendor References) will provide more headroom, but the card and terminal replacement cycle is measured in years. Mastercard's Enhanced Contactless (Ecos) announcement of January 26, 2021 describes quantum-resistant protection for the account information exchanged between the card or wallet and the terminal, delivered by software upgrade with no new hardware or terminals and with the contactless interaction kept under half a second. The announcement names no algorithm (the AES attribution comes from later trade press, not from Mastercard) and says nothing about offline data authentication, so it is read as a transaction-channel measure and not as an answer to the offline-authentication question.

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's HSM requirement for network participants comes from its Customer Security Programme and is checked at that source rather than assumed from the sector: an institution reads the current Customer Security Controls Framework for the version of the standard it names and records that version with the certificate reference in the Activity 6.2 register; PCI compliance requires a separate validation.

Validation is decided per product, per operation and per certificate (Universal, Deployment Environment Classification). Validated software with ML-KEM as an approved service (CMVP certificate #5247, April 2026, at ML-KEM-768 and ML-KEM-1024 only) and validated Level 3 hardware with ML-KEM, ML-DSA, SLH-DSA and LMS inside the approved boundary (CMVP certificate #5497, August 2026) both exist; payment HSMs, which also need a PCI PTS HSM approval, follow one product at a time.

Two qualifications from its Security Policy travel with every citation of #5497: the §2.7 statement printed in the alignment section's validation subsection, and the fact that HSS key generation, signing and verification are vendor-affirmed rather than CAVP-tested. Separately, the module's own firmware-update verification service verifies with ECDSA and with HSS. Each module's certificate is checked for the operation required and recorded in the Activity 6.2 register beside the PCI PTS HSM certificate reference, and a vendor's "PQC support" claim is a non-approved service until the certificate lists the operation. Running PQC operations outside the validated boundary is a documented risk decision under the FIPS-aware class, not a compliance posture for a FIPS-required system.

Payment HSM product lines carry PQC firmware and PCI certification timelines that organizations do not control. The product names as the June 2026 edition listed them are in Tool and Vendor References. Until the module that covers an operation is validated, an institution with a FIPS-required system records the dependency with the vendor's evidence, the interim controls, the exception authority and the next decision date, and the migration of that system waits on the certificate while the program does not.

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 production-grade settlement infrastructure, run in the Eurosystem's T2 test environment. Software-based post-quantum signature verification averaged 209.9 milliseconds compared to 28.1 milliseconds for RSA, a 7.5× slowdown on the one step the experiment timed. The client-side signing cost was not measured because no HSM was used, and the test used pre-standard CRYSTALS-Dilithium category 3 signatures, the NIST Round 3 predecessor of ML-DSA-65.

A 7.5× factor on one verification step, in a system that processes trillions of euros daily, is a capacity planning concern worth taking seriously. It is also a published case study on a pre-standard algorithm and one measured step, not a number to plan against. Whether hardware acceleration narrows the gap on a given payment path is a measurement on that path and its target implementation, not a property of the technology.

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.

In BIS Project Leap Phase 2, every test scenario passed on the signature itself (correctly signed transfers accepted, a transfer signed with the wrong key rejected with the standard error message, participants on different cryptographic libraries interoperating), and settlement did not complete because no certificate for the test key existed in T2's common reference data (T2 succeeded TARGET2 in March 2023). The

report records that outcome as expected and reads it as the system's reliance on centralized certificate data under post-quantum signatures as well.

The June 2026 edition described the missing certificate as a failure. It is corrected here to the report's text, as in the Payments Extension. An algorithm swap alone does not complete the migration. The issuers, the validation software, the trust stores and the reference data the validation reads move together, and a migration that changes the signature without changing the reference data settles nothing, which is what the T2 result demonstrated on the architecture it tested.

Whether that requires parallel certificate hierarchies, or a single hierarchy supporting both algorithms, follows from the compatibility strategy chosen for the deployment rather than from the test.

Swift's public statements, checked September 2026: SwiftNet 8.0 is Swift's upgraded network enabled for post-quantum cryptography, to be released in 2027; Alliance Release 8.0 is a mandatory major release planned to be available at the end of July 2027; Alliance Release 7.9 lays the foundations for release 8.0 and PQC readiness. It will need to be deployed by the majority of the community because there is no upgrade path from release 7.7 to 8.0.

It goes out of support 15 months after release 8.0 ships. The June 2026 edition's "around 2027" and "12 to 18 months" are replaced by those statements. What PQC use release 8.0 will require of participants, and on what date, is not stated publicly. The grade is announced, with that requirement unknown (Payments Extension, SwiftNet 8.0 Migration Planning). 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) authenticates most sessions at session level, over TLS, a VPN or a private circuit, with per-message signature fields used in some deployments rather than in all of them; which of the two a given connection relies on is a Phase 1 finding, not an assumption. The regulatory obligations most often cited here are clock obligations, not signature obligations: MiFID II transaction reporting and SEC Rule 613 CAT require business clocks

synchronized to a stated tolerance and accurate event timestamps on reportable events.

Neither requires a cryptographic signature on a market data feed. A timestamp field in a message and a cryptographic timestamping service that binds a hash to a trusted time are different controls with different failure modes, and a feed that implements the first has not deployed the second. Phase 1 records which of the two each feed actually uses. TNFL exposure is scored against the cryptographic signing and timestamping services the inventory finds in use: trade confirmations, signed feed content where a feed signs, and the session authentication above.

An adversary able to forge those signatures could pass off fabricated confirmations or altered timestamped records, which reaches regulatory reporting and settlement integrity. Clock synchronization is a separate control and is not made quantum-safe by this migration.

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, recording per connection whether authentication is session-level (the transport is the Track A entry) or per-message (a Track B entry). Organizations place the signed flows in Track B of the 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.

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 in Phase 3 risk scoring and engage reinsurance partners on PQC readiness in Phase 7 vendor governance.

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

Post-trade infrastructure depends on authenticated messaging among the trading parties, their custodians, central counterparties (CCPs) for clearing and central

securities depositories (CSDs) for settlement. Securities lending and repo transactions, collateral management, corporate actions processing and settlement confirmation run on a mixture of authenticated transport, application-level message authentication and, on some flows, a cryptographic signature over the instruction itself.

Which of the three a given flow uses is a Phase 1 finding, not a property of the sector. TNFL reaches the asymmetric dependency the finding names, and a flow authenticated only at session level is a Track A entry whose forgery risk attaches to the transport. Where an instruction does carry a signature a relying party validates, 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 regulatory filings electronically 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. These channels do not share one signature architecture, and "digitally signed" collapses four different things: authentication to the submission portal, the transport security carrying the file, a cryptographic signature over the filed object, and a legal signature requirement that a named officer attest to the content.

A channel can require the first, the second and the fourth and carry no cryptographic signature on the object at all. Phase 1 inventories each submission channel separately and records five facts about it: the portal authentication mechanism, the transport security, any document signature and its algorithm, the legal-signature or attestation requirement and who holds it, and the receiving authority's validator. TNFL is then scored against the asymmetric dependency that inventory finds.

Where a filed object carries a signature a receiving authority validates, forgery of that signature would let an adversary file fraudulent data in the institution's name. That is a systemic exposure. Where the channel authenticates a session and attests by officer declaration, the exposure is in the authentication and the transport instead, and migrates on Track A.

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 (the provider's KMS, managed encryption services, cloud-native certificate management). PQC migration requires upgrading the algorithms those services use at the same time. Each major cloud provider's key-management service publishes its own PQC key-type roadmap and validation timeline, and a bank using multiple cloud providers tracks several independent roadmaps for key management alone, each date graded for firmness and each provider asked for both halves of the disclosure (the current negotiated state per service and the dated targets per service; Activity 7.7). Provider names are in Tool and Vendor References.

Cloud-hosted workloads also raise shared-responsibility questions: who is responsible for migrating the storage encryption of 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 in storage. Its HNDL exposure could compromise ongoing investigations if a future quantum adversary decrypts it.

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, to CBDCs (central bank digital currencies), to distributed ledger technology (DLT) for settlement (bank-operated DLT platforms. The European Central Bank's DLT settlement trials), or to 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 surrogate values that have no value to an attacker outside the tokenization system. How the surrogate relates to the original differs by scheme. The three schemes a bank holds are protected by different mechanisms. A vault token is a surrogate whose mapping to the original is held in a store the tokenization system controls.

An encrypted surrogate, typically format-preserving encryption on FF1 or FF3-1 with AES underneath, is a ciphertext and is reversible with the key. A network payment token issued by a card scheme is neither. It is usable for the payment transactions its domain controls permit, and its protection comes from those restrictions, from the transaction cryptogram and from the scheme's enforcement rather than from any inability to reverse it.

None of the three is irreversible in the sense a hash is. The June 2026 edition's "cryptographically irreversible" is corrected here. Symmetric cryptography and the access controls around the vault, the key or the token domain provide the protection, and AES is not vulnerable to Shor's algorithm (Grover's algorithm gives only a quadratic speedup, addressed by AES-256). Tokenized data harvested for future quantum decryption yields token values that are useless without the vault, the key or the ability to transact inside the token's domain.

Those are the components that stay in scope: the token vault, the detokenization APIs, the key-management layer, the domain and cryptogram enforcement the scheme performs on the bank's behalf, the logs, and every system that still processes cleartext. Tokenization is therefore a documented reduction in HNDL-exposed surface and in migration scope, ahead of full PQC migration. It does not remove the key-management layer, the detokenization path or the authentication around them from the 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 tokenization has taken out of the exposed path, which retain cleartext or reversible surrogates, and which of the supporting components (vault, keys, detokenization, authentication) still need the migration. Expanding tokenization scope may be faster and cheaper than waiting for end-to-end PQC for certain data categories.

ALIGNMENT WITH UNIVERSAL FRAMEWORK V3.0

Universal Framework v3.0 (September 2026) is a major version. Readiness against dated obligations is the mandate; crypto-agility is the method. The PQC migration is the first exercise of a standing capability. For financial institutions the version changes the method, the records and the vendor governance, and corrects four published positions.

- **Method.** The charter states both outcomes (Phase 0). The program runs ten workstreams, with Discovery separated from the permanent Cryptographic Record and Crypto-Agility funded from Year 1 (Activity 0.3). Every migration gate and wave exit applies the agility criterion, and a system whose algorithm cannot be changed by configuration and rehearsed with rollback is recorded as migrated with agility debt rather than as migrated (Activities 4.6 and 5.4).

Every wave carries an algorithm-change rehearsal (Activity 5.2). Closure requires a rehearsed second algorithm change per track inside the agility window (the 48-hour assessment plus the organization's change window, ten business days by default) and zero unaccepted agility debt (Migration Verification & Program Closure). Phase 3 produces an agility-debt register.

- **Records and evidence.** Every discovery finding receives an evidence grade E1 to E5; coverage is measured against a denominator enumerated before discovery ran. The accepted-gaps register is signed at gate G1 → G2 (Activity 1.2). The CBOM minimum record is the Universal's own (Activity 2.1), with the Applied Quantum CBOM Profile v1.0-RC or later cited as informative carriage and never required. The Cryptographic Concentration Framework is cross-referenced where the question is how many distinct implementations execute beneath the vendors (Activity 3.1), and no concentration figure is computed in this extension.
- **Vendor governance.** Every roadmap date is graded for firmness (committed, forecast, announced, unknown). The questionnaire opens with the two agility questions and the firmness question; four certificate-authority questions, the non-

standardized-algorithm rule with its one-afternoon test, the provider-roadmap reading rule and the counterparty pattern apply (Activities 7.2, 7.3, 7.5, 7.6 and 7.7). In financial services the same set enters the third-party risk management cycle the institution already runs; supervisory outsourcing guidance now asks for contractual crypto-agility in the same terms (Phase 7 adaptations).

- **Corrections made in the open.** HNDL is stated as inference from demonstrated capability, never as observed harvesting. The June 2026 attribution to the Federal Reserve is corrected to the staff working paper behind it, cited under that paper's own disclaimer. The June 2026 statement that no validated module offered approved PQC was wrong when published (CMVP certificate #5247, April 2026); validation is decided per product, per operation and per certificate (Deployment Environment Classification). The HKMA Quantum Preparedness Index is dated to its first publication, July 27, 2026 (the June 2026 edition dated the February 2026 announcement).

Standards currency runs to September 2026: RFC 9954 and RFC 10024 for hybrid key establishment in TLS; RFC 10042 for hybrid key establishment in SSH; RFC 9964 for ML-DSA in JOSE and COSE, which token signing in Open Banking reads; RFC 9881 and RFC 9882 for ML-DSA certificates and CMS; the Chrome Root Program Policy v1.8 client-authentication separation; and the section 8 conditions of SP 800-208 on the deploy-now signing action.

The subsections below read each element for financial institutions. The last three read elements the June 2026 edition did not cover (the agility criterion and rehearsal; evidence grades and the coverage denominator; vendor dates and questions). The remaining Universal positions (the stored-data strategy decision 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 and the Re-Baseline Protocol in 4.8, the risk-weighted coverage KPI, algorithm sovereignty and standards fragmentation, crisis communications, the skills matrix, and Appendices G, H and I) apply to financial institutions as written, with two notes.

Supervisory record-retention regimes supply the confidentiality-horizon inputs the Activity 5.6 decision requires, so the stored-data strategy is chosen per retention class, not per system. 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's two-track migration model (Phase 5) maps to financial services as follows:

Track A (Confidentiality / Key Exchange): External-facing TLS on the internet banking edge, the mobile APIs and the 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, the trust service provider inquiry in the qualified-signatures subsection below). Both tracks run as parallel workstreams, each with its own milestones, rehearsals (Activity 5.2) and closure proof (Universal, Migration Verification & Program Closure). The Universal's default weights (HNDL 0.35, TNFL 0.25) stand for the sector, ratified by the SteerCo before the first scoring run.

Validation Decided Per Product, Per Operation, Per Certificate

Financial services operates predominantly in FIPS-aware or FIPS-required environments. The obligation is checked at its source, never assumed from the sector:

- A payment HSM's obligation comes from PCI PTS as much as from FIPS 140-3.
- A SWIFT interface's comes from the network's own security requirements.
- A government-facing system's comes from the contract that names validated modules.

The June 2026 edition stated that no FIPS 140-3 validated PQC module existed, with validation expected in mid-2027 at the earliest. That statement was wrong when published. As of September 2026 the CMVP validated-modules list includes post-quantum operations as approved services in software and in hardware, and the two certificates this framework cites are not interchangeable evidence.

Property	Certificate #5247	Certificate #5497
Module	Go Cryptographic Module (versions v1.0.0 and v1.0.1, Geomys LLC)	QASM Cryptographic Module (Crypto4A Technologies, hardware version QASM 1.1, firmware 5.0.1.158)
Type and level	FIPS 140-3 Level 1 software module	FIPS 140-3 Level 3 multi-chip standalone hardware module

Property	Certificate #5247	Certificate #5497
Dates	Validated April 27, 2026; updated July 7, 2026	Initially validated August 19, 2026; updated August 21, 2026; sunset date August 18, 2031
ML-KEM	KeyGen and EncapDecap, which covers encapsulation and decapsulation, at ML-KEM-768 and ML-KEM-1024 only and not at ML-KEM-512	KeyGen and EncapDecap at ML-KEM-512, -768 and -1024
ML-DSA	None. The Go module version that implements ML-DSA is on the Modules in Process list, not on the validated list	KeyGen, SigGen and SigVer at ML-DSA-44, -65 and -87
Other approved algorithms	Not applicable	SLH-DSA across all twelve parameter sets, and LMS

Two qualifications from #5497's Security Policy apply to every citation of it. The first is that §2.7 states that the module does not establish SSPs using an approved KEM, and instead exposes ML-KEM functionality for an external application to use as part of an approved KEM. The second is that HSS key generation, signing and verification are vendor-affirmed, not CAVP-tested.

A sentence asserting that approved post-quantum key establishment exists in a validated module cites one certificate with its qualification (#5247 with its parameter-set limit, #5497 with its §2.7 statement), never both as a single proposition. Every ML-DSA statement in this extension cites #5497 alone. A module that lists PQC only among its non-approved services does not count.

Neither certificate is a payment HSM's. A payment HSM has a PCI PTS HSM approval beside its FIPS certificate, and the payment HSM product lines follow one product at a time (Challenge 10; Payments Extension).

The planning rule is per product. For each FIPS-required deployment, record:

- the governing requirement
- the exact module and version
- the certificate number and status
- the approved services the certificate lists
- the required security level

- the tested operating environment

Confirm that the intended operation is covered (Universal, Deployment Environment Classification). Where no validated product covers a system's operation, record the dependency with the vendor's evidence, the interim controls, the exception authority and the next decision date. It constrains that system and sets no date for the program.

Sequence the rollout in three steps:

1. **Pilots**, in unrestricted environments such as development and staging, now.
2. **FIPS-aware systems**, with documented risk acceptance on CAVP-tested algorithms.
3. **FIPS-required production**, last, per system on the certificate date of the module that covers it, planned, staged and rehearsed in advance.

The certificate date is then only a change window.

On September 21, 2026, the CMVP moved every remaining FIPS 140-2 certificate to the Historical list, the date stated in the maintained prose of NIST's FIPS 140-3 Transition Effort page (its transition-schedule table, stamped 2021, prints September 22, 2026). CMVP states a permission for those modules, not a prohibition: it supports their purchase and use for existing systems and notes that the selection of FIPS 140-3 modules may be limited for several years.

CMVP also recommends that purchasers consider every module on the validated-modules search page regardless of whether it was validated against FIPS 140-2 or FIPS 140-3. The exclusion of a Historical module from procurement for a new system follows from that scoping to existing systems and from supervisory and contractual policy, not from a CMVP prohibition; whether an existing deployment on a Historical certificate may continue is decided under the applicable supervisory or contractual risk policy, and the two questions are assessed separately. Financial institutions plan the FIPS 140-3 and PQC migrations together. The two intersect at the HSM layer, and one refresh should serve both.

Merkle Tree Certificates for Customer-Facing Infrastructure

For public-facing web banking and API infrastructure, Merkle Tree Certificates (MTCs) are the path the major browser and public-CA operators have announced for post-quantum authentication in the public Web PKI (Universal, PKI Architecture Evolution). The Chrome Root Program is implementing a Chrome Quantum-resistant Root Store targeted for Q3 2027 and has stated that it has no immediate plan to add traditional PQC X.509 certificates to the Chrome Root Store.

Let's Encrypt announced on June 3, 2026 that MTCs are its chosen path, with staging environments in late 2026 and production issuance in 2027. The IETF PLANTS working group holds the specification. Checked for this edition: public root CAs have issued no

ML-DSA roots that chain into the major browser and operating-system trust stores. The CA/Browser Forum ballot that would permit ML-DSA in publicly trusted TLS certificates is in draft.

The Universal's PKI fork applies unchanged: public-facing certificates track MTC on the operators' dates; internal banking PKI (interbank mTLS, HSM certificate chains, internal service mesh, the private hierarchy that replaces publicly trusted client certificates under the Chrome Root Program Policy v1.8 separation) proceeds on X.509 with PQC algorithms now. Financial institutions invest in ACME-based certificate automation now, both to prepare for MTCs and to keep pace with the CA/Browser Forum Ballot SC-081v3 lifetimes for publicly trusted TLS certificates: 200 days from March 15, 2026, 100 days from March 15, 2027 and 47 days from March 15, 2029. Every public CA and every scheme or trust-framework CA the institution depends on is asked the four certificate-authority questions of Activity 7.2, its MTC roadmap among them.

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.

CNSA 2.0 excludes SLH-DSA, which means financial institutions adopting this standard are committing to lattice-based algorithms for general-purpose digital signatures (CNSA 2.0 allows the stateful hash-based signatures LMS and XMSS for software and firmware signing and recommends beginning that transition with them, and approves ML-DSA-87 for all signature use cases, including software and firmware signing; NSA CNSA 2.0 FAQ, Version 2.1, December 2024).

This is a defensible choice for institutions that prioritize interoperability with government clients, but it forecloses the SLH-DSA conservative fallback. An institution that adopts CNSA 2.0 voluntarily inherits its schedule as a design target, not as an obligation. The CNSSP 15 milestones (new NSS acquisitions from January 1, 2027; phase-out by December 31, 2030; mandated use by December 31, 2031) bind National Security Systems. A financial institution's binding dates are its own supervisors' and contracts'.

Hybrid and Composite Signatures as the Track B Default

The Universal takes the position (Activity 5.2) 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 on the artifacts with the longest verification periods. Regulatory filings, trade confirmations, e-signed legal documents, and audit trails must remain verifiable for years or decades. A composite signature keeps them so even if one component algorithm is later broken or an implementation flaw surfaces in first-generation PQC deployments.

The hedge exists only where the verifier enforces it: a dual-signed filing is hedged only when the receiving authority or counterparty accepts it solely if both signatures validate. The verifier acceptance policy is recorded with the format. 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 document it as a risk decision per the Universal position.

Algorithm Weighting Across ECC and RSA Estates

The Universal's algorithm-specific vulnerability weighting (Activity 3.1) applies 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. The 2026 resource estimates for 256-bit curves moved down while the RSA figures did not. This reverses 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.

The vulnerability weighting does not assign a tier. The tier comes from the ordered test of Activity 3.2, which reads dimension scores and factor values from the record, and neither the algorithm nor the key size is among them. The attack-cost evidence orders entries that tie on the composite score inside a tier, with the larger classical key sequenced later where nothing else separates them. Institutions should not let "modern crypto" stand in for "quantum-safe" in Phase 3 scoring, and should record algorithm family and key size for every CBOM entry.

Ordering then reads one recorded value rather than a judgment re-debated per system. 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

The Universal 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; OAuth/OIDC/FAPI token signing with ES256 or PS256 JWS underpins Open Banking; 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-validity signing keys and enrolled credentials, not ephemeral session material. Two actions follow. Carve an identity slice in the Phase 1 inventory and carry it into the Phase 2 CBOM (identity providers, token signing keys, federation trust chains, authenticator policies). 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-duration access tokens are low priority. The signing keys and root-of-trust credentials behind them are standard Track B targets. One dated dependency reaches this slice from the public Web PKI: under the Chrome Root Program Policy v1.8, publicly trusted TLS subscriber certificates issued from March 15, 2027 assert serverAuth only, so partner APIs, Open Banking mutual TLS and host-to-host links that authenticate clients with publicly trusted certificates need a private hierarchy inside the program's Year 1 to 2, built agile from the first ceremony (Universal, Activity 6.1).

Qualified Signatures and Seals in Onboarding, Lending and Custody Documentation

Qualified electronic signatures and qualified electronic seals are different instruments with different subjects under eIDAS. A signature is a natural person's: the customer, the guarantor, the authorized officer signing in person. A seal is a legal person's: the institution or the custodian, sealing what it issues. A document class may use both.

Together they anchor three document classes a bank cannot re-execute at will:

- **Onboarding.** Account-opening contracts, mandates, KYC declarations.
- **Lending.** Loan agreements, mortgage deeds and assignments, guarantees.
- **Custody.** Agreements with the custodian, instruction mandates, corporate-action elections.

Their legal effect lasts as long as the document is relied on, which for a mortgage deed or a trust instrument is decades. The qualified status of either depends on a qualified certificate issued by an accredited trust service provider, and on a qualified creation device. The institution can replace neither with its own PKI.

The Universal's Qualified Trust Services and Electronic Signature Law subsection (GRC Implementation) sets the treatment, and this extension applies it to the three classes. The regimes differ. The EU's eIDAS and Switzerland's ZertES define certificate-based classes. The US ESIGN Act and UETA are technology-neutral and attach effect to intent and attribution. Each jurisdiction and service type is assessed separately.

At this edition no accredited provider has been found offering qualified services on post-quantum algorithms, and no conformity-assessment criteria for them have been published. The trust service provider is therefore a Phase 7 vendor-dependency class in its own right. Ask every provider the four certificate-authority questions of Activity 7.2, plus the question of when its qualified status will extend to post-quantum algorithms, and grade the answer for firmness. The institution's migration date for statutory signatures is the provider's date.

Phase 1 inventories the e-signature platforms, the signing services and the signed archives by document class. It records the retention obligation and, separately, the period over which a relying party will still verify the signature.

Phase 3 scores each on Dimension 2 from that verification period. The verification period is the verifier's service life, or the signing authority's period of authority where every relying party can be updated when it ends, whichever is longer for the anchor.

Retention is evidence toward that period, and is frequently longer than it. A sealed archive kept for twenty years, whose seal nobody validates after the seventh, is a seven-year verification exposure and a twenty-year retention obligation. Where the document is relied on for as long as it is held, as a mortgage deed or a trust instrument is, the two periods coincide, and the record says so rather than assuming it.

Long-validity signed archives are re-anchored under a post-quantum signature or qualified timestamp before the classical algorithm is deprecated, on a schedule recorded per archive in the CBOM. eIDAS Article 34 qualified preservation is the instrument the re-anchoring strategy maps to.

A statutory presumption of validity meets a forgeable algorithm. That is the keyholder-liability question. EIDAS gives a qualified electronic signature the legal effect of a handwritten signature (Article 25) and a qualified electronic seal a presumption of the integrity and origin of the data it seals (Article 35). The legal effect attaches to the qualified certificate and the qualified creation device, not to the mathematics alone: a signature or seal computed with a future CRQC from a recovered private key is not thereby a qualified signature or seal.

Whether a relying party's validation would nonetheless have accepted it as one, and what presumption then applies until the keyholder rebuts it, are questions of the applicable law and the validation practice at the time. Where the loss falls (on the institution as keyholder or seal creator, the trust service provider or the relying counterparty) is litigated on what each party knew and did at the time, under the applicable law and the facts.

Legal and compliance own the position, which is left open here, and review it annually with counsel. The evidence dossier records when the exposure was identified, which provider dates set the migration date, and which compensating measures (dual-signing where the verifier enforces both signatures, qualified timestamps applied now under a

classical algorithm as a bridge, the re-anchoring schedule) were applied meanwhile (Universal, GRC Implementation).

SP 800-208 for Application Release and Firmware Signing

The Universal makes stateful hash-based signatures (LMS and XMSS, NIST SP 800-208) the component of Track B that deploys now (Two-Track Migration Model). They are standardized and conservative. As the CNSA 2.0 subsection above notes, CNSA 2.0 recommends them for software and firmware signing, and NSA prefers to begin the transition with them, because validated implementations of those schemes are commercially available. ML-DSA-87 is approved under CNSA 2.0 for all signature use cases, including software and firmware signing.

An institution that adopts CNSA 2.0 voluntarily therefore chooses between the two for that use, rather than inheriting a commitment (NSA CNSA 2.0 FAQ, Version 2.1, December 2024).

"Deploy now" comes with SP 800-208's own conditions, in section 8 of that publication:

- Key generation and signature generation happen inside a hardware module with at least Level 3 physical security.
- The private key is never exported, in any form.
- Signing state is managed inside the module, in a way that backup, replication and failover designs cannot reuse.

A signing service that does not meet section 8 is not a conforming deployment, and the verifiers must accept the parameter set chosen.

State safety is an acceptance item evidenced inside the conforming implementation, not an inference from "HSM-backed" or "controlled ceremony":

- the supported parameter sets
- exhaustion monitoring
- atomic state handling
- tested backup, replication, crash-recovery and concurrent-signing behavior The validated LMS implementation this framework can evidence is CMVP certificate #5497, whose CAVP entry covers one parameter set, LMS_SHA256_M24_H5 with LMOTS_SHA256_N24_W2, while the module's own security-function table lists more. XMSS support is materially rarer than LMS, and the CMVP search form offers no filter for either scheme, so the validated population cannot be enumerated and no broader claim is made in either direction.

The deploying institution verifies parameter-set coverage on the specific certificate rather than inferring it from the algorithm's presence. The deploy-now action for financial services is to move the release-signing pipelines for applications and firmware to SP 800-208 signatures, dual-signed with classical during transition and operated

from signing infrastructure. The Phase 6 register records that infrastructure's module certificate, the parameter sets the certificate covers and its entropy validation.

The state-management constraint that keeps these schemes out of general-purpose signing is met only where that evidence exists. The controlled, ceremonial signing environments banks already operate are where the evidence is gathered, not a substitute for it. 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 Against Examination and Due-Diligence Requests

The Universal's Activity 2.5 treats the CBOM and the migration program artifacts as 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, insurers and counterparty due diligence teams all generate standing requests for exactly this material.

The default answer to each of them is the Universal's rule: attest, do not send. The examiner, the QSA or the counterparty receives a signed commitment to the snapshot (a hash and its signing record), a coverage statement that gives its denominator and discovery method (Activity 1.2), and the predicate the requester needs ("no internet-facing Tier-1 endpoint negotiated classical-only key establishment during the observation window"; "every PCI-scoped cipher suite and protocol is inventoried and was reviewed within twelve months"), in place of the document.

Where a supervisor's examination powers require the record itself, it is a point-in-time extract scoped to the inquiry, delivered through a controlled channel, never standing access to the queryable inventory. Apply the remaining provisions of Activity 2.5 through the three lines. The second line owns the access policy and the third line audits adherence to it. The CBOM is marked AMBER or RED at generation and never left at the default; and the CBOM repository joins the SOC's high-sensitivity exfiltration watch list. The Cryptographic Concentration Framework's Discovery Coverage Attestation is the family's published predicate of this kind and is cross-referenced, not reproduced.

Verification, Decommissioning, and Program Closure

The Universal's Migration Verification & Program Closure section defines what "done" means. It asks for four things:

- Observed cryptographic negotiation on the wire, rather than configuration-file assertions.

- Negative testing, showing that classical-only connections are refused once policy requires it.
- A rehearsal record showing the algorithm was changed by configuration and rolled back.
- An evidence standard for retiring systems and keys. For financial services this is examination material. Verification records (observed handshakes, negative test results, rehearsal timings, decommissioning logs with key destruction certificates) are the artifacts supervisory examinations and DORA ICT risk documentation ask for, and they are far stronger evidence than attestations. Decommissioning includes trust-store cleanup across branch, ATM, and client-side estates. A key is retired only when nothing trusts it.

It also covers the qualified-signature archives above, where the classical material is preserved as verification evidence. Closure reads three things:

1. **A verification disposition for every Tier-1 and Tier-2 service**, in one of the Universal's four states: migrated with no agility debt left outstanding; migrated with agility debt and a funded closure date; enclosed or compensated under an accepted exception; or retired.
2. **The closure proof.** A rehearsed second algorithm change on at least one Tier-1 system per track, inside the agility window, minuted, with the segment timings in the evidence dossier.
3. **The agility-debt register at zero unaccepted debt.** Every remaining entry has a funded treatment with a date, or a SteerCo-signed exception.

In a bank the expected debt entries are the vendor-locked core platform, the shared interbank and scheme interfaces whose algorithm the network sets, and the HSM firmware family with no configuration-driven algorithm selection. Each closes as migrated with agility debt against a dated vendor or network release with a firmness grade, or as an exception the SteerCo signs and the second line challenges. Closure means handover into business as usual through the three lines: the Cryptographic Record owner keeps the CBOM. The Crypto-Agility workstream transfers with its owner, budget and standing rehearsal cadence; second-line ownership of cryptographic risk reporting stands; and algorithm transitions become routine change management.

The Agility Criterion and Rehearsal in Financial Services

The Universal's agility criterion (Activity 4.6) asks four things of a migrated system: the negotiated outcome observed; classical-only refused and tested where policy requires it; the algorithm changeable by configuration; and a rehearsal in staging with the rollback exercised. In financial services the first two conditions are met on the customer-facing edge, the API gateway and the corporate host-to-host links the institution controls. The third and fourth are met on those same layers and on the internal PKI and code-signing pipelines, and they fail on the vendor-locked core

platform, on shared interbank and scheme interfaces where the network sets the algorithm, and on HSM firmware that changes algorithms only with a release.

This extension states the sector's agility objective in those terms: a bank is crypto-agile when it can change the algorithm on its own edge, its own issuers and its own signing services on a planned date, and can name the date on which each shared interface will follow its network. Every wave includes an algorithm-change rehearsal on at least one system in the wave, chosen from the layer the institution controls: a parameter-set change (ML-KEM-768 to ML-KEM-1024) on the API gateway or the internet banking edge; a hybrid-to-composite switch on the code-signing pipeline; a certificate-signature-algorithm change on the internal issuer; for custody and HSM-backed signing, one of those three, or a key ceremony that generates a PQC-authorized signing key and retires it.

Each rehearsal is timed across assessment, decision, change and verification, with the rollback exercised in a staging replica. It is scheduled outside the quarter-end, year-end and regulatory-reporting freezes the change advisory board already enforces. Its timings feed the rehearsed time-to-change KPI (KPI supplement). A quarterly failover to the backup HSM partition exercises state management, failover and the SP 800-208 state design, and changes no algorithm.

It is recorded and reported as a failover exercise whose timings do not feed that KPI. A rehearsal that cannot be scheduled because the change requires a vendor release or a network cutover has found agility debt before production did. The entry goes to the Phase 3 register with its treatment.

Evidence Grades and the Coverage Denominator in Financial Services

Every discovery finding is graded in the Universal's five tiers (Activity 1.2): E1, runtime observed; E2, binary confirmed; E3, inventory declared; E4, vendor attested; E5, inferred. In a bank the distribution is split by ring:

- **The internet edge, the API gateway and the interbank links.** Passive monitoring produces E1 for the traffic it sees.
- **Mainframe and mid-range core platforms, mortgage servicing and vendor appliances.** E2 for the minority of binaries that can be analyzed, and E4 or E5 for the remainder.
- **The identity stack and the certificate estate.** Largely E3, from the identity provider, certificate manager and HSM exports.
- **Counterparty cryptography** (SWIFT, schemes, correspondents, market infrastructures). E4 at best, from the counterparty's own statements, until observed negotiation on the shared connection upgrades it to E1. The grade attaches to a claim, not to the row. It stays with the finding when the finding is recorded in the

CBOM and when it is scored in Phase 3. There an E5 entry scored Critical is a finding to verify before it is a finding to fund.

Coverage is measured against a denominator enumerated before discovery runs, built from the CMDB, the application portfolio, the certificate inventory, the HSM register and the PCI DSS 12.3.3 documentation the institution already maintains, never from what the tools found. A coverage figure states its denominator ("92 percent of the 3,400 TLS endpoints enumerated from the load-balancer and API-gateway registries"). The accepted-gaps register, signed at gate G1 → G2 by the Discovery lead, the CISO and the SteerCo, records the scope the denominator contains and discovery did not reach.

The counterparty ring is on it by design, with the reason and the readiness-inquiry date. Asset classes the method cannot observe (the mainframe internals, the terminal fleet) are named as unobserved, with coverage recorded as unknown. The same denominator is the one the PCI 12.3.3 evidence, the supervisor's readiness survey and the Inventory Completeness KRI (Universal, GRC Implementation) all read.

Vendor Dates and Questions in Financial Services

Every vendor and counterparty date in this extension's tables and in the vendor scorecard is graded with one of the Universal's four firmness grades (Activity 7.5): committed (contractual, with remedies), forecast (a planning date stated in writing), announced (a public roadmap statement) or unknown. Phase 3 Dimension 3 scores the grade, not the calendar date. The questionnaire opens with the two agility questions and the firmness question (Activity 7.2).

In a bank the answer to the first agility question sets the migration path for the core platform and the HSM estate. The answer to the second sets it for the customer-side verifiers (banking apps with certificate pinning, corporate host-to-host clients, the terminal fleet treated in the Payments Extension). The four certificate-authority questions go to every issuer the institution depends on: its public CAs, the scheme and network CAs, the SWIFT PKI, the Open Banking trust-framework CAs and the qualified trust service providers. The last also receive the qualified-status question.

The non-standardized-algorithm rule and its one-afternoon test (Activity 7.3) apply to every product sold to the sector as "quantum-safe" on a proprietary or pre-standard algorithm. The provider-roadmap reading rule (Activity 7.7) applies to every cloud and SaaS vendor. The Phase 7 adaptations place the whole set inside the third-party risk management cycle the institution already runs.

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 implement these alongside (not instead of) the Universal Framework's phase guidance. Where the Universal changed a gate, a record, a KPI or a procurement clause at v3.0, the change is mirrored here only where this extension already adapts the element; everything else applies as the Universal states it.

Phase 0 – Executive Mandate & Business Case

Additional Business Case Arguments

- **Systemic risk framing:** The business case should quantify potential systemic impact, referencing the $2 to $3.3 trillion GDP-at-risk scenario in the Hudson Institute's April 2023 "Prosperity at Risk" analysis, as relayed in the BIS Project Leap Phase 2 report (Systemic Risk Amplification, above). This moves quantum risk from an IT security issue to a financial stability concern, a category boards and regulators already govern.
- **Regulatory trajectory:** Map the convergence of the requirement types that bind the institution: the inventory requirement PCI-scoped entities already meet (12.3.3), the EU sector regime and its crypto-agility provision (DORA), the dated supervisory expectations (a roadmap by mid-2027 in one jurisdiction; the readiness indices), and the cross-sector anchors (end-2030 for high-risk use cases under the EU roadmap; 2030 and 2035 under NIST IR 8547).

The business case claims three things: the institution's binding dates are set; the supervisor has stated the scale it scores on; and early movers face lower costs and less disruption. It does not claim that regulators require PQC today. The sector bodies and their status are in this extension's Regulatory Alignment Map.

- **HNDL as quantifiable exposure:** For institutions handling wealth management, cross-border payments, sovereign wealth data or trade finance, 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.

Shared Machinery with the AI-Security Mandate in Banking

Supervisors have begun pairing AI-security and quantum-readiness expectations, in the same blueprints, surveys and guidance and on the same examination cycles, and the two obligations share their expensive components. The first shared component is the asset and dependency inventory. Every model endpoint, training-data store, feature pipeline and inference service a bank runs is reached over TLS, authenticates with keys and certificates, signs or verifies artifacts and stores data under keys the KMS holds.

The AI-risk action plan is therefore built with cryptographic assets in its scope. Each AI asset receives a CBOM entry in place of a parallel register. The second is the vendor register: the model vendors, cloud providers and core-banking vendors the AI plan must assess are the Phase 7 vendors. The questionnaire that asks for a model card and a data-provenance statement asks in the same round for the PQC feature matrix, the two agility questions and a graded roadmap date.

The third is legacy remediation: the mainframe and mid-range systems that cannot be patched for either obligation are compensated once, with the gateway or enclosure pattern recorded for both. The shared work is funded once, under the readiness heading. The AI-risk plan and the quantum-readiness roadmap cite the same inventory, the same vendor register and the same remediation entries. This subsection is the banking version of the Universal's argument (Activity 0.2b).

The dual outcome in the supervisor's terms. The charter states both outcomes (Universal, Phase 0), and in a bank each maps onto something the supervisor already measures. Readiness is what the supervisor scores. The readiness indices and sector surveys stage the institution across awareness, planning, pilots and preparedness; the plan-by dates ask for a roadmap; and the funding request, the examination responses and the insurer questionnaire are framed as readiness against those instruments.

Crypto-agility is what supervisory outsourcing guidance now asks contracts to contain, and it is what the program executes through. The procurement clause and its acceptance test (Activity 7.3), the rehearsal per wave and the closure proof are the evidence that the institution can change its cryptography on a planned date, which is the capability the supervisor's next algorithm question will test. A charter that states both outcomes settles on day one whether the program is a PQC project or an agility

program; in this sector it also settles which of the supervisor's questions each artifact answers.

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 channels (cards, corporate banking, wealth management, digital assets). A dedicated "Quantum Readiness Working Group" under the existing Technology Risk Committee, with a direct reporting line to the board risk committee, is the recommended structure.

Two owners are named in Phase 0 and never merged: the Crypto-Agility workstream owner, with a budget line from Year 1 and the agility-debt register, the mechanisms catalogue and the rehearsal program as scope, placed in the function that controls the customer-facing edge, the internal PKI and the signing services; and the Cryptographic Record owner, who keeps the CBOM after the Discovery workstream ends (Universal, Activity 0.3).

The charter (Activity 0.4) states readiness against the institution's dated obligations as the purpose and crypto-agility as the method, with the success criterion that an algorithm change has been rehearsed on Tier-1 systems inside the agility window, and it pre-authorizes discovery access (passive taps at the internet edge and the interbank links, configuration exports across business units, credentialed scans) with a sponsor-level escalation path for refusals. The SteerCo ratifies the Phase 3 scoring model, its weights and the appeals rule before the first scoring run.

Three Lines of Defense Integration

The Universal states the three lines by function (Activity 0.3; GRC Implementation), and the mapping into the three lines of defense structure most regulated financial institutions already operate is direct. The first line is the program and the estate owners: the QRPM, the CISO where the CISO directs the program, and the business and technology teams that migrate their domains. It plans, executes, measures its own progress and proposes risk acceptances.

The second line is the risk function that does not deliver the migration: it validates the scoring model and its runs under the model-risk treatment in Phase 3, challenges the gate decisions and the closure decision, drafts the risk appetite statement for the board, monitors the KRIs and runs the regulatory intelligence and third-party assessment functions. The third line is internal audit, providing independent assurance that the program is governed as chartered, the inventory is accurate and the KPIs are measured honestly.

Titles do not move a function between lines. A CISO who directs the program is first line for it, and the record shows which role a person acted in for each decision where one person holds two roles in sequence. Financial institutions do not need to create parallel governance structures for PQC migration. They integrate quantum readiness into the existing risk governance architecture, which is faster and more sustainable.

The board approves the risk appetite and receives the KPI pack. The board risk committee receives quarterly PQC migration reporting as a standing agenda item, using the same risk appetite and tolerance framework applied to other technology risks, with the five board KPIs of the Universal (Coverage, Trust, Inventory, Vendors, Agility) and the sector supplement carried in the enterprise risk dashboard.

Phase 1 – Discovery & Inventory

Financial Services Inventory Tracks

In addition to the Universal Framework's three parallel inventory tracks (Activity 1.1: the Cryptographic Inventory; the Sensitive Data Inventory, discovery and classification; the Systems and Assets Inventory), financial institutions add the sector-specific tracks below. The first seven apply across the financial services sub-sectors. The last three are payments-specific and are grouped at the end, with the Payments Extension covering their detail. Every finding on every track has an evidence grade E1 to E5 (Activity 1.2), and each track states, before it runs, the denominator it will be measured against (the alignment section's evidence-grades subsection).

- **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, which is the first agility question asked of the estate rather than the vendor. Expected grades: E3 from configuration and vendor documentation, E4 from the vendor questionnaire, E2 where binaries can be analyzed.
- **Customer-facing digital channel cryptography:** Inventory TLS configurations, certificate pinning and authentication cryptography across internet and mobile banking, wealth management portals and corporate banking platforms. These are the primary Track A (key exchange) targets; passive monitoring at the edge grades them E1.
- **Identity and authentication stack:** Inventory the identity providers, token signing keys (OAuth, OIDC, FAPI), federation trust chains, authenticator and passkey policies, smart card logon PKI and e-signature platforms. These are Track B targets, mostly graded E3 from the identity provider and certificate manager exports (the alignment section's identity-stack subsection).
- **Regulatory submission and document signing infrastructure:** Inventory all systems producing digitally signed regulatory filings, trade confirmations, audit reports,

mortgage instruments, and legal contracts, with the signed archives by document class and retention period. Include e-signature platforms and the trust service providers behind qualified signatures and seals. These are Track B (signature) targets.

- **Long-retention data stores:** Identify every encrypted store with a retention period exceeding 10 years: mortgage records, insurance policy records, trust and estate files, M&A archives, compliance records, and KYC/AML data. A long retention period is the flag that sends a store to this list, not the horizon itself. Record the continuing confidentiality obligation on each store and read HNDL priority from that (Activity 1.1); the retention regime, any legal preservation period and the supervisory record-keeping rule are evidence toward the obligation and do not lengthen it on their own. M&A archives are the clear case: the retention rule outlives the confidentiality value of the material by years.
- **Third-party cryptographic interfaces:** Map every one of them: SWIFT connections, Open Banking APIs, card network links, clearing house integrations, correspondent banking channels, digital asset custody interfaces. For each, record the protocol and algorithm in use and the counterparty's PQC posture from observed negotiation on the shared connection (E1) or, failing that, from a readiness inquiry (E4). This ring is on the accepted-gaps register by design.
- **Certificate authority hierarchy:** Map all CA hierarchies in which the institution participates: internal enterprise PKI, qualified trust service providers, card network CAs, SWIFT PKI, domestic payment scheme CAs, Open Banking trust frameworks. These are PQC migration units that require coordinated root key rotation, and each issuer receives the four certificate-authority questions of Activity 7.2.
- **Payment-infrastructure tracks (Payments Extension):** Three tracks, with the method for each in the Payments Extension.
  - **The payment message formats.** Every format in use, field-level cryptographic dependencies, and fixed-size fields that cannot carry PQC payloads.
  - **The payment HSM estate.** Model, firmware family, FIPS and PCI PTS certificate references, and the vendor-published roadmap with a firmness grade. Classify each as PQC-ready, PQC-upgradeable or PQC-blocked.
  - **The card and terminal estate.** Platform generations, firmware and EMV kernel versions per terminal model, and offline versus online authentication reliance by card program.

Risk-Driven Scoping for Financial Services

The Universal Framework recommends risk-driven scoping to avoid the "boil the ocean" trap (Activity 1.0). For financial services, the recommended initial scoping should prioritize: (1) customer-facing digital channels (internet and 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 storage encryption are lower priority: the institution controls them directly and they are less exposed to HNDL collection. Priority A discovery reports coverage against the enumerated denominator for each of the five scopes, and the SteerCo signs the accepted-gaps register at gate G1 → G2 knowing which of them discovery did not reach.

Discovery Tooling Reachable Through the Existing HSM Vendor

Financial institutions should assess whether their current HSM vendor offers integrated cryptographic discovery capability, directly or through a partner, before procuring separate discovery tools. Discovery reachable from the HSM management plane, together with the storage-encryption inventory the vendor's key-management platform exposes, may cover a significant portion of the Phase 1 discovery scope at lower cost and faster deployment than standalone discovery tools.

The HSM vendor already integrates with the institution's cryptographic infrastructure. The capability is evaluated against the Universal's discovery categories (Activity 1.2) and its findings are graded like any other source (E3 for what a management plane declares; E1 only for observed negotiation). The vendor and product names are in Tool and Vendor References with an as-of date.

This does not eliminate the need for discovery at the network and code levels (the Universal Framework's discovery Layers 1 to 3). It may, though, provide a faster start on discovery Layer 4 (embedded and third-party) and on the CBOM Layer 2 platform cryptography (the HSM and KMS estate) that a bank's CBOM must cover first.

Phase 2 – CBOM & Documentation

Financial Services CBOM Complexity

The Minimum Viable CBOM model from the Universal Framework applies. The record for each entry is the Universal's own minimum record (Activity 2.1): identifier, algorithm OID, key size, protocol context, implementation and version, certificate reference, cryptographic function, confidentiality horizon, regulatory deadline with its source instrument, data classification and quantum vulnerability status. Each entry also records migration status, owner and vendor-dependency flag.

Institutions that carry the record in the Applied Quantum CBOM Profile (v1.0-RC or later) record the same fields as Profile properties and add its financial-services context fields where they apply (Phase 3 below). Carriage in the Profile is informative and never required. An institution that does not open it executes every phase. Financial services

institutions should expect their CBOMs to be substantially larger and more complex than in other sectors.

The order of magnitude the discovery exercise in the sector characteristics illustrates (tens of thousands of unique cryptographic functions across one payment's nine-party chain) means the CBOM must span organizational boundaries, something the standard CBOM model does not address. CBOM Layers 1 and 2 (infrastructure and platform cryptography, including the HSM and KMS estate) are the coverage target before CBOM Layer 3 application cryptography is attempted for the core platforms.

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 the institution can document but not directly modify).

The third ring is inherently incomplete. That is acceptable. The goal is to make dependencies visible, not to document counterparty internals exhaustively. The third ring is where the evidence grades are used most: an entry graded E4 from a counterparty's statement is recorded as E4, and the accepted-gaps register names what the ring does not reach.

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. Requirement 12.3.3 asks for three things: an up-to-date inventory of the cipher suites and protocols in use, with purpose and where used; active monitoring of industry trends regarding their continued viability; and a documented strategy to respond to anticipated changes in cryptographic vulnerabilities, the whole reviewed at least once every 12 months.

A well-structured CBOM supplies the first and is the largest input to the other two. The review cadence, the monitoring and the documented response strategy are evidenced separately, and the Phase 3 scoring runs and the Phase 4 roadmap are the natural evidence for them. Financial institutions should ensure their CBOM structure and metadata fields are sufficient to produce the 12.3.3 inventory evidence as a standard output.

Phase 3 – Risk Scoring & Prioritization

Adapted Risk Scoring Model

The Universal's four dimensions (Activity 3.1) stand: Dimension 1, data sensitivity and exposure (HNDL); Dimension 2, trust infrastructure criticality (TNFL); Dimension 3, migration feasibility, including interoperability constraints; Dimension 4, regulatory and compliance pressure. The June 2026 edition added two dimensions for the sector. This edition adds no dimension: the two are restated as factors inside the Universal's dimensions, scored with the Universal's arithmetic (Activity 3.2): Low = 1, Medium = 2, High = 3, Critical = 4; a dimension scores the highest of its factors; a dimension that does not apply to an entry is excluded with the weights renormalized; and an unknown value is left unscored, listed and resolved before the entry is tiered.

- **Systemic criticality (a factor inside Dimension 2):** Does a forged instruction or a compromised trust anchor on this element cascade to other institutions or market infrastructure? Links to RTGS systems, CCPs, CSDs and scheme settlement = Critical; correspondent and interbank messaging = High; internal services whose compromise stays inside the institution = Medium; none = Low.
- **Multi-party dependency (a factor inside Dimension 3, the Universal's interoperability-constraints factor read for the sector):** Can the migration complete unilaterally? Change requires the network or the scheme to move (SWIFT interfaces, card network connections, RTGS access, Open Banking trust frameworks) = Hard; change requires a bilateral counterparty to move (correspondents, custodians, host-to-host clients) = Medium; internal only = Easy.
- **Verifier updatability (the Universal's Dimension 2 factor, read for the sector):** The factor scores the implementation that performs the verification, and nothing else. Verifiers that cannot be updated (terminal fleets, customer devices holding pinned certificates that no campaign reaches) = Critical; updatable by campaign (an app-store release, a scheduled client release) = Medium; centrally managed trust stores = Low. A counterparty's or a receiving authority's validation software is updatable and scores Medium or Low on that basis. That it updates on the counterparty's timetable is recorded in the delivery state (dependent), never in the factor.

Enrolled customer credentials are read the other way round. For a WebAuthn assertion the relying party is the verifier. Its verification implementation is server-side and updatable, so enrolled passkeys score Medium or Low on this factor. The customer's authenticator holds the private key and signs. What is hard is the signer side: re-enrolling every customer's authenticator on a new algorithm. Record signer-side migration difficulty and credential re-enrollment as a separate constraint against the entry, recorded in its delivery state, and score this factor on the verification implementation. Verifier updatability is the strongest single indicator of agility debt in the estate.

- **Weighting:** The Universal's default weights (HNDL 0.35, TNFL 0.25, regulatory 0.25, feasibility 0.15) stand for financial services. HNDL on external interfaces is the most immediately exploitable threat in this sector. The SteerCo ratifies the dimensions, the weights and the appeals rule before the first scoring run (Activity 0.3).

Model-risk treatment. The scoring model is a model, and is treated as one under the institution's existing model risk management function, on whichever supervisory model-risk guidance binds it. Four disciplines apply (Universal, GRC Implementation, Model Risk in the Phase 3 Scoring Model):

- It is versioned.
- It is documented with its dimensions, its weights, its data sources (the inputs map in Activity 3.1) and its known limitations.
- After each re-scoring run, someone other than the person who ran it validates a sample of entries, with the second line owning the validation.
- It changes only by a minuted SteerCo decision that records the weight change and its rationale. A business owner who contests a tier appeals under the pre-approved rule. The model is not relitigated per system.

Delivery state and the agility-debt register. Every scored entry carries a delivery state (available, dependent, blocked, unknown; Activity 3.2). A blocked entry keeps the tier the ordered test gives it and is never demoted for the block. It is shown as blocked, with the dependency that unblocks it and that dependency's firmness grade. It appears on the roadmap against its unblocking date. In a bank the blocked Tier-1 entries are the shared interbank and scheme interfaces waiting on a network release and the FIPS-required systems waiting on a module certificate.

The agility-debt register lists every Tier-1 and Tier-2 entry scored Hard on control posture, system age or multi-party dependency, or Critical on verifier updatability, with the reason: the mainframe-embedded cryptographic routines in core banking and mortgage servicing (hardcoded algorithm), the vendor-locked core platform (configuration controlled by the vendor), the shared interface whose algorithm the network sets, and the HSM firmware family with no configuration-driven algorithm selection.

The register is derived from the scores already recorded, adds no dimension, feeds the Crypto-Agility workstream and the Phase 4 roadmap, and reaches zero unaccepted debt before closure.

Multi-Party Dependency, the Profile's Sector Fields and the CCF Cross-Reference

Institutions that keep the CBOM in the Applied Quantum CBOM Profile (v1.0-RC or later) record the multi-party dependency factor in the Profile's three financial-services context fields:

- `fs:paymentContext` – swift, card-network, rtgs, ach, instant, correspondent, securities or none.

- `fs:crossBorder` – whether the usage involves counterparties in other jurisdictions.
- `fs:interopConstraint` – whether changing the algorithm requires coordination with external parties.

These are written here as shorthand for the fully qualified `appliedquantum:fs:*` names the Profile specifies. `fs:interopConstraint` is the field Dimension 3's interoperability factor reads, and `fs:paymentContext` names the network whose release date the delivery state waits on.

The record stands without the Profile: an institution on plain CycloneDX records the same three facts in its own fields. The factor does not answer how many distinct cryptographic implementations, trust roots, custody firmware families or key-generation designs execute beneath the counterparties and vendors an entry depends on. That question belongs to the Cryptographic Concentration Framework's Financial Services extension (CCFramework.org), which aligns to this framework's sector taxonomy, classifies counterparties and measures concentration per layer per service. This extension cross-references the CCF result in the Quantum Readiness Assessment and does not compute a concentration figure of its own.

Financial Services Priority Tiers

Priority	System Category	Rationale	Typical Delivery State
Tier 1	Internet-facing entries: internet banking and mobile banking TLS endpoints, Open Banking API endpoints, internet-facing payment and partner APIs, customer portals for wealth management. Partner-facing entries carrying long-horizon data: corporate banking host-to-host connections, interbank messaging channels (including SWIFT), settlement system connections. Trust anchors and	Placed by the ordered test of Activity 3.2: Dimension 1 Critical on an internet-facing entry, or on a partner-facing entry with a confidentiality horizon over 15 years; or Dimension 2 Critical on any factor, which the sector's systemic-criticality factor reaches for links to RTGS, CCPs, CSDs and scheme settlement, the trust-scope and key-lifetime factors reach for roots and enterprise-wide anchors, and verifier	Available for the institution's own edge, API gateways, portals and host-to-host links; dependent for interbank, scheme and settlement connections and the shared trust hierarchies, on the network's release with a firmness grade; dependent or blocked for FIPS-required HSM operations, on the module certificate, and for card and terminal fleets, on the hardware refresh cycle. A dependent or blocked entry keeps

Priority	System Category	Rationale	Typical Delivery State
	long-lifetime signing keys: the internal PKI root, the card network, SWIFT and Open Banking trust hierarchies the institution participates in, HSM-protected root and long-lifetime keys, signed archives verified for 15 years or more. Keys whose verifiers cannot be updated: card and terminal offline authentication (Payments Extension), and any signing key whose verifiers sit in an unmanaged device fleet	updatability reaches for verifiers that cannot be updated (terminal fleets, customer devices holding pinned certificates that no campaign reaches); or Dimension 4 Critical on a mandatory deadline within 2 years. Enrolled customer credentials are not placed by this factor, whose subject is the relying party's verification implementation; where they sit in this tier they sit there on the risk their own dimensions give them, with re-enrollment recorded in the delivery state. Systemic criticality and regulatory visibility follow from the same facts.	this tier and runs under a bridging pattern of Activity 7.4 until the dependency lands (gateway TLS termination in front of a constrained endpoint, PQC key-wrapping around a classical HSM, a double-encryption layer over a shared link the counterparty admits) or, where no bridge reaches a counterparty's verifier, under that activity's documented residual-risk acceptance with a re-evaluation date
Tier 2	Internal platforms carrying data with a confidentiality horizon over 10 years: core banking platform TLS, mortgage servicing platform encryption, database encryption and key wrapping for long-horizon records.	Dimension 1 Critical or High below the Tier-1 conditions (internal, or partner-facing with a horizon of 15 years or less), unless air-gapped; or Dimension 2 High; or Dimension 4 High on the deadline or the contractual-	Available for the platforms the institution operates, except the vendor-locked core platform, which is dependent on a vendor release and has an agility-debt entry; dependent on the partner, the venue,

Priority	System Category	Rationale	Typical Delivery State
	Partner-facing links on private circuits carrying data with a horizon of 15 years or less. Shared intermediate issuers and signing keys that several applications or external parties rely on, with updatable verifiers: trading platform authentication, whether the institution or the venue operates the verifier; regulatory submission signing verified by the receiving authority's software; code signing relied on across several applications. Where the verifier is a counterparty's or an authority's, the entry is dependent on that party's release, recorded in the delivery state. Entries under a contract that requires PQC or a mandatory deadline within 5 years. Digital asset custody, tiered under the Digital Assets Extension's reading of the same test	requirement factor.	the receiving authority, the intermediate issuer or the protocol elsewhere; the entry keeps its tier and shows the unblocking dependency

Priority	System Category	Rationale	Typical Delivery State
Tier 3	Internal services whose data horizon is 10 years or less and whose keys are relied on by one application: internal API gateways and service-to-service TLS carrying short-horizon data, single-application code signing verified through centrally managed trust stores, internal tooling that holds no customer record beyond a 10-year horizon	Any applicable risk dimension (1, 2 or 4) Medium or above, none higher. Internally controlled; migrates on the institution's timeline without external dependencies, and moves to Tier 2 the day a longer horizon, a shared trust dependency or a contractual requirement is recorded against it.	Available
Tier 4	Legacy batch interfaces and archival systems whose contents have no remaining confidentiality need beyond 5 years and no trust dependency, session-only credentials, and test and development estates holding no production data	Every applicable risk dimension Low. Monitor; compensating controls; migrate when feasible. A blocked migration does not place an entry here: card and terminal offline authentication is hardware-constrained and sits in Tier 1 on its risk with the delivery state blocked (Payments Extension).	Blocked entries are shown in the tier the ordered test gives them, not in this one

Phase 4 – Roadmap & Governance

External Dependency Mapping

The financial services roadmap must incorporate external timelines that the institution does not control. Every date below is graded for firmness (Activity 7.5: committed, forecast, announced, unknown). The grade is what Phase 3 Dimension 3 scores. A Tier-1 entry that waits on one of these dates keeps its tier, takes the delivery state dependent or blocked, and appears on the roadmap against the date with its grade:

- **Swift Alliance Release 8.0 and SwiftNet 8.0:** Alliance Release 8.0, the mandatory major release, planned to be available at the end of July 2027; SwiftNet 8.0 released in 2027 as Swift's network enabled for post-quantum cryptography; Release 7.9 first for the majority of the community still on 7.7 (no upgrade path from 7.7 to 8.0) and out of support 15 months after 8.0 ships. Grade: announced. What PQC use the release will require of participants, and when: unknown. Re-checked against Swift's statements in the Payments Extension at each release.
- **Card network PQC timelines:** Visa and Mastercard CA migration timelines and EMV specification updates for PQC certificate handling. Grade: unknown at the June 2026 edition (no committed date obtained). The September 2026 re-check is in the Payments Extension.
- **HSM vendor certification:** FIPS 140-3 Level 3 CMVP validation with PQC algorithms within the validated boundary, and PCI PTS HSM certification of the same firmware for payment HSMs, tracked per product and per firmware family; grade per vendor from the questionnaire. Product names are in Tool and Vendor References.
- **Smart card silicon availability:** PQC-capable smart card silicon announced for 2026 mass production by the major chip suppliers (Payments Extension; grade: announced; supplier names in Tool and Vendor References).
- **Central bank RTGS upgrades:** T2, Fedwire and Bank of England RTGS modernization timelines for PQC adoption. Grade: unknown at this edition; obtained through the counterparty pattern (Activity 7.6), not the vendor questionnaire.
- **Domestic payment scheme upgrades:** ACH, SEPA, Faster Payments scheme-level PQC adoption decisions. Grade: unknown at this edition.
- **Qualified trust service providers:** The date on which each provider's qualified signature, seal and timestamp services extend to post-quantum algorithms (the alignment section's qualified-signatures subsection). Grade: unknown at this edition. The institution's statutory-signature date is the provider's date.
- **Regulatory enforcement milestones:** The plan-by, procure-by and migrate-by dates in this extension's Regulatory Alignment Map and the Universal's roster; PCI SSC standalone PQC guidance (expected; none published at the June 2026 edition); national supervisor examination cycles.

These external dependencies should be visualized on a single timeline map with their grades and reviewed quarterly. Where external timelines slip, the institution's roadmap

adapts through the Re-Baseline Protocol (Activity 4.8): a network or a vendor slipping a committed date beyond the bridging capacity recorded in Activity 7.4, or a supervisor moving a plan-by date, opens a re-baseline review at the next SteerCo, minuted to the evidence dossier, with the authority that owns the date moving it. Internal preparation (Phases 0 to 3) and the migration of everything the institution controls proceed regardless of external readiness.

Gates and Recorded States

Every gate record from G5 → G6 onward, and every wave-exit record, shows two results as separate fields (Universal Activities 4.6 and 5.4): the protection result (which functions and boundaries are verified, which remain exposed) and the agility result (which change was rehearsed, through which mechanism, in what elapsed time, with which constraints). A customer-facing channel that passes on protection and whose gateway can change its algorithm by configuration exits as migrated. A corporate channel that passes on protection behind a vendor-locked core platform exits as migrated with agility debt, with the entry and its closure date in the Phase 3 register; neither result stands in for the other, and the Coverage and Agility KPIs read them separately. Gate records are examination material and are filed to the evidence dossier in the form the supervisor and the auditor read.

Recommended Year-1 Plan Adaptations

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

- **Q1:** Establish governance with cross-business-line representation. Name the owners of the Crypto-Agility workstream and of the Cryptographic Record. Begin PCI 12.3.3 aligned cryptographic inventory on PCI-scoped systems with evidence grades and the denominator stated. Initiate HSM and core-platform vendor engagement (Phase 7 early start), agility questions first. Commission the SWIFT readiness assessment and the trust service provider inquiry.
- **Q2:** Expand inventory to the identity stack, the document-signing infrastructure and the long-retention data stores; payments-scoped entities add message format analysis and the card and terminal estate (Payments Extension). Begin CBOM construction for Tier-1 systems on the minimum record. Join industry coordination forums (FS-ISAC Post Quantum Computing Working Group, Europol QSFF, national supervisor forums). Sign the accepted-gaps register at gate G1 → G2.
- **Q3:** Ratify the scoring model, weights and appeals rule at the SteerCo; complete Tier-1 risk scoring with delivery states; produce the agility-debt register. Produce the initial Quantum Readiness Assessment for board and regulatory consumption, mapped to the supervisory stage the institution reports. Begin Tier-1 pilot design (internet banking edge or external API using hybrid ML-KEM-768 with X25519 for TLS key exchange).

- **Q4:** Execute the first Tier-1 pilot in a test environment and rehearse an algorithm change on the pilot endpoint, timed across the four segments and rolled back. Establish the external dependency timeline map with firmness grades. Produce the Year-2 roadmap with the budget request and the agility milestones on it.

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, and produces candidates for both tracks (Activity 5.1). For financial services, the following pilot targets are recommended, broad banking and capital markets first:

- **Internet banking TLS endpoints:** Enable hybrid key exchange (X25519MLKEM768) on the institution's primary online banking portal. Client-side support is the default across the major browsers (Universal, PQC Deployment Status). 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. Force a fresh handshake on a defined interval for persistent sessions, require the hybrid group on resumption and disable 0-RTT for the flows in scope (Activity 5.2).
- **Mobile banking API endpoints:** Enable hybrid key exchange on the mobile banking API gateway. Mobile app certificate pinning configurations may need updating, and the pinned clients are the sector's first verifier-updatability test. Test against all supported app versions and mobile platforms.
- **Corporate banking host-to-host connections:** Treasury management system links, platforms for cash management, 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 and a published dual-stack window for the corporate clients (Activity 7.6).
- **Internal service-mesh PQC:** Enable hybrid key exchange in the internal TLS mesh between core banking microservices from the mesh control plane. This provides production-scale performance data without external coordination risk.
- **Internal code signing for banking applications:** Pilot dual-signing (ML-DSA-65 alongside existing ECDSA/RSA) for one internal banking application's release pipeline, with the verifier acceptance policy set to require both signatures. 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. Record the receiving authority's verifier acceptance policy.
- **HSM PQC key generation:** If HSM firmware supports PQC key generation (even as a non-approved service outside the validated boundary), pilot PQC key generation and

storage to validate operational key management procedures and the key ceremony. Record the module, firmware family and entropy validation in the Phase 6 register.

- **Payment-channel pilots (Payments Extension):** 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; scheme-interface and terminal pilots are sequenced in the Payments Extension.

The Rehearsal per Wave and the Wave-Exit Criterion

Every wave includes an algorithm-change rehearsal in staging on at least one system in the wave (Activity 5.2), chosen from the layer the institution controls: a parameter-set change from ML-KEM-768 to ML-KEM-1024 on the API gateway or the internet banking edge; a hybrid-to-composite switch on the code-signing pipeline; a certificate-signature-algorithm change on the internal issuer. The rehearsal is timed across assessment, decision, change and verification, with the rollback exercised, scheduled outside the change advisory board's quarter-end, year-end and regulatory-reporting freezes, and the four elapsed times feed the rehearsed time-to-change KPI.

Every wave exit from Wave 1 onward applies the agility criterion (Activity 4.6): negotiated outcome observed; classical-only refused and tested where policy requires it; algorithm changeable by configuration; rehearsal run with the rollback exercised. A system that fails the last two conditions exits the wave as migrated with agility debt. The wave-exit record shows the protection and agility results as separate fields for every system in the wave.

Wave 3 (external, controlled) is where the institution applies the counterparty pattern: published dual-stack windows on host-to-host and Open Banking interfaces, interoperability test events before enforcement, and the refusal decision recorded in the risk register for the counterparty that will not move.

Tokenization Coverage Assessment

Before designing migration pilots for stored-data 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 this framework's default deployment pattern for the transition period, confirmed per deployment profile against the applicable authority rather than required everywhere

(Universal, Activity 5.2, Hybrid mandate divergence). The BIS Project Leap Phase 2 report states that hybridization was not envisaged in T2's original cryptographic design, that the verification software accepts one signature algorithm at the header level, and that payment systems need to be made more agile before or as part of the migration.

Financial institutions should expect hybrid deployments to be more complex than simple algorithm addition: issuance changes in the PKI, extended certificate handling, modified verification logic, expanded message formats, and updated reference data at all counterparties. Whether the issuance change means a second parallel hierarchy or one hierarchy issuing on both algorithms is decided by the compatibility strategy, per deployment, and the T2 experiment tested one architecture rather than settling the question.

Plan for hybrid as an architectural change. Once the verification path is built to accept more than one algorithm, the next algorithm switch is a configuration change. The agility criterion's third condition (algorithm changeable by configuration) tests that it was.

Phase 6 – Infrastructure Modernization & Performance

The HSM and KMS Register

The Universal's Activity 6.2 register is the Phase 6 instrument for the whole HSM estate, general-purpose and payment alike. It records, for each module: the visible platform (the product as procured), the supplier's canonical firmware family, the manufacturer of origin, and the certificate reference, which for a payment HSM is both the FIPS 140-3 certificate and the PCI PTS HSM certificate. Two products under two names can be one firmware family. A cloud KMS is recorded as a dependency boundary rather than as a manufacturer.

The four fields are therefore recorded separately. The boundary-verification rule of Activity 7.7 applies to the cloud rows. Key generation and entropy are recorded beside them: every module that generates long-term PQC keys draws from an SP 800-90B validated source, with the ESV certificate reference (or the ENT designation on the module certificate) and the operating envelope recorded. A "quantum" label on a randomness product is not a requirement of this framework or of any standard it cites.

Institutions carrying the register in a Profile-conformant CBOM record the same facts as `custody:*` and `entropy:*` properties. The register stands without them. Whether two product lines share one firmware family is a Cryptographic Concentration Framework question (layer 4), cross-referenced from the register. Model, firmware and certification references as the June 2026 edition listed them are in Tool and Vendor References.

General-Purpose HSM and KMS Modernization

- **Firmware-upgradeable vs. hardware-replacement HSMs:** Classify the general-purpose estate from the register and the vendor questionnaire: current firmware generations include initial ML-KEM and ML-DSA support on some product lines, on others PQC arrives as an in-field application package or a new hardware variant; older units require replacement, with procurement, certification and deployment lead times of 12 to 24 months. The answer to the first agility question (algorithm change by configuration, without new hardware) sets the class.
- **Validation per product:** Record, per module, the certificate that covers the PQC operation required and its status. Where the module performs the operation as a non-approved service, document the risk decision for the FIPS-aware class and the dependency for the FIPS-required class (the alignment section's validation subsection). Monitor the Modules in Process list for the modules the estate depends on.
- **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. The rehearsal is timed and filed like any other (Activity 5.2).
- **Dual-key management:** During the hybrid period, HSMs must manage both classical and PQC key material simultaneously. Dual-algorithm operation is not twice the key-storage bytes: it adds a second key lifecycle (generation, backup, rotation, destruction) with its own ceremonies, its own backup and replication design, and, for stateful signatures, state handling the classical estate never needed.
- **Cloud KMS:** For each provider's key-management service, record the current PQC key types offered per service and region and the dated targets, graded for firmness, and verify the provider's side of the boundary by observed negotiation where the connection is visible (Activity 7.7). Provider names are in Tool and Vendor References.

Payment HSM Modernization (Payments Extension)

Payment HSMs have their own modernization track, separate from the general-purpose guidance above. A PQC firmware that breaks the PCI PTS HSM certification is not deployable until re-certified. The register records both certificate references per module. The strategy is in the Payments Extension: the firmware-upgradeable versus hardware-replacement classification of the payment HSM estate; the PCI and FIPS certification tracking per firmware family; and the vendor engagement on certification timelines.

Settlement System Performance Benchmarking

Financial institutions participating in RTGS or real-time payment systems should conduct PQC performance benchmarking specific to settlement workflows, with the method in the Payments Extension:

- **Signature verification throughput:** Measure how many ML-DSA verifications per second production-equivalent hardware sustains at peak transaction volumes. Establish the baseline on the institution's own payment path and its target implementation, measuring end-to-end latency, throughput and tail latency separately from the cost of the primitive. Read the Project Leap Phase 2 figure (7.5× on software verification, the one step it timed) as a published case study on pre-standard CRYSTALS-Dilithium in the T2 test environment, and as the reason to run the measurement rather than as the number it will return. Test with hardware acceleration and with the HSM in the loop, and record the benefit on this path as a measured result.
- **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 traffic 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 (Activity 7.1). Financial services requires a finer-grained classification. The table below groups vendors by their role in the financial services infrastructure; entities a reader deals with regardless of choice (schemes, SWIFT, RTGS operators, the regulators) are named, and entities a reader selects among are described by class, with the names as the June 2026 edition listed them in Tool and Vendor References.

Alternative sourcing removes a dependency only if the alternative does not share it. Whether two vendors' products run on one implementation lineage or one firmware family is a question for the Cryptographic Concentration Framework's Financial Services extension. The vendor register records its result by cross-reference. 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 through the counterparty pattern (Activity 7.6). Participate in industry forums and pilot programs. Align institutional roadmap to published network timelines, each graded for firmness.

Vendor Category	Examples	Engagement Approach
Crypto infrastructure	HSM vendors (Tool and Vendor References), PKI/CA providers, qualified trust service providers, key management platforms	Quarterly PQC roadmap reviews. FIPS/PCI certification tracking per firmware family. The four certificate-authority questions to every issuer. Early access to PQC firmware for lab testing.
Platform vendors	Core banking vendors (Tool and Vendor References), card management systems, payment gateways, identity and authentication vendors	The two agility questions and the firmness question first. PQC readiness questionnaires. Contractual PQC upgrade commitments with the acceptance-test rehearsal. CBOM exchange requirements. The credential migration question for identity vendors.
Fintech providers	Open Banking providers, aggregators, TPPs, digital wallet platforms	Coordinate through Open Banking trust framework governance. PQC requirements in TPP onboarding criteria. Dual-stack windows on the API versions.
Digital asset infra	Custody providers, blockchain protocol teams, DLT platform operators	Monitor protocol-level PQC upgrade plans; the protocol is a counterparty (Activity 7.6). Assess custody provider quantum readiness. Evaluate PQC-native chain alternatives (Digital Assets Extension).

Questionnaire Order, Contractual Crypto-Agility and the Acceptance Test

The vendor PQC readiness questionnaire of Activity 7.2 enters the third-party risk management cycle the institution already runs, in the Universal's order: the two agility questions first (can the algorithm be changed by configuration without recompilation,

reinstallation or hardware replacement; can the verifiers and trust stores be updated in the field), then the firmness grade of every date, then the feature, GA-date, interoperability, performance, fallback and CBOM questions.

Contractual crypto-agility is the pattern supervisors are adopting, and one instrument now states it in the framework's own terms: FINMA Guidance 05/2026 (July 9, 2026) recommends that crypto-agility be made a prerequisite for all new outsourcing arrangements in the software and data sectors and incorporated into existing arrangements at the earliest opportunity, with responsibility for the outsourced function remaining with the outsourcing institution.

The Universal's procurement clause (Activity 7.3) already warrants configuration-driven algorithm change. The acceptance test turns the clause into evidence a supervisor accepts: before the product enters production, the institution's own team executes a rehearsed algorithm change on the product using the rehearsal pattern of Activity 5.2, with the elapsed times recorded and the rollback exercised. A product that passes its functional acceptance tests and fails the rehearsal has not met the clause.

The non-standardized-algorithm rule and its one-afternoon test (Activity 7.3) apply to every product offered to the sector as "quantum-safe" on a proprietary or pre-standard algorithm: a public specification, published cryptanalysis, a standards-body track and a validated implementation. A product that fails the first two is excluded. The four certificate-authority questions go to every issuer in the Phase 1 hierarchy map, and every cloud and SaaS vendor is asked for both halves of the roadmap disclosure (Activity 7.7).

Industry Coordination Forums

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

- **Europol Quantum Safe Financial Forum (QSFF):** Published, with FS-ISAC and the Quantum-Readiness Working Group of the Canadian Forum for Digital Infrastructure Resilience, "Prioritising post-quantum cryptography migration activities in financial services" (January 2026), a prioritization methodology that scores quantum risk against migration time. Institutions cross-reference their Phase 3 outputs with it for supervisory defensibility. It is advisory.
- **FS-ISAC Post Quantum Computing Working Group:** Sector-specific threat intelligence and migration guidance, including payment card industry quantum impact analysis and a global coordination timeline (January 2026).
- **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 regulators are establishing quantum readiness working groups. A seat in the working group lets the institution shape regulatory expectations as they form.

FINANCIAL SERVICES REGULATORY ALIGNMENT MAP

Key Regulatory and Industry Coordination Developments

Financial services faces the densest regulatory environment of any sector for PQC migration, and the instruments are read through the Universal's mechanism: the deadline archetype each sets (plan-by, procure-by, migrate-by), the enforcement tier at which it binds, and the framework output that satisfies it. Three instruments, one per archetype, illustrate the shapes the sector meets. PCI DSS v4.0 Requirement 12.3.3 (required after March 31, 2025) is the recurring requirement type: a documented, annually reviewed inventory of cipher suites and protocols, a documentation obligation rather than a remediation mandate, and a market-access requirement for PCI-scoped entities.

DORA (Regulation (EU) 2022/2554) with its ICT risk management standards (Commission Delegated Regulation (EU) 2024/1774, Article 6) is the EU sector regime: a policy on encryption and cryptographic controls with provisions for updating or changing cryptographic technology as cryptanalysis develops, in force since January 17, 2025 with no PQC date, which makes the crypto-agility obligation current rather than future. FINMA Guidance 05/2026 (July 9, 2026) is the dated supervisory expectation: a post-quantum roadmap by mid-2027, a cryptographic inventory, HNDL protection for critical data and crypto-agility as a prerequisite in new outsourcing arrangements, all under existing operational-risk and resilience rules.

The table below lists the coordination bodies whose publications supervisors read and the two national regulators that have issued a readiness index or a date for the sector, with their status at this edition and their enforcement tier. Jurisdiction rows that repeat the Universal's roster (NIST IR 8547, the EU coordinated roadmap, NCSC UK) are not reproduced here. The roster is in the Universal's Regulatory Timeline Context and, kept current, on the Global PQC Migration Clock page, and the instruments that bind a given

institution are recorded in its Regulatory Horizon Report (Universal, GRC Implementation).

The table is a dated snapshot of the sector bodies and the national regulators that set a sector expectation, as of September 2026. The enforcement tiers follow the Universal's definition of the tier by who enforces (tier 1, market access; tier 2, supervisory directive with a named enforcer; tier 3, binding government mandate with an audit trail; tier 4, authoritative guidance; tier 5, advisory); Phase 3 Dimension 4 reads the tier. Every date is re-checked against its instrument at each release, and readers verify status and applicability for their own institution before planning against a row.

Instrument	Requirement and dates	Status at this edition (enforcement tier)	Framework phases and financial-services implication
PCI DSS v4.0 Requirement 12.3.3 (PCI SSC)	Document and annually review all cryptographic cipher suites and protocols in use; required after March 31, 2025	In force (tier 1: a market-access requirement for PCI-scoped entities, assessed by QSAs)	Phase 1 and Phase 2: the inventory requirement in all but name; the CBOM produces the 12.3.3 inventory evidence as a standard output, with the review cadence, the viability monitoring and the documented response strategy evidenced from the program. PCI SSC had published no standalone PQC guidance at the June 2026 edition; re-checked at each release.
DORA, Regulation (EU) 2022/2554, with the RTS on the ICT risk management framework, Commission Delegated Regulation (EU) 2024/1774 (Articles 6 and 7)	A policy on encryption and cryptographic controls, with provisions for updating or changing cryptographic technology on the basis of	In force (tier 3: binding EU regulation with supervisory examination and reporting obligations)	Phase 0, 4 and 7: the crypto-agility obligation is current; the procurement clause and its acceptance test, the rehearsal records and the verification records are the DORA

Instrument	Requirement and dates	Status at this edition (enforcement tier)	Framework phases and financial-services implication
	developments in cryptanalysis, and key-management rules; in application since January 17, 2025; no PQC date		ICT risk evidence.
G7 Cyber Expert Group, Statement on Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector (January 13, 2026)	Phased activities from awareness and inventory to migration; critical systems and assets prioritized within 2030–2032; non-critical systems by around 2035	Published; states that it sets no guidance or regulatory expectations (tier 5, advisory; hardening through the national supervisors that co-chair and cite it)	Phase 0 and Phase 4: the business-case trajectory and the roadmap's outer dates.
Europol Quantum Safe Financial Forum with FS-ISAC and the CFDIR Quantum-Readiness Working Group, "Prioritising post-quantum cryptography migration activities in financial services" (January 2026)	Prioritization methodology: quantum risk scored against migration time, with cryptographic agility as a design requirement	Published (tier 5, advisory)	Phase 3: the closest external method to this extension's scoring; cross-reference the Phase 3 outputs for supervisory defensibility.
FS-ISAC Post Quantum Computing Working Group	Technical guides and a global coordination timeline (January 2026); payment card impact analysis	Published (tier 5, advisory)	Phase 0 and Phase 7: the coordination channel; join as a Phase 0 action.
BIS Papers No. 158, "Quantum-readiness for the financial system: a roadmap" (Bank for	Awareness, governance and cryptographic inventory as foundations; crypto-	Published; the authors' views, not necessarily the BIS's (tier 5, advisory)	Phase 0: the central-bank-authored reference for the business case; Project Leap results

Instrument	Requirement and dates	Status at this edition (enforcement tier)	Framework phases and financial-services implication
International Settlements, July 2025)	agility, defense in depth, hybrid schemes and phased migration		in the Payments Extension.
HKMA Quantum Preparedness Index and Whitepaper on Quantum Preparedness of Hong Kong's Banking Sector (announced February 3, 2026; first index and whitepaper published July 27, 2026)	Banks assessed across awareness, planning, pilots and practical preparedness, from a survey conducted in early 2026; a stated sector target for 2030	First reading published; scores belong on the Global PQC Migration Clock page and are not reproduced here (tier 2: a supervisor with examination powers has stated the scale it scores on)	Maturity Model supplement and the QRA: institutions operating in Hong Kong expect examination questions on the index; the crosswalk of its four stages to the framework phases is in Universal Appendix G.
FINMA Guidance 05/2026, Quantum computing (July 9, 2026)	Strategy and roadmap by mid-2027 at the latest; risk analysis and cryptographic inventory; protection of critical data against HNDL; crypto-agility as a requirement for procured and developed systems and a prerequisite in new outsourcing arrangements; a survey of 60 institutions (November 2025 to January 2026)	Supervisory communication in force under existing technology-neutral rules; survey figures belong on the Global PQC Migration Clock page and are not reproduced here (tier 2: supervisory expectation with a named enforcer and a date)	Phase 0, 1, 4 and 7: the plan-by date, the inventory, the data-at-rest priority and the contractual crypto-agility clause map one to one.
Swift Alliance Release 8.0 /	Release 7.9 as the foundation for 8.0 and PQC readiness,	Announced (firmness grade: announced; the participant PQC	Phase 5 and Phase 7: the interbank pilot and the counterparty

Instrument	Requirement and dates	Status at this edition (enforcement tier)	Framework phases and financial-services implication
SwiftNet 8.0 (Swift)	needed by the majority of the community because there is no upgrade path from 7.7; Alliance Release 8.0, mandatory, planned for end July 2027; SwiftNet 8.0 released in 2027 enabled for post-quantum cryptography; 7.9 out of support 15 months after 8.0 ships	requirement and its date unknown); re-checked in the Payments Extension at each release (tier 1 once mandated for the community: a market-access gate on the network)	pattern; the date drives the delivery state of every SWIFT-dependent Tier-1 entry.

Enforcement tiers the Universal does not assign are recorded here as this extension's reading: PCI DSS 12.3.3 tier 1; DORA tier 3; the G7, Europol, FS-ISAC and BIS publications tier 5; the HKMA index and FINMA Guidance 05/2026 tier 2; SwiftNet 8.0 tier 1 once the network mandates it. The June 2026 edition's MAS row (an advisory circular with no date) is not carried. A 2026 MAS supervisory statement reported to set an end-of-decade target is on the verify-first register and enters the map when verified against the instrument.

FINANCIAL SERVICES MATURITY MODEL SUPPLEMENT

The levels, names and descriptions are the Universal's single 0 to 5 scale (Maturity Levels), used by the enterprise model and every per-phase table alike. The sector indicators are read beside them. Each level from 2 upward has an indicator for Track B, which measures the signature track on its own (Challenge 2).

Level	Universal Level	Financial Services Indicator
0	Unaware: no organizational awareness of quantum cryptographic risk; no activities planned or underway	No sector indicator.
1	Aware: quantum risk acknowledged at leadership level; initial education conducted; no formal program	PCI 12.3.3 compliance may be ad hoc. No inventory of the HSM estate or the trust service providers. No engagement with SWIFT, the schemes or the supervisor on quantum readiness; the supervisor's readiness survey answered from awareness alone.
2	Initiated: formal program chartered; budget allocated; discovery underway; initial CBOM in development	Charter states both outcomes; Crypto-Agility and Cryptographic Record owners named. PCI 12.3.3's inventory element met with structured

Level	Universal Level	Financial Services Indicator
		cryptographic documentation on the minimum record. HSM estate in the four-field register with certificate status. SWIFT, scheme and trust service provider readiness inquiries issued. Priority A inventory complete with evidence grades and a stated denominator; accepted-gaps register signed. Initial QRA produced for the board and the supervisor, with the Track B findings stated separately.
3	Progressing: CBOM operational; risk scoring complete; hybrid pilots in production; vendor engagement active; KPIs reported	Scoring model ratified with the sector factors and under model-risk treatment; agility-debt register produced. External dependency timeline map maintained with firmness grades. Year-1 plan in execution. HSM and core-platform vendor roadmap reviews quarterly, agility questions answered. Industry forum participation active. Tokenization coverage assessed. Regulatory alignment map current in the Regulatory Horizon Report. First algorithm-change rehearsal run on the customer-facing edge; code-signing dual-signing pilot run.
4	Advanced: Tier-1 systems migrated to hybrid/PQC; PKI modernized; crypto-agility demonstrated; vendor	Hybrid key exchange deployed on Tier-1 systems (customer-facing channels, host-to-host links, external APIs) with the negotiated

Level	Universal Level	Financial Services Indicator
	commitments secured	outcome observed; interbank interfaces pass the protection result at their gates (the hybrid negotiated with the network and accepted by it); each that fails the configuration or rehearsal conditions is recorded as migrated with agility debt against a graded network date. HSM PQC operations in validated or risk-accepted mode per product. Two results in every gate and wave-exit record. An algorithm change rehearsed on the edge and on the internal issuer inside the agility window. Private hierarchy for client authentication in place. CBOM integrated into the PCI compliance workflow and the examination response. Contractual crypto-agility with the acceptance test in every new outsourcing arrangement.
5	Optimized: estate-wide PQC migration substantially complete; crypto-agility is organizational capability; continuous monitoring and posture management operational	All customer, interbank and market-infrastructure channels quantum-safe or hybrid; every shared interface has followed its network or has a SteerCo-signed exception. Qualified-signature archives re-anchored on schedule; statutory signatures on the provider's post-quantum services or under a recorded bridge. Full CBOM exchange with Tier 1 vendors. Standing

Level	Universal Level	Financial Services Indicator
		rehearsal cadence on the edge, the issuers and the signing services; the closure proof run per track. Agility-debt register at zero unaccepted debt: every remaining entry funded with a date or under a SteerCo-signed exception. Payment channels per the Payments Extension.

FINANCIAL SERVICES KPI SUPPLEMENT

The Universal Framework defines board-level, operational, agility and evidence-dossier KPIs (Metrics, KPIs & Reporting). The following additional KPIs are recommended for financial services, broad banking first, with the payments-specific measures grouped and detailed in the Payments Extension:

Board-Level KPIs (Quarterly)

- **External interface quantum exposure:** Number of external-facing interfaces (interbank messaging, host-to-host, Open Banking APIs, market-infrastructure links, scheme connections) operating without hybrid or PQC key establishment observed / total external interfaces, with the incidental line reported separately (Universal, enforcement counting rule).
- **HNDL data-at-risk volume:** Estimated volume of data in transit across external interfaces with confidentiality requirements exceeding 10 years that is not yet protected by hybrid or PQC key exchange. The risk-weighted companion to Coverage.
- **TNFL exposure, signature track:** Number of long-validity signed artifact classes (regulatory filings, trade confirmations, qualified-signature archives, code-signing keys, root and intermediate CAs) with no post-quantum or composite signature path and no re-anchoring schedule, reported beside the Universal's Trust KPI on its own line.
- **Regulatory readiness:** Status against each binding instrument in the Regulatory Horizon Report (PCI 12.3.3 evidence current; DORA cryptographic-controls policy with its update provision. The plan-by dates that apply), and the supervisory stage the institution reports on its readiness index, with the Track B finding stated beside it.
- **Payment HSM PQC readiness (Payments Extension):** Percentage of payment HSMs with PQC-capable firmware installed and the certificate that covers the operation / total payment HSM estate.

Operational KPIs (Monthly)

- **Vendor PQC roadmap alignment:** Number of critical vendors (HSM, core banking, identity, messaging, trust service providers) with dated PQC roadmaps, by firmness grade / total critical vendors. A date graded unknown does not count.
- **Counterparty readiness:** Share of external interfaces on which the counterparty has negotiated hybrid key exchange (observed), is inside a published dual-stack window, or is past a deprecation date without moving (each on its own line).
- **Tokenization coverage:** Percentage of high-sensitivity data categories protected by tokenization (providing interim HNDL defense).
- **Message format PQC readiness (Payments Extension):** Number of payment message formats analyzed for PQC payload accommodation / total formats in use.

Agility KPIs (CISO cascade, monthly; summarized to the board under the Agility KPI)

The four agility KPIs of the Universal (Metrics, KPIs & Reporting) are measured on the layer the institution controls, and the shared interfaces whose algorithm the network sets are reported beside them, never inside them.

KPI	Financial services measurement	Threshold
Configuration-driven share	Percentage of Tier-1 and Tier-2 systems (the internet banking edge, the API gateway, host-to-host endpoints, the internal issuers, the code-signing and document-signing services, the HSM and KMS estate) whose key-establishment and signature algorithms change by configuration, verified by rehearsal; the vendor-locked core platform and the network-set shared interfaces are their own line and never enter the numerator	Target by year from the roadmap's agility milestones; a year missed by more than 10 points triggers Crypto-Agility workstream review
Rehearsed time-to-change	Elapsed time across assessment, decision, change and verification on the most recent rehearsal, per track:	Inside the agility window; a rehearsal whose change segment cannot run without a vendor release or a network

KPI	Financial services measurement	Threshold
	on the edge or the API gateway for Track A, on the internal issuer or the code-signing service for Track B (Activity 5.2), scheduled outside the change advisory board's freezes	cutover has found agility debt on that system, recorded in the register rather than as a variance
Agility-debt burn-down	Entries closed on the Phase 3 register per quarter, with the vendor-locked and network-set populations reported as their own denominators	Any quarter with no reduction triggers workstream review; before closure every remaining entry carries a funded treatment with a date or a SteerCo-signed exception
New-system agility compliance	Percentage of new deployments passing the CI/CD crypto-policy check and the provider-pattern review, and percentage of new outsourcing arrangements that include the contractual crypto-agility clause with the acceptance-test rehearsal passed before go-live	Below 95% in any month triggers architecture and procurement governance review

RECOMMENDED IMMEDIATE ACTIONS

For financial institutions at Maturity Levels 1 (Aware) and 2 (Initiated), the following actions can begin immediately and do not depend on external vendor readiness. Actions 1 to 8 apply across financial services; actions 9 and 10 are the sector's agility actions. The payments-specific actions are in the Payments Extension:

#	Action	Timeline	Framework Phase
1	Establish a Quantum Readiness Working Group with representation from IT security, risk management, compliance, treasury, retail banking, corporate banking, capital markets, and digital channels; charter the program on both outcomes	0–1 month	Phase 0
2	Launch a structured cryptographic inventory across internet banking, core banking, the identity stack and trading platforms, with an evidence grade on every finding and the denominator stated before the tools run. For PCI-scoped entities, align with	0–3 months	Phase 1 / Phase 2

#	Action	Timeline	Framework Phase
	Requirement 12.3.3 so the same inventory serves PQC readiness and the 12.3.3 inventory element		
3	Map the complete HSM and KMS estate (general-purpose and payment HSMs) into the four-field register with certificate status. Check whether the current HSM vendor offers integrated discovery capability. Initiate vendor engagement on PQC firmware and certification timelines, agility questions first	0–3 months	Phase 1 / Phase 6 / Phase 7
4	Inventory the trust service providers behind qualified signatures and seals and the signed archives by document class and retention; ask each provider the certificate-authority questions and the qualified-status question	0–3 months	Phase 1 / Phase 7
5	Conduct a tokenization coverage assessment to identify data categories already quantum-defended	0–3 months	Phase 5

#	Action	Timeline	Framework Phase
	and prioritize remaining exposed data		
6	Join at least one industry PQC coordination forum (Europol QSFF, FS-ISAC Post Quantum Computing Working Group, the national supervisor's forum)	0–3 months	Phase 0 / Phase 7
7	Produce an initial Quantum Readiness Assessment suitable for the board risk committee and the supervisor's readiness inquiry, with the Track B findings stated on their own	3–6 months	Phase 3
8	Enable hybrid key exchange (X25519MLKEM768) on at least one internet banking or external API endpoint to gain operational experience, and count it toward Coverage only once the negotiated outcome is observed and the policy is tested	3–9 months	Phase 5
9	Name a Crypto-Agility workstream owner in the function that controls the	0–1 month	Phase 0

#	Action	Timeline	Framework Phase
	customer-facing edge, the internal PKI and the signing services, with a budget line from Year 1 and the agility-debt register as scope; name the Cryptographic Record owner beside it		
10	Schedule the first rehearsal on the pilot endpoint of action 8: change the key-establishment parameter set by configuration, time the four segments, roll it back, and file the timings as the first agility KPI reading and the first entry in the closure evidence	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.
- **Why Harvest Now, Decrypt Later Cannot Be Detected –** https://postquantum.com/post-quantum/cannot-detect-harvest-now-decrypt-later/ – The July 2026 analysis of why a passive collector leaves no evidence, and why the absence of evidence is not reassurance. The reasoning behind the inference this extension plans on.
- **Hong Kong's HKMA Launches Quantum Preparedness Index to Safeguard Finance –** https://postquantum.com/security-pqc/hkma-quantum-preparedness-index/ – The

index's four dimensions and what an institution operating in Hong Kong should expect at examination.

- **FINMA Quantum Guidance: Swiss PQC Roadmaps by Mid-2027 –** https://postquantum.com/security-pqc/finma-quantum-guidance/ – FINMA Guidance 05/2026 read for practitioners: the plan-by date, the inventory expectation and the outsourcing clause.
- **The Global PQC Migration Clock –** https://postquantum.com/pqc-migration-timelines/global-pqc-migration-clock/ – The maintained jurisdiction roster this extension's regulatory map points to, updated from the PQC Migration Brief.

APPENDIX J: REQUIREMENTS REGISTER

This register is generated from the text of this edition at each build and lists every statement in this extension that uses *must*. The four program-level provisions of the Universal Framework's Normative Convention bind this extension through its parent and are listed in the Universal's Appendix J; they are not repeated here. Every statement below binds inside the section that states it, and a statement that appears here without its section's conditions is read with them. The appendix letter matches the Universal's, so "Appendix J" names the requirements register in every document of the set.

Statements in document order

1. *Why Financial Services Requires a Sector Extension, Multi-Party Coordination as the Binding Constraint.* Vendor and supply chain governance (Phase 7) is therefore a critical-path constraint that must start in Phase 0.
2. *Industry-Specific Challenges, Challenge 2: Trust Now, Forge Later (TNFL) Risks in Financial Systems.* Phase 3 risk scoring must assess TNFL exposure on signed artifacts with long verification periods as well as HNDL exposure on encrypted data.
3. *Industry-Specific Challenges, Challenge 3: Core Banking Platform Dependency.* A global bank running one platform on each of three continents must coordinate a separate PQC migration stream per platform, against a different vendor roadmap for each, with every date graded for firmness (Activity 7.5).
4. *Industry-Specific Challenges, Challenge 3: Core Banking Platform Dependency.* Phase 7 vendor governance must identify core banking vendors as Strategic Blocking vendors from the outset.
5. *Industry-Specific Challenges, Challenge 8: Payment Message Format Constraints (See Payments Extension).* Framework Impact: Phase 1 (Discovery) must include message format analysis as a distinct inventory track.
6. *Industry-Specific Challenges, Challenge 8: Payment Message Format Constraints (See Payments Extension).* Phase 3 (Risk Scoring) must weight message-format-constrained systems separately.
7. *Industry-Specific Challenges, Challenge 8: Payment Message Format Constraints (See Payments Extension).* Phase 5 (Pilots) must include message-format-specific testing with realistic payload sizes.

8. *Industry-Specific Challenges, Challenge 9: Smart Card and Terminal Constraints (See Payments Extension).* Framework Impact: Phase 4 (Roadmap) must incorporate hardware refresh cycles for cards and terminals as hard constraints on migration timelines.

9. *Industry-Specific Challenges, Challenge 9: Smart Card and Terminal Constraints (See Payments Extension).* Phase 5 must include a triage strategy separating online (symmetric-safe) from offline (asymmetric-vulnerable) authentication.

10. *Industry-Specific Challenges, Challenge 10: The Payment HSM Certification Bottleneck (See Payments Extension).* Framework Impact: Phase 6 (Infrastructure) must include HSM certification tracking as a gating dependency.

11. *Industry-Specific Challenges, Challenge 10: The Payment HSM Certification Bottleneck (See Payments Extension).* Phase 7 (Vendor Governance) must establish structured engagement with HSM vendors specifically around FIPS/PCI certification timelines.

12. *Industry-Specific Challenges, Challenge 11: Settlement Latency and Performance (See Payments Extension).* 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.

13. *Industry-Specific Challenges, Challenge 11: Settlement Latency and Performance (See Payments Extension).* Framework Impact: Phase 6 (Infrastructure) must include settlement-system-specific performance benchmarking.

14. *Industry-Specific Challenges, Challenge 12: Cross-Border and Multi-Network Coordination (See Payments Extension).* Framework Impact: Phase 0 (Executive Mandate) must establish cross-industry coordination mechanisms from the outset.

15. *Industry-Specific Challenges, Challenge 12: Cross-Border and Multi-Network Coordination (See Payments Extension).* Phase 4 (Roadmap) must map external dependency timelines from SWIFT, card networks, and central banks as hard constraints.

16. *Industry-Specific Challenges, Challenge 15: Securities, Custody, and Post-Trade Infrastructure.* Custodian banks face a specific challenge: they hold assets on behalf of institutional clients and must authenticate instructions from those clients.

17. *Industry-Specific Challenges, Challenge 19: Digital Assets and Blockchain Quantum Vulnerability (See Digital Assets Extension).* 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.

18. *Alignment with Universal Framework v3.0, Hybrid and Composite Signatures as the Track B Default.* Regulatory filings, trade confirmations, e-signed legal documents, and audit trails must remain verifiable for years or decades.

19. *Alignment with Universal Framework v3.0, SP 800-208 for Application Release and Firmware Signing.* A signing service that does not meet section 8 is not a conforming deployment, and the verifiers must accept the parameter set chosen.

20. *Phase 0 adaptation, Shared Machinery with the AI-Security Mandate in Banking.* The second is the vendor register: the model vendors, cloud providers and core-banking vendors the AI plan must assess are the Phase 7 vendors.

21. *Phase 0 adaptation, Governance Adaptation.* The steering committee must have the authority to coordinate across business lines that control different channels (cards, corporate banking, wealth management, digital assets).

22. *Phase 1 adaptation, Discovery Tooling Reachable Through the Existing HSM Vendor.* It may, though, provide a faster start on discovery Layer 4 (embedded and third-party) and on the CBOM Layer 2 platform cryptography (the HSM and KMS estate) that a bank's CBOM must cover first.

23. *Phase 2 adaptation, Financial Services CBOM Complexity.* The order of magnitude the discovery exercise in the sector characteristics illustrates (tens of thousands of unique cryptographic functions across one payment's nine-party chain) means the CBOM must span organizational boundaries, something the standard CBOM model does not address.

24. *Phase 4 adaptation, External Dependency Mapping.* The financial services roadmap must incorporate external timelines that the institution does not control.

25. *Phase 6 adaptation, General-Purpose HSM and KMS Modernization.* - Dual-key management: During the hybrid period, HSMs must manage both classical and PQC key material simultaneously.

ABOUT

ABOUT THE AUTHOR

Marin Ivezic is a former Fortune Global 500 CISO/CTO, the founder and CEO of Applied Quantum, and the founder of Quantum Academy (QuantumAcademy.com). PostQuantum.com is his personal blog. 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 standards, products and deadlines change, and the book supplies the depth that a methodology document omits by design.

QUANTUM ACADEMY

Quantum Academy (QuantumAcademy.com), founded by the author, offers trainings and certifications on the topics this framework covers, from executive education on quantum risk to practitioner courses on PQC migration, crypto-agility and cryptographic inventory, for the roles and training levels described in Skills & Team Structure.

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