SEPTEMBER 2026

APPLIED QUANTUM

THE APPLIED QUANTUM PQC MIGRATION FRAMEWORK

PAYMENTS EXTENSION

Card, interbank and settlement infrastructure – *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 These references may become outdated quickly.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	Payment infrastructure engineers, card network architects, HSM operations teams, terminal fleet managers, payment security officers, CISOs and program managers with payment system responsibility
Assumed knowledge	Familiarity with the Universal PQC Migration Framework v3.0 and its 8-phase lifecycle; working knowledge of card payment systems, RTGS/settlement infrastructure, SWIFT messaging, terminal and ATM fleets, and payment HSM operations
Scope	Payment-infrastructure-specific PQC migration challenges and framework adaptations: card networks, RTGS systems, SWIFT/ISO

	20022 messaging, payment HSMs, POS terminals and ATMs, mobile payments, and cross-border correspondent banking. Companion to the Financial Services Extension, which carries the broader banking picture. Not a standalone document: intended to be used alongside the Universal Framework and the Financial Services Extension.
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 & Program Closure section, identity and authentication stack in

Version	Date	Changes
		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 payment infrastructure: the agility objective stated for the sector (a payment organization is crypto-agile when it can change the algorithm on its own gateways, HSM estate and signing services on a planned date and can name the date on which each scheme, network and terminal population will follow), the agility criterion and a rehearsal per wave on the external payment API gateway, the firmware-signing pipeline and the internal issuer, with a key ceremony that generates a PQC-authorized key as the payment HSM estate's rehearsal and the quarterly failover to the backup HSM partition recorded as a failover and state-management exercise outside the rehearsed time-to-change KPI, "migrated with agility debt" as the expected recorded state for the scheme-set interfaces and the enclosed terminal populations, and closure at zero unaccepted agility debt with the four verification dispositions read against terminal fleets and scheme dependencies. The Universal's five-point Payments note expanded (the attacker's horizon on cardholder data with the sensitive-authentication-data prohibition; scheme and PCI requirements as market-access gates at enforcement tier 1; both certificate references per payment HSM in the Activity 6.2 register; terminal fleets as the long tail enclosed under the OT extension's Encapsulate Strategy; HSM vendor concentration as a Cryptographic Concentration Framework question). Corrections made in the open: the

Version	Date	Changes
		validation subsection rewritten to the per-product rule (CMVP certificates #5247, April 2026, and #5497, August 2026, each with its qualifications) in place of the June 2026 mid-2027 expectation; the Project Leap Phase 2 account restated from the BIS report of December 11, 2025 (the missing certificate recorded as expected, not resolved by hand; the header change achieved through new components, not a buffer overrun; Dilithium Round 3, software keys and raw key pairs as the report's stated limits); the EMVCo reference corrected from a "quantum working group" to EMVCo's position statement and its January 30, 2026 statement expecting no practical threat to EMV before 2040, maybe never; the Swift dates restated from Swift's own pages (Alliance Release 8.0 planned for end July 2027; Release 7.9 needed first by the majority of the community, out of support 15 months after 8.0; SwiftNet 8.0 released in 2027 enabled for PQC); PCI PTS HSM v5.0 (May 18, 2026) replacing the v4 references throughout, with the v4 Security Requirements open for new device security approvals until June 30, 2027 and the v3 and v4 device approval expirations extended to April 2028 and April 2033 per PCI SSC's bulletin of March 2, 2026; the systemic-loss figures attributed to the Hudson Institute as the BIS report relays them; the ISO 8583 field-limit statement restated as the base standard's 999-byte ceiling and the 255-byte Field 55 implementation limit. 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: the dual-outcome charter with named Crypto-Agility and Cryptographic Record owners and the three lines by function (Phase 0); evidence grades, the enumerated denominator and verifier updatability on the terminal track (Phase 1); the minimum record, the concentric rings mapped to the CBOM layers and the Profile as informative carriage (Phase 2); the two sector dimensions restated as factors inside Dimensions 2 and 3 with the arithmetic, verifier updatability at the Universal's reading, the priority tiers assigned by the Universal's ordered test, delivery state and the agility-debt register (Phase 3); firmness grades on every external date, two results per gate record and the Re-Baseline Protocol (Phase 4); the rehearsal per wave, the wave-exit criterion and a terminal firmware-signing pilot (Phase 5); the four-field HSM register with both certificate references and entropy references (Phase 6); questionnaire order, the

Version	Date	Changes
		certificate-authority questions to the scheme, EMV and SWIFT CAs, the one-afternoon test and the Profile's fs:* fields with the Cryptographic Concentration Framework's Payments extension cross-referenced (Phase 7). Regulatory content restructured under E1: three named instruments in the prose (PCI DSS 12.3.3; PCI PTS HSM v5.0; the Singapore Quantum-Safe Migration Handbook's CII milestones); the map rebuilt at four columns with status and enforcement-tier columns and the jurisdiction roster replaced by the Global PQC Migration Clock pointer; the MAS and ECB announced-but-unissued instruments carried as verify-first items. Commercial vendor and product names moved to Tool and Vendor References. Maturity supplement on the Universal's 0 to 5 scale; four agility KPIs; twelve 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 both the Applied Quantum PQC Migration Framework (Universal) and the Financial Services Extension. It does not replace either document but extends them with payment-infrastructure-specific guidance. The Universal's Payments note (Sector Adaptation Notes) is the binding summary of the five constraints this extension expands; the Financial Services Extension covers challenges common to all financial sub-sectors, and this Payments Extension goes deeper into the transaction processing infrastructure itself and points to the Financial Services Extension for the broader banking picture. For each topic, this extension identifies the payment-specific challenge and then maps specific adaptations to the relevant Universal Framework phase. Readers should have the Universal Framework open alongside this document and cross-reference its phase definitions, maturity indicators, and templates.

WHAT'S NEW IN V3.0

Version 3.0 of the Payments 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 payment organization is crypto-agile when it can change the algorithm on its own payment gateways, its own HSM estate and its own signing services on a planned date, and can name the date on which each scheme, network and terminal population will follow; the agility criterion and the rehearsal per wave run on those layers, with a key ceremony that generates a PQC-authorized key as the payment HSM estate's rehearsal and the quarterly failover to the backup HSM partition recorded as a failover and state-management exercise outside the rehearsed time-to-change KPI, "migrated with agility debt" is the expected recorded state for the scheme-set interfaces and enclosure with a dated bridge or a signed exception is the recorded state for the terminal populations that will not migrate natively, 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.

The Universal's Payments note, expanded. The five points of the Universal's new Payments note are the frame of this edition. Cardholder-data horizons are phrased as the attacker's horizon, with the PCI DSS prohibition on retaining sensitive authentication data after authorization stated beside them (Challenge 6; Track A). Scheme and PCI requirements are treated as market-access gates at enforcement tier 1 (Challenge 6; the regulatory map). Payment HSMs carry both certificate references, FIPS 140-3 and PCI PTS HSM, in the Activity 6.2 register, and a PQC firmware that breaks the PCI certification is not deployable until re-certified (Challenge 2; Phase 6). Terminal fleets are the long tail of the payments estate, inventoried with verifier updatability and, where they will never migrate natively, enclosed under the OT & Critical Infrastructure Extension's "The Encapsulate Strategy" by its name (Challenges 3 and 10; Phase 5). HSM vendor concentration is a Cryptographic Concentration Framework question, cross-referenced with the Profile's fs:* fields and never computed here (Phase 7).

Corrections made in the open. 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 June 2026 account of BIS Project Leap Phase 2 is restated from the report of December 11, 2025: the missing certificate was an expected outcome that confirmed settlement's reliance on centralized certificate data, not a failure resolved by hand; the header change was achieved through new and reconfigured components rather than recorded as a buffer overrun; and the report's stated limits (Dilithium Round 3 rather than ML-DSA, software key files rather than an HSM, raw keys rather than certificates, one algorithm at the header level so no hybrid signature could be tested) are carried with the figures. The "EMVCo quantum working group" is corrected to EMVCo's published position statement and its January 30, 2026 statement that it expects no practical threat to the EMV infrastructure before 2040, maybe never. The Swift dates are restated from Swift's own pages: Alliance Release 8.0 planned for end July 2027, Release 7.9 needed first by the majority of the community because there is no upgrade path from 7.7, out of support 15 months after 8.0, SwiftNet 8.0 released in 2027 enabled for post-quantum cryptography; the Visa and Mastercard CA migration dates are graded unknown as of September 2026. PCI PTS HSM v5.0 (May 18, 2026) replaces the v4 references throughout, with the v4 transition stated from PCI SSC's bulletin of March 2, 2026: the v4 Security Requirements open for new device security approvals until June 30, 2027, and the v3 and v4 device approval expiration dates extended to April 2028 and April 2033. The systemic-loss figures are attributed to the Hudson Institute as the BIS report relays them, in place of the June edition's joint attribution; the six-month-recession framing is the study's own and is retained, and the GDP range and dollar figures are described as conditional estimates in its scenarios. The ISO 8583 statement is restated as the base standard's 999-byte ceiling on variable-length fields and the 255-byte Field 55 implementation limit.

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, its closure subsection rewritten to the four dispositions read against terminal fleets and scheme dependencies, 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: the dual-outcome charter, named Crypto-Agility and Cryptographic Record owners and the three lines by function (Phase 0); evidence grades, the enumerated denominator and verifier updatability on the card and terminal track (Phase 1); the minimum record, the concentric rings mapped to the CBOM layers and 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, verifier updatability at the Universal's reading, the priority tiers assigned by the Universal's ordered test, delivery state and the agility-debt register, and a delivery-state column in the priority-tier table (Phase 3); firmness grades on every external date as of September 2026, two results per gate record and the Re-Baseline Protocol (Phase 4); the rehearsal per wave, the wave-exit criterion and a terminal firmware-signing pilot (Phase 5); the four-field HSM register with both certificate references and entropy references, and the partition failover recorded as a failover and state-management exercise beside the estate's key-ceremony rehearsal (Phase 6); the questionnaire order, the certificate-authority questions to the scheme, EMV and SWIFT CAs, the acceptance-test rehearsal, the one-afternoon test and the HSM-concentration cross-reference to the Cryptographic Concentration Framework's Payments extension (Phase 7). The regulatory map is rebuilt at four columns as a dated snapshot with status and enforcement-tier columns, with PCI PTS HSM v5.0, the Singapore CII milestones and the BIS report added and the EMVCo row restated; the MAS supervisory expectations announced for later in 2026 and the ECB's pre-announced quantum letter are carried as verify-first items, not rows. The maturity supplement is re-based on the Universal's 0 to 5 scale; the KPI supplement gains a terminal-fleet disposition line, a counterparty-readiness line and the four agility KPIs; twelve immediate actions include naming the agility owner and scheduling the first rehearsal, with the first partition failover recorded outside the agility KPI. Commercial vendor and product names move to Tool and Vendor References; Further Reading adds the July 2026 HNDL analysis, the Singapore and MAS analyses, the Global PQC Migration Clock and the BIS report; Appendix J lists the extension's own requirements.

WHAT'S NEW IN V2.1

Version 2.1 of the Payments 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 payment infrastructure: composite and dual signatures under payment message size constraints; algorithm-specific vulnerability weighting and the EMV ECC transition; the identity stack in payments (payment passkeys, 3DS signing, wallet credentials, token signing); SP 800-208 stateful hash-based signatures as the deploy-now action for terminal, ATM, and HSM firmware signing; protection of the payment CBOM as a high-value intelligence target; and verification and decommissioning in multi-party payment networks. 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, a duplicated passage in Challenge 2 was removed, and payment passkeys were added to the mobile wallet challenge. A cross-reference to the companion book, *Quantum Ready*, was added.

WHAT'S NEW IN V2.0

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

Alignment with Universal Framework v2.0. The parent framework introduced a two-track migration model, deployment-environment classification addressing the FIPS 140-3 validation gap, and a position on Merkle Tree Certificates for public Web PKI. This extension maps those changes to payment infrastructure: card networks, RTGS systems, SWIFT and ISO 20022 messaging, payment HSMs, terminals, ATMs, mobile wallets, and real-time payment schemes.

Dedicated payments scope. Payments-specific content has been separated from the Financial Services Extension and substantially expanded. This document covers transaction-processing infrastructure, payment message formats, payment HSMs, POS and ATM fleets, card and wallet ecosystems, tokenization, real-time payment systems, and cross-border payment dependencies.

Payments-sector evidence and coordination. BIS Project Leap Phase 2 provides the first production-grade payment-system PQC experiment. SwiftNet 8.0, PCI DSS 12.3.3, PCI PIN and PTS dependencies, EMVCo and X9 workstreams, and G7/Europol/FS-ISAC coordination are treated as external planning inputs.

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, the domestic schemes, the RTGS operators, EMVCo, PCI SSC, the wallet platforms cardholders use) 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.

Payment HSMs (sector characteristics; Challenge 2; Phase 4; Phase 6; Phase 7): the June 2026 edition named Thales (payShield, including payShield 10K with post-2024 firmware), Utimaco (Atalla; CryptoServer with Quantum Protect), Futurex (CryptoHub) and Entrust (nShield, a general-purpose line) as the product lines under most of the sector, and stated that Utimaco's Quantum Protect firmware supports ML-DSA and LMS and that Thales payShield offers PQC-enabled firmware. Verified September 2026 for the general-purpose line only: 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 CryptoHub) carry their own PQC firmware and PCI PTS HSM certification timelines, unverified at this edition; each is read per product from the CMVP validated-modules list and the PCI Approved PTS Devices list, never from a product name, and PCI PTS HSM v5.0 (May 18, 2026) is the current major version, with the v4 Security Requirements open for new device security approvals until June 30, 2027 under PCI SSC's bulletin of March 2, 2026.

Discovery capability reachable through the HSM vendor (Challenge 2): the June 2026 edition named the Utimaco partnership with Keyfactor (which acquired InfoSec Global and CipherInsights), whose AgileSec Analytics platform integrates with Utimaco u.trust HSMs. Dedicated cryptographic discovery platforms are listed in the Universal's Tool and Vendor References and analyzed on PostQuantum.com.

Card and terminal vendors (Challenge 3; Phase 7): the June 2026 edition named IDEMIA, Thales and G+D as card manufacturers and Ingenico/Worldline, Verifone and PAX Technology as terminal manufacturers. 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, the second agility question first, and graded for firmness.

Smart card silicon (Challenge 3; Phase 4): the June 2026 edition named IDEMIA with GlobalFoundries (28 nm chips on the GF 28ESF3 platform, targeted for 2026 mass production) and Infineon SLC38 and equivalent next-generation secure microcontrollers. Grade: announced; status re-checked at each release.

Payment processors and gateways (Phase 7 vendor classification): the June 2026 edition named Fiserv, FIS, Global Payments, Adyen, Stripe, Worldpay and ACI Worldwide as examples of the class. The list is illustrative of the class, not an assessment of any provider's PQC readiness, which is established through the questionnaire and both halves of the roadmap disclosure for hosted services (Activity 7.7).

Mobile platforms and wallets (Challenge 9; Phase 7): the June 2026 edition named Qualcomm, Samsung and Apple as the handset and secure-element chipset vendors on whose PQC support wallet credential storage depends, and Apple Pay, Google Pay, Samsung Pay and PayPal as the wallet platforms cardholders use. The platforms are counterparties; the chipset vendors' PQC support arrives on their schedules and is graded from their public statements.

Validated modules (alignment section; Challenge 2): 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; whether a payment HSM firmware carries the PQC operation in approved mode under both its FIPS 140-3 and its PCI PTS HSM certificate is checked one product at a time. Consult the CMVP validated-modules and Modules in Process lists and the PCI Approved PTS Devices list 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 PAYMENTS REQUIRES ITS OWN EXTENSION

The Financial Services Extension addresses challenges common to banking, capital markets and insurance, and the Universal's Payments note (Sector Adaptation Notes) states the five constraints that make payments the specialization of that sector: cardholder data and credentials that keep their value to an attacker for the life of the card, scheme requirements that arrive as market-access gates, payment HSMs certified twice, terminal fleets as the estate's long tail, and HSM vendor concentration.

This extension expands those five points and contradicts none of them. Payments concentrates several financial-services challenges to an extreme degree and introduces constraints that have no parallel elsewhere in financial services. 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 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 authorization decision runs on a latency budget set per scheme and per kernel test requirement, which an organization reads for its own deployment. The infrastructure executing that decision includes hardware that may remain in service for 15 years. And no single entity controls more than a fraction of the chain.

This section identifies the characteristics that make payment infrastructure a distinct PQC migration domain.

Cryptographic Density at Transaction Scale

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 unit is unique cryptographic functions, which is neither a count of static references nor a count of runtime invocations. The chain those functions cross spans the cardholder's device, the merchant terminal, the acquirer, the card network, the issuing bank, one or more payment processors, SWIFT's messaging layer, correspondent banks, and the central bank RTGS system.

Each of those functions is a quantum-vulnerable dependency, and different organizations own different segments of the chain, each on its own upgrade cycle. The cryptographic inventory challenge (Phase 1) for a payments organization dwarfs what a typical enterprise faces.

Multi-Party Coordination Without Central Authority

Payment chains lack a single coordinating authority for cryptographic upgrades. A domestic card payment involves at minimum the cardholder, the merchant, the acquirer, the card network, and the issuer. A cross-border payment adds correspondent banks, messaging networks, clearing houses, and central bank settlement systems. Each participant operates independently, with its own vendors, certification timelines, risk appetites and regulatory jurisdictions.

Migrating one node to PQC protects the links and services that node controls, but the end-to-end payment chain remains quantum-vulnerable as long as counterparties and shared trust infrastructure stay classical. A single unmigrated participant exposes the entire path. This N-party synchronization problem has no equivalent in sectors where organizations control their own cryptographic estate.

Hardware Fleet with Decade-Long Replacement Cycles

Payment infrastructure runs on purpose-built, heavily certified hardware. Almost 20 billion payment cards are in circulation, most running 32-bit processors with 48 KB of RAM. Millions of POS terminals and ATMs are deployed globally, with typical replacement cycles of 7 to 15 years. Payment HSMs are subject to dual certification requirements (FIPS 140-3 and PCI PTS) with validation processes measured in years, not months. This hardware takes new cryptographic capability through a software path only where the existing silicon already runs the algorithm, which is how Ecos adds protection on the transaction channel (Challenge 3).

A card cannot: its chip generation and RAM fix what it can compute. A terminal or ATM generation cannot where it lacks the processing headroom for a post-quantum algorithm or a remote update channel to receive one. A payment HSM takes PQC firmware only where its generation supports it and only through the re-certification of

Challenge 2. It must be physically manufactured, distributed, certified, and installed, creating migration timelines that are constrained by logistics and certification bureaucracy.

Real-Time Performance with Zero Tolerance for Degradation

Payment authorization decisions operate within strict latency budgets, set per scheme and per kernel test requirement, which an organization reads for its own deployment. RTGS systems settle transactions worth many multiples of GDP per year under tight throughput guarantees (BIS, Project Leap Phase 2 report, December 2025). That report measured software-based verification of a post-quantum signature on the T2 test environment at 209.9 milliseconds on average against 28.1 milliseconds for the RSA signature it replaced, a 7.5× slowdown on the one step the experiment timed.

That overhead, applied to a system handling thousands of transactions per second at peak, creates capacity planning challenges specific to payment processing and absent from most other enterprise PQC migration contexts.

Message Format Constraints That Predate the Internet

ISO 8583, the binary format underpinning global card payment authorization, was designed when every byte was expensive. Its variable-length fields carry at most 999 bytes in the base standard, and the implementation specifications of the schemes and switches narrow them further (Field 55, the ICC system-related data, is commonly limited to 255 bytes of EMV data). An ML-DSA-44 signature is 2,420 bytes (FIPS 204). It 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 problem extends beyond the wire format to every switch, gateway, parser, logging system, database schema, and archive built around current field size assumptions.

What BIS Project Leap Phase 2 Showed on T2

On December 11, 2025 the BIS Innovation Hub Eurosystem Centre, Banca d'Italia, Banque de France, Deutsche Bundesbank, Nexi-Colt and Swift published the report of Project Leap Phase 2 (bis.org/publ/othp107), the first post-quantum experiment run on an operational payment system's test environment. The experiment ran on inbound application-to-application liquidity transfers (camt.050) in the Eurosystem's T2 test environment.

It replaced the RSA signature in the ISO 20022 Business Application Header with a CRYSTALS-Dilithium category 3 signature, the NIST Round 3 predecessor of ML-DSA-65;

ML-DSA itself could not be tested in the project's time frame. Every test scenario passed: correctly signed transfers were accepted and a transfer signed with the wrong key was rejected with the standard error message, and participants using different cryptographic libraries interoperated.

The report's findings set the sector's planning assumptions. RSA verification averaged 28.1 milliseconds in the same test. Verification of the post-quantum signature averaged 209.9 milliseconds, a 7.5× slowdown on the one step the experiment timed. The RSA signature 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 signature could not be carried by configuration: the network service providers shipped updated modules, the central banks reconfigured their connectors, and a new verification component was built because the existing verification software accepts one signature algorithm at the header level. That single-algorithm limit is also why a hybrid signature at that level could not be tested. Settlement did not complete because no certificate for the test key existed in T2's common reference data. 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 experiment used software key files rather than an HSM and raw key pairs rather than certificates, so certificate validity and trust-chain validation are untested and the client-side signing cost is unmeasured. The report's own conclusion is that hybridization was not envisaged in T2's original cryptographic design and that payment systems will need to be made more agile before or as part of the migration. The June 2026 edition of this extension described the missing certificate as a failure resolved by hand and the message-size finding as a buffer overrun. Both statements are corrected here to the report's text.

Payment Structural Advantages for PQC Migration

Despite severe migration challenges, payment infrastructure possesses structural advantages that organizations should recognize and use in their program design.

PCI Compliance Infrastructure as CBOM Accelerator

PCI DSS v4.0 Requirement 12.3.3 (required after March 31, 2025) already mandates that PCI-scoped entities document all cryptographic cipher suites and protocols in use, with annual review. Most payment organizations are PCI-scoped across a broad swath of their infrastructure. The CBOM construction effort can be structured to satisfy PCI 12.3.3 as a standard output, producing both PQC readiness assessment and PCI compliance evidence from the same data collection. This dual-use approach produces both PCI 12.3.3 evidence and a PQC readiness assessment from a single data collection effort, justifying the investment against compliance obligations already in force.

ISO 20022 Migration as a Parallel Modernization Window

The global migration from SWIFT MT messages to ISO 20022 MX format continues: SWIFT's MT/MX coexistence period for cross-border payments ran to November 2025, and domestic market infrastructures adopt ISO 20022 on their own timelines. This concurrent infrastructure modernization creates an opportunity: organizations redesigning message-handling systems for ISO 20022 can incorporate PQC payload accommodation into the same engineering effort, rather than retrofitting it later. Where ISO 20022 migration budgets and teams are already funded, PQC requirements can be integrated at marginal additional cost.

Concentrated HSM Vendor Market

Most of the sector runs on a small number of payment HSM product lines, and most organizations in it use one or two of them (the names as the June 2026 edition listed them are in Tool and Vendor References). This concentration simplifies Phase 7 vendor governance: fewer vendor relationships to manage, fewer PQC roadmaps to track, and more weight in negotiations on certification timelines. The same small number of product lines also narrows the dependency: whether two acquirers' alternatives share one firmware family is a Cryptographic Concentration Framework question, cross-referenced from the Phase 6 register and never answered here.

Existing Key Management Teams and Cryptographic Expertise

Payment organizations maintain dedicated key management functions within their security operations. These teams manage HSM estates and perform key ceremonies. They handle PIN translation key hierarchies and certificate lifecycles. Their institutional knowledge of the cryptographic estate shortens Phase 1 discovery: they know where the HSMs are, what applications use them, which key ceremonies are performed annually, and which DUKPT key hierarchies serve which terminal populations. Most organizations outside financial services begin Phase 1 without this existing institutional knowledge.

Change Management Discipline

Payment organizations run formal change advisory boards with change freezes around month-end, quarter-end, and peak transaction periods (Black Friday, holiday seasons, fiscal year-end). PQC pilots fit naturally into this structure. The rollback requirements in Phase 5 align with existing change management practices: payment organizations already maintain rollback procedures, test in staging environments that mirror production, and schedule deployments in controlled maintenance windows.

PAYMENT-SPECIFIC CHALLENGES

This section details the technical and operational challenges specific to payment infrastructure PQC migration. Each challenge is presented with its technical basis, real-world evidence where available, and the Universal Framework phases it most directly impacts. The subsequent section maps these challenges to specific framework adaptations.

Challenge 1: The Signature Size Problem

PQC algorithms produce signatures and public keys that are orders of magnitude larger than their classical equivalents. This mismatch is a structural incompatibility with payment message formats engineered for minimal payload sizes.

Field Limits in ISO 8583

ISO 8583 is the binary format underpinning global card payment authorization. Its variable-length fields carry at most 999 bytes in the base standard, and scheme and switch implementation specifications narrow them: Field 55 (ICC system-related data) is commonly limited to 255 bytes of EMV data, and the authentication data fields are smaller. An ML-DSA-44 signature is 2,420 bytes, 37.8× the 64-byte ECDSA P-256 signature in the profiles that carry a per-message asymmetric signature; many ISO 8583 profiles carry no such signature and authenticate the message with a symmetric MAC, which is not a Shor target, so the comparison applies to the profiles and fields that do carry one, which the Phase 1 message format analysis identifies.

An ML-DSA-65 signature is 3,309 bytes per FIPS 204 (3,293 bytes in the pre-standard Dilithium variant Project Leap tested). Neither fits in any ISO 8583 field; carrying one requires a format revision or a split across fields that every party on the path parses the same way.

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 field-by-field engineering of accommodating larger payloads across thousands of institutions has not started.

Payload Accommodation in ISO 20022

ISO 20022's XML/JSON-based structure is more extensible than ISO 8583, and the industry migration from MT to MX messages continues. Extensibility does not mean zero-effort accommodation. BIS Project Leap Phase 2 replaced the 256-byte RSA signature in the ISO 20022 Business Application Header with a 3,293-byte Dilithium category 3 signature, a 12.9× increase in the signature field. The change reached production-grade code only through updated network service provider modules, reconfigured connectors and a new verification component, because the header-level software accepts one signature algorithm. Storage and archival systems that retain message copies for regulatory compliance face multiplicative increases in data volume.

Archive and Storage Multiplication

Payment message archives are among the largest data stores in financial institutions. Regulatory retention requirements (typically 5 to 10 years) mean that the signature size increase compounds across every stored message. A system archiving 10 million messages daily with an average PQC signature overhead of 3 KB per message adds approximately 30 GB of additional storage per day, or roughly 11 TB per year, for signature data alone. Certificate chains add further overhead. Organizations must model this storage impact during Phase 6 capacity planning.

Framework Impact: Phase 1 (Discovery) must include message format analysis as a distinct inventory track, identifying every fixed-size field carrying cryptographic data. Phase 3 (Risk Scoring) must weight message-format-constrained systems separately. Phase 5 (Pilots) must include message-format-specific testing with realistic payload sizes. Phase 6 (Infrastructure) must model archive storage growth.

Challenge 2: Payment HSM Certification Bottleneck

Hardware Security Modules are the root of trust for every payment cryptographic operation: PIN translation, MAC generation and verification, key injection, card personalization, and transaction signing. Payment HSMs are subject to dual certification requirements that create a compounding bottleneck for PQC adoption.

The Double Certification Problem

Payment HSMs must satisfy two independent certification regimes. FIPS 140-3 Level 3 (or higher) validates the cryptographic module's security properties, and SWIFT's Customer Security Programme sets its own HSM validation requirement for network participants (the June 2026 edition recorded FIPS 140-2 Level 2 or higher. The current control text is re-checked at each release, because the CMVP moved every remaining FIPS 140-2 certificate to the Historical list on September 21, 2026).

PCI PTS HSM validates the module's suitability for payment-specific operations (PIN handling, key management). On May 18, 2026 PCI SSC published PCI PTS HSM v5.0, a major revision of the Modular Security Requirements. It adds post-quantum cryptography considerations and definitions, requires device-security keys of at least 128-bit effective strength with TDES no longer permitted for that purpose, and prohibits weak firmware-authentication methods.

New evaluation modules cover key-transfer functionality, remote administration and HSM-as-a-service deployments. What v5.0 asks of a PQC firmware is read from the requirements document and is not summarized here. The transition is longer than the publication date suggests. Under the Council's standing twelve-month minimum overlap between major versions of the PTS Security Requirements, PCI SSC's bulletin of March 2, 2026 keeps the v4 Security Requirements open for new device security approvals until June 30, 2027.

The same bulletin moves the v4 device approval expiration date from April 2032 to April 2033 and the v3 device approval expiration date from April 2026 to April 2028. A payment HSM estate can therefore hold v3, v4 and v5.0 approvals concurrently well past this edition, and the Phase 6 register records the version of the standard each approval was granted under. Validation of the PQC operation 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, with the qualifications the alignment section's validation subsection states) both exist; payment HSMs, which also need a PCI PTS HSM approval, follow one product at a time.

Organizations track validation status at the specific product, firmware version and certificate number, for FIPS 140-3 and for PCI PTS HSM separately, rather than relying on vendor marketing claims of PQC support.

HSM vendors ship firmware with PQC support (the product lines and firmware families the June 2026 edition named are in Tool and Vendor References). Running a PQC operation as a service that is not approved under the module's validation is a risk decision for the FIPS-aware class and a recorded dependency for the FIPS-required class. Such a service may still execute inside the module's cryptographic boundary in a non-approved mode.

The Phase 6 register records approved-service status and boundary placement as two separate facts. A PQC firmware that breaks the PCI PTS HSM certification is not deployable on a payment HSM until re-certified. The June 2026 edition expected the first validated PQC module in mid-2027 at the earliest. That expectation was wrong

when published (CMVP certificate #5247, April 2026; CMVP certificate #5497, August 2026), and the calendar is replaced by the per-product rule above.

For each FIPS-required or PCI-scoped deployment, the Phase 6 register records the governing requirement, the module and firmware family, both certificate references and their status, and the approved services each certificate lists. Where no certificate covers the operation, the register also records the interim controls, the exception authority and the next decision date. The dependency constrains that system and sets no date for the program.

Payment HSM Vendor Concentration

The payment HSM market is concentrated among a small number of product lines (Tool and Vendor References). This concentration simplifies vendor governance and narrows the migration risk surface: a certification delay on one firmware family affects a significant fraction of the global payment infrastructure, and two products procured under two names can share one family. The Phase 6 register records the visible platform, the firmware family, the manufacturer of origin and both certificate references separately so the sharing is visible; how many distinct implementations execute beneath the sector's payment HSMs is a Cryptographic Concentration Framework question, cross-referenced and not computed here.

Some HSM vendors offer discovery capability through a partner platform that integrates with their HSM estate (the partnership the June 2026 edition named is in Tool and Vendor References). Payment organizations should ask their current HSM vendor what discovery capability the existing relationship already provides before procuring standalone tooling (Phase 1), and grade what it finds with the evidence tiers of Activity 1.2 like any other source.

Framework Impact: Phase 6 (Infrastructure) must include HSM certification tracking as a gating dependency, with FIPS 140-3 and PCI PTS HSM recorded as two certificate references per module in the Activity 6.2 register. Phase 7 (Vendor Governance) must establish structured quarterly engagement with HSM vendors on certification timelines and early access to PQC firmware for lab testing, with the two agility questions asked first and every date graded for firmness.

Challenge 3: Terminal and Card Fleet Migration

The payment card and terminal fleet represents the most physically distributed PQC migration challenge in any sector. The Universal's Payments note treats terminal fleets as the long tail of the payments estate, the way OT is treated: multi-year lifecycles, in-field key-injection and remote-update constraints, and vendor-controlled cryptography. This challenge applies that reading.

Card Hardware Constraints

Almost 20 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. 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, exceeding 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.

Command and response limits are separate facts. A short APDU carries up to 255 bytes of command data and returns up to 256 bytes of response data. Extended-length APDUs and command chaining already exist in the relevant smart-card interfaces, subject to support in the card, the transport, the EMV kernel and the scheme profile. A larger PQC object does not by itself establish that a new command is required. Per product, the inventory records four fields: the command-data limit, the response-data limit, extended-length support and chaining support. The finding to carry forward is that PQC may require changes to how objects are transported and parsed, validated against the exact EMV profile in use.

FS-ISAC's payment card guidance explicitly notes that it is not known whether EMV can accommodate quantum-safe certificates. Next-generation 28 nm smart card silicon announced for 2026 mass production (supplier names in Tool and Vendor References; grade: announced) will provide more computational headroom. The card replacement cycle is measured in years: the average card has a 3-to-5-year lifespan, and full fleet turnover takes longer.

Terminal Fleet Scale and the Mastercard Ecos Approach

Millions of POS terminals and ATMs are deployed globally, with replacement cycles of 7 to 15 years. Upgrading terminal firmware for PQC requires not just software development but re-certification under PCI PTS. 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 (which relies on asymmetric signatures on the chip) or EMV certificate chains, so it is read as a transaction-channel measure and not as an answer to the offline-authentication question.

EMVCo's published position, at its own strength: its security position statement on quantum computing and EMV chip cryptography, plus a statement by the chair of its Board of Managers (January 30, 2026) that EMVCo does not expect quantum computing to pose a practical threat to the EMV infrastructure before 2040, maybe never, with industry engagement on post-quantum cryptography planned through 2026. The assessment covers offline data authentication and the chip's own cryptography: EMVCo's reasoning is that online cryptograms are symmetric (AES, in the EMV specifications since 2010) and expire after use, and it concedes that RSA and ECC are used where terminals lack online connectivity. It says nothing about the rest of the card and terminal estate.

No specification change and no date have been published. The June 2026 edition's "EMVCo quantum working group" is not a body EMVCo names in public, and the reference is corrected to the position statement. The firmness grade on every EMV specification date is therefore unknown at this edition. The statement places nothing in a tier: under the ordered test of Activity 3.2, offline data authentication is Dimension 2 Critical, because the scheme CA public keys it depends on are trust anchors relied on across the whole card and terminal estate and the terminal populations that verify it cannot all be updated, so it falls in Tier 1 with the delivery state blocked on the card and terminal refresh cycle (Phase 3). EMVCo's statement concerns chip cryptography and says nothing about the HNDL exposure of the transaction channel, which Track A addresses on the organization's own schedule.

For the terminals and PIN pads that will not support post-quantum cryptography within their remaining service life, the pattern is the one the OT & Critical Infrastructure Extension names "The Encapsulate Strategy". Place the cryptography in front of the population at the layer the organization controls: the acquirer host, the terminal management system, the estate gateway. Record the population as migrated by enclosure, with the gateway as the migrated component.

State what the enclosure does not cover: the offline data authentication on the chip; firmware-signing integrity, which is Track B. Give every enclosed population a bridge end date on the refresh roadmap or a SteerCo-signed exception with a re-evaluation date. The strategy's conditions and record format are in that extension and are not restated here.

Framework Impact: Phase 4 (Roadmap) must incorporate hardware refresh cycles for cards and terminals as hard constraints on migration timelines, with each population's delivery state recorded. Phase 5 must include a triage strategy separating online authentication (protectable with symmetric cryptography now) from offline data authentication (dependent on asymmetric PQC on constrained hardware), with enclosure per the OT extension's Encapsulate Strategy for the populations that will never migrate natively. Phase 1 must inventory the card and terminal estate by chip generation, RAM capacity, PQC feasibility and verifier updatability.

Challenge 4: Settlement Latency and Performance

BIS Project Leap Phase 2 provided the first empirical evidence of PQC performance impact on production-grade settlement infrastructure.

BIS Project Leap Phase 2 Performance Data

Software-based post-quantum signature verification on the T2 test environment averaged 209.9 milliseconds compared to 28.1 milliseconds for RSA, a 7.5× slowdown; verification was the only step the experiment timed, and the client-side signing cost was not measured because no HSM was used. The test used pre-standard CRYSTALS-Dilithium category 3 signatures on ISO 20022 liquidity transfer orders. ML-DSA-65, the standardized successor, has a slightly larger signature (3,309 bytes versus the 3,293 bytes tested), and its performance is comparable. The report itself notes that HSM performance varies by manufacturer and that production figures need benchmarking with every component under post-quantum cryptography.

At peak throughput on a system processing thousands of transactions per second, each carrying an enlarged PQC certificate chain, the aggregate bandwidth and compute overhead is substantial. RTGS systems (T2, Fedwire, BOJ-NET, CHAPS), real-time payment networks (FedNow, TIPS, Faster Payments, UPI), and high-frequency trading venues all operate within tight latency budgets where PQC overhead must be engineered out through hardware acceleration or architectural changes.

Certificate Chain Overhead and Hardware Acceleration

PQC certificate chains compound the signature size problem. A three-level certificate hierarchy with ML-DSA-65 adds approximately 20 KB of overhead per chain validation. Hardware-accelerated PQC (via FPGA or ASIC in next-generation HSMs) will narrow the performance gap, potentially by an order of magnitude. However, hardware-accelerated PQC modules must themselves pass FIPS 140-3 validation and PCI PTS HSM evaluation before production deployment on a payment HSM, so the certification dependency of Challenge 2 sits on the performance optimization path as well.

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

Challenge 5: SWIFT Dependencies and Cross-Border Coordination

SWIFT is the backbone of cross-border payment messaging, connecting over 11,000 institutions in more than 200 countries. SWIFT's PQC migration timeline directly constrains every organization connected to the SWIFT network. This challenge section provides the detailed SWIFT dependency analysis that payment organizations need for planning.

SWIFT Customer Security Programme and PQC

SWIFT's Customer Security Programme (CSP) establishes mandatory and advisory security controls for all SWIFT-connected institutions. The CSP's mandatory controls include requirements for securing the local SWIFT infrastructure (operator workstations, Alliance Gateway/Lite2 software, HSMs used for message signing), managing credentials, and hardening the operating environment. As SWIFT transitions to PQC, these mandatory controls will likely be updated to include PQC requirements for message authentication and channel encryption. Organizations should monitor CSP updates for PQC-specific control additions and assess their current CSP architecture for PQC readiness.

SWIFT Alliance Architecture and PQC Readiness

SWIFT-connected institutions typically operate SWIFT Alliance Gateway (for larger institutions) or Alliance Lite2 (for smaller institutions). Both products handle message encryption, signing, and PKI certificate management. PQC migration for SWIFT connectivity requires updates at multiple layers: the Alliance software itself (SWIFT's responsibility to update), the HSMs used for message signing (the institution's responsibility, subject to HSM vendor certification timelines), the PKI certificates used for authentication (requiring coordinated certificate rotation with SWIFT's CA hierarchy), and the network connectivity layer (TLS for IP-based SWIFT access).

Organizations should inventory their SWIFT Alliance deployment model and identify the HSMs used for SWIFT message signing. They should also verify the firmware's PQC capability and assess the certificate management process for PQC certificate handling. For institutions using Alliance Gateway in a high-availability configuration, the PQC migration must be coordinated across primary and backup sites.

SwiftNet 8.0 Migration Planning

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 and must be deployed by the majority of the community, because there is no upgrade path from release 7.7 to 8.0.

Alliance Release 7.9 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. Grade: announced (a public roadmap statement); what PQC use release 8.0 will require of participants, and on what date, is not stated publicly and is graded unknown. Four dates are tracked separately. Only the last of them scores the Dimension 4 deadline factor: the availability date of Alliance Release 8.0 (end July 2027, announced); the prerequisite deployment of Release 7.9; the end of support for 7.9, 15 months after

release 8.0 ships; and the date on which Swift requires participants to use PQC, which is unknown.

A mandatory software release and a PQC activation requirement are distinct obligations, and the availability date is not evidence of the second. Planning follows from what is known: the 7.9 deployment is the prerequisite for every institution still on 7.7. The institution's SWIFT-facing HSMs must generate and use PQC keys within the validated boundary by the time release 8.0 requires them, on the certificate date of the module that covers them; and the message-handling systems must process PQC-signed ISO 20022 messages with enlarged signature payloads.

Organizations register for Swift's PQC pilot and sandbox programs as they open. They run readiness assessments against the release 8.0 requirements as Swift publishes them. Each SWIFT-dependent Tier-1 entry carries the delivery state dependent against these dates with their grades.

SWIFT PKI and Certificate Management

SWIFT operates its own PKI hierarchy for message authentication. Member institutions receive certificates from SWIFT's CA and use them for message signing and mutual TLS authentication. The transition from classical to PQC certificates in SWIFT's PKI requires coordinated action: SWIFT must update its root and intermediate CA certificates to PQC, member institutions must deploy the new PQC certificates on their Alliance infrastructure, and message verification logic must be updated to handle PQC signatures.

BIS Project Leap Phase 2 showed the dependency in its plainest form: a correctly PQC-signed transfer passed signature verification and did not settle because no certificate for the test key existed in T2's common reference data, an outcome the report records as expected and as confirmation that settlement relies on centralized certificate data under post-quantum signatures as well. Certificate provisioning at every counterparty must therefore be sequenced before – not after – production deployment of the PQC signature.

The Correspondent Banking Chain

Beyond SWIFT, cross-border payments traverse the originating bank, its correspondent bank, the receiving correspondent bank, and the beneficiary bank, with one or more central bank RTGS systems for settlement. Each entity operates independent cryptographic implementations with independent PKI hierarchies. Card networks (Visa, Mastercard) operate their own CAs and will set independent PQC migration timelines. No dated public roadmap for either scheme's CA migration was found when checked for this edition, so both dates are graded unknown as of September 2026.

Domestic payment schemes (ACH, SEPA, Faster Payments, BACS, UPI, PIX) operate under national governance with their own adoption timelines. No coordination

mechanism exists to synchronize PQC migration across all of these independent entities. The counterparty pattern of Activity 7.6 is the general case of the coordination this challenge specifies, and where the two overlap this extension governs.

Framework Impact: Phase 0 (Executive Mandate) must establish cross-industry coordination mechanisms from the outset. Phase 4 (Roadmap) must map SWIFT, card network, domestic scheme, and central bank timelines as hard constraints, each graded for firmness, with the delivery state of every dependent entry read from them. Phase 7 must include strategic-level engagement with SWIFT on the release 8.0 requirements and timeline through the counterparty pattern.

Challenge 6: PCI Standards and Payment Security Requirements

The PCI Security Standards Council (PCI SSC) maintains several standards that intersect with PQC migration. PCI SSC had published no standalone PQC guidance when checked for this edition (September 2026); PCI PTS HSM v5.0 (May 18, 2026) is the first PCI standard to include post-quantum considerations in its text, and multiple PCI standards create both compliance drivers and migration constraints for payment organizations. PCI requirements and card-scheme rules reach a merchant, an acquirer or a processor as market-access gates: an organization that fails them loses the ability to process the scheme's transactions.

The Universal's Regulatory & Standards Alignment Map places such requirements at enforcement tier 1, and Phase 3 Dimension 4 scores them as mandatory when they carry a date, whatever their legal form.

PCI DSS v4.0 and Cryptographic Documentation

PCI DSS v4.0 Requirement 12.3.3 (required after March 31, 2025) mandates that PCI-scoped entities document all cryptographic cipher suites and protocols in use, with annual review. This requirement already creates a compliance driver for Phase 1 (Discovery) and Phase 2 (CBOM), because a thorough PCI 12.3.3 assessment will surface the quantum-vulnerable algorithms in use. Organizations should structure their cryptographic inventory to satisfy both PCI 12.3.3 and PQC readiness assessment simultaneously.

Requirement 3.5.1 requires that a stored Primary Account Number (PAN) is rendered unreadable by one of four methods: a one-way hash of the entire PAN based on strong cryptography (a keyed cryptographic hash for hashes generated after March 31, 2025, under 3.5.1.1), truncation where the hash cannot substitute for the truncated segment, index tokens, or strong cryptography with associated key-management processes and procedures. It does not mandate encryption of all stored PAN.

Of the four, only the encryption method carries a quantum-vulnerable dependency, and only where the key management around it uses RSA or ECC for key transport, wrapping or distribution. A keyed hash, a truncation or an index token is not a Shor target. As

quantum computing advances, the definition of "strong cryptography" will evolve. Organizations should anticipate that PCI SSC will eventually update its cryptographic guidance to reflect PQC requirements, and prepare accordingly.

The confidentiality horizon that Phase 3 Dimension 1 scores for cardholder data is the attacker's horizon: account numbers and track data keep their value to an attacker for the life of the card and beyond, so a captured authorization or clearing flow is worth decrypting years later. That is a statement about the attacker, not a license to retain the data. PCI DSS prohibits storing sensitive authentication data after authorization, and the framework's Activity 5.6 decision applies to what the organization is permitted to hold.

PCI PIN Security and DUKPT Key Hierarchy

PCI PIN Security requirements govern the handling of cardholder PINs, including PIN block encryption, PIN translation between encryption zones, and the key management hierarchies that protect PIN data in transit. The Derived Unique Key Per Transaction (DUKPT) key management scheme, widely used for PIN encryption at the point of sale, derives per-transaction keys from an initial key loaded during terminal manufacturing. DUKPT uses TDEA (Triple DES) or AES as its underlying cipher.

While AES-based DUKPT is quantum-resistant (symmetric cryptography is not vulnerable to Shor's algorithm), many terminal populations still use TDEA-based DUKPT, which faces deprecation under PCI PIN Security requirements regardless of quantum considerations. Organizations must track the intersection of PCI's TDEA deprecation timeline with their PQC migration timeline, as both require key hierarchy updates at the terminal and HSM layers.

PCI 3-D Secure and E-Commerce Authentication

3-D Secure (3DS) is the protocol used for cardholder authentication in e-commerce transactions (Visa Secure, Mastercard Identity Check, AmEx SafeKey). 3DS 2.0+ uses digital signatures and TLS for communication between the merchant, the card network's directory server, and the issuer's access control server. The cryptographic dependencies span multiple organizations: the card network operates the directory server, the issuer operates the ACS, and the merchant's payment service provider integrates the client-side SDK.

PQC migration for 3DS requires coordinated action across all three parties, following the same N-party synchronization pattern as other payment channel migrations. Organizations should inventory their 3DS infrastructure during Phase 1 and include it in Phase 7 vendor governance.

PCI Point-to-Point Encryption (P2PE)

PCI P2PE solutions encrypt cardholder data at the point of interaction (the terminal) and decrypt it only in a secure decryption environment (the HSM), eliminating exposure of

cleartext cardholder data throughout the payment chain. P2PE implementations use asymmetric cryptography for key distribution and symmetric cryptography for bulk data encryption. The asymmetric key distribution layer is quantum-vulnerable. Organizations operating validated P2PE solutions should assess whether the key distribution mechanism uses RSA or ECC (quantum-vulnerable) or AES key wrapping (quantum-resistant), and plan accordingly.

Framework Impact: Phase 1 (Discovery) must include PCI-scoped systems as a priority inventory track, structured to satisfy both PCI 12.3.3 and PQC readiness. Phase 3 (Risk Scoring) must score PCI and scheme requirements at enforcement tier 1 on Dimension 4 and the attacker's horizon on Dimension 1. Phase 7 (Vendor Governance) must include 3DS network providers and P2PE solution providers in vendor PQC readiness assessment.

Challenge 7: Real-Time Payment Systems

Real-time payment (RTP) systems have proliferated globally over the past decade: FedNow (United States, launched 2023), TIPS (Euro area), Faster Payments (UK), UPI (India, which processed 22.64 billion transactions in March 2026 alone), PIX (Brazil), and dozens of others. These systems operate 24/7/365 with confirmation to payer and payee in seconds and, in some of them, settlement finality in seconds, creating specific PQC migration constraints.

Continuous Availability and Migration Windows

Unlike batch-settlement systems that have overnight processing windows, RTP systems run continuously. Traditional migration approaches that rely on scheduled downtime are not available. PQC migration for RTP must be executed through rolling upgrades with hybrid cryptography, maintaining backward compatibility throughout the transition. Any performance degradation from PQC overhead is felt immediately and continuously, not just during batch processing windows.

Latency Sensitivity at Scale

RTP systems impose end-to-end processing time limits that are tighter than RTGS systems. UPI processed 22.64 billion transactions in March 2026 with sub-second confirmation of the customer payment. Behind those confirmations, the interbank movement of funds runs on deferred net settlement: NPCI computes each member's net position and settles through accounts at the Reserve Bank of India in several cycles a day. The budget that PQC overhead has to fit on UPI is the authorization and confirmation path.

The settlement path is a batch process with a different performance profile. FedNow targets settlement in under 5 seconds. The PQC performance overhead observed in Project Leap Phase 2 (7.5× for software-based signature verification, the only step timed) would need to be reduced significantly through hardware acceleration before

production deployment on high-volume RTP systems. Organizations participating in RTP schemes should benchmark PQC performance against their specific scheme's latency requirements.

Framework Impact: Phase 5 (Pilots) should include RTP interface testing with PQC to measure real-world latency impact. Phase 6 (Infrastructure) must include RTP-specific hardware acceleration planning.

Challenge 8: Tokenization as Interim Quantum Defense

Payment infrastructure makes extensive use of tokenization, providing a structural advantage for quantum resilience that most other sectors lack.

Why Tokenization Reduces Quantum Exposure

Tokenization replaces 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. A vault token is a surrogate whose mapping to the original is held in a store the tokenization system controls. A format-preserving encryption token (below) is a ciphertext under a symmetric key and is reversible with that key.

Neither is irreversible in the sense a hash is. The protection depends on the symmetric cryptography and on the access controls around the vault or the key. AES symmetric cryptography is not vulnerable to Shor's algorithm (Grover's algorithm provides only a quadratic speedup, addressed by using AES-256). Tokenized data harvested for future quantum decryption yields token values that are useless without the vault or the key, which are the components that remain in scope.

However, the token vault, detokenization APIs, key-management layer, logs, and any systems that still process cleartext data remain in scope for PQC migration. Tokenization reduces exposure and narrows the migration scope. It does not eliminate the need to migrate the key-management layer, the detokenization APIs and the token vault's own cryptographic controls. Card issuers, payment processors, and acquirers that have deployed tokenization broadly should quantify what percentage of their sensitive payment data is already quantum-defended. This assessment reduces Phase 3 scope by identifying data categories that already have quantum-resistant protection.

Format-Preserving Encryption Caveat

Some tokenization implementations use format-preserving encryption (FPE) rather than true tokenization with a vault. FPE (typically based on FF1 or FF3-1, using AES as a building block) preserves the format of the original data. While AES itself is quantum-resistant, the security properties of FPE schemes under quantum attack are less well-studied than AES in standard modes. Organizations using FPE should assess whether

their specific implementation retains adequate security margins under quantum threat models.

Framework Impact: Phase 3 (Risk Scoring) should incorporate tokenization coverage as a risk-reducing factor. Phase 5 should include a tokenization coverage assessment as an early action.

Challenge 9: Mobile and Digital Wallet Cryptography

Mobile payments and digital wallets introduce a distinct cryptographic surface. Mobile payment apps implement multiple layers of cryptography: TLS for API communication, certificate pinning for MITM prevention, local data encryption using the device keystore or secure element, biometric template protection, and application-level token generation. The TLS layer benefits from browser and OS-level PQC adoption. Cryptography inside the application depends on the app developer's own migration.

Secure Element (SE) and Trusted Execution Environment (TEE) hardware used for payment credential storage faces similar constraints to payment cards: limited memory, limited processing power, and dependency on the handset and secure-element chipset vendors, whose PQC support arrives on their schedules (the vendors the June 2026 edition named are in Tool and Vendor References). Certificate pinning configurations in mobile payment apps require updates when server certificates transition to PQC, creating a coordination requirement between server-side PQC deployment and client app updates.

Payment authentication itself is moving onto this surface: payment passkeys (FIDO credentials used in 3DS flows and Click to Pay) are replacing OTPs at scale, and each enrolled passkey is a long-lived classical credential, typically ES256 on P-256 or RS256. The Phase 1 inventory records the algorithm actually enrolled for each credential population rather than assuming one (Universal, Track B identity stack). The Universal Framework places the identity stack explicitly in Track B. The Alignment section of this extension maps the payment-specific implications, including the credential re-enrollment question for ACS and wallet vendors.

Phase 3 scores the relying party's verification implementation on verifier updatability and records the re-enrollment of the enrolled credential population as a separate control-posture constraint.

Framework Impact: Phase 1 must include mobile payment app cryptographic dependencies as a distinct inventory track. Phase 5 must coordinate server-side PQC deployment with mobile app update cycles. Phase 7 must include mobile platform vendors as dependencies for SE/TEE PQC support.

Challenge 10: ATM Network Security and Remote Key Loading

ATMs represent a distinct PQC challenge within the terminal estate. ATM networks use asymmetric cryptography for remote key loading (RKL), host-to-ATM communication authentication, and software update verification. TR-34, the certificate-based asymmetric remote key loading protocol, establishes the key by asymmetric key transport and authenticates the parties with certificates and digital signatures. Both operations use classical public-key cryptography and both are Shor targets, and they are inventoried as two functions because they fail differently (a broken transport key exposes the loaded key material; a forged signature loads an attacker's key) and migrate on different tracks.

TR-31 is a symmetric key-block format for protecting keys in storage and transport, succeeded by ANSI X9.143. It is not an asymmetric protocol and should be inventoried separately under symmetric key management, where the AES or TDEA wrapping it uses is not a Shor target. The installed ATM base has a typical replacement cycle of 10 to 15 years, and many ATMs run on hardware platforms that cannot support PQC key sizes or computational requirements.

Organizations should inventory their ATM fleet by model, processor capability, and RKL protocol version during Phase 1. ATMs capable of firmware-based PQC updates should be identified and prioritized. For ATMs that cannot support PQC, the fallback strategy may include physical key injection (reverting from remote to manual key loading), accelerated hardware replacement, or enclosure behind the host under the OT extension's Encapsulate Strategy with the exclusions stated. Each ATM population's entry records who can change its cryptography (the vendor's firmware, the operator's configuration, an integrator-held key) and carries its agility-debt state to closure.

Framework Impact: Phase 1 (Discovery) must include ATM network cryptographic dependencies and RKL protocol versions. Phase 4 (Roadmap) must incorporate ATM replacement cycles as hardware constraints.

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 payment organizations the version changes the method, the records and the vendor governance, and corrects 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), one of the three the Universal names or, for the payment HSM estate, a key ceremony that generates a PQC-authorized key and retires it. The quarterly failover to the backup HSM partition exercises state management, failover and the SP 800-208 state design. It changes no algorithm. It is recorded and reported as a failover exercise whose timings do not feed the rehearsed time-to-change KPI.

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, and in payments the terminal fleet and the scheme-set interfaces fill most of it.

- **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 HSM and KMS register has four fields (visible platform, firmware family, manufacturer of origin, certificate reference), and for a payment HSM the certificate reference is two references, FIPS 140-3 and PCI PTS HSM (Activity 6.2).

The Cryptographic Concentration Framework is cross-referenced where the question is how many distinct firmware families execute beneath the sector's payment HSMs (Phase 7), 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 go to every issuer, the scheme and SWIFT CAs included; 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 payments the schemes, SWIFT, the central banks and the RTGS operators are counterparties under Activity 7.6, and their dates set the delivery state of every entry that waits on them.
- **Corrections made in the open.**

On validated modules. 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 (April 2026) covers ML-KEM at ML-KEM-768 and ML-KEM-1024 in a Level 1 software module. CMVP certificate #5497 (August 2026) covers ML-KEM, ML-DSA, SLH-DSA and LMS inside the approved boundary of a Level 3 hardware module. Each comes with the qualifications the validation subsection states. Validation is decided per product, per operation and per certificate (Deployment Environment Classification).

On Project Leap Phase 2. The June 2026 account described the missing certificate as a failure resolved by hand, and the message-size finding as a buffer overrun. Both are corrected to the report's text (sector characteristics).

On EMVCo and Swift. The June 2026 "EMVCo quantum working group" is corrected to EMVCo's published position statement, and the SwiftNet 8.0 and Alliance Release 8.0 dates are restated from Swift's own pages (Challenges 3 and 5).

On PCI PTS HSM. Version 5.0 (May 18, 2026) replaces the June 2026 edition's v4 references throughout. The v4 transition is stated from PCI SSC's bulletin of March 2, 2026: the v4 Security Requirements open for new device security approvals until June 30, 2027, and the v4 and v3 device approval expiration dates extended to April 2033 and April 2028 (Challenge 2).

Three further positions from the June 2026 edition are corrected here.

On card hardware, the June 2026 edition said that "EMV commands' 256-byte data transfer limits require new extended commands for PQC certificate and signature exchange."

Short APDUs distinguish up to 255 command-data bytes from up to 256 response-data bytes. Extended length and command chaining already exist in the relevant smart-card interfaces, subject to card, transport, EMV kernel and scheme-profile support. A larger PQC object does not by itself establish that a new command is required, and ISO/IEC 7816-4 defines both the length fields and the chaining. That claim was unsupported rather than false. A particular profile may still need a new command, and what the published sentence lacked was the evidence for asserting it (Challenge 3).

On key ceremonies, the June 2026 edition said that "PQC key generation requires updated procedures for HSM root keys and PIN translation master keys."

That was wrong. PIN translation keys, and most payment-HSM master and wrapping keys, are symmetric. A PQC transition changes the asymmetric key transport, signatures and key establishment around them, rather than replacing a PIN-encryption key with a KEM or a PQC signing key. PCI PIN Security's key-management hierarchy and the TR-31 and ANSI X9.143 key-block formats settle which keys are which. An organization that budgeted a second PQC key lifecycle for its PIN estate on the published text should re-scope it against an inventory of each key by function and algorithm (Phase 6 adaptation).

On tokenization, the June 2026 edition said that "Tokenization replaces sensitive data (card PANs, account numbers, personal identifiers) with cryptographically irreversible tokens."

That was wrong for format-preserving encryption, and for reversible token schemes generally. Network payment tokens are usable for permitted payment transactions, protected by domain restrictions, cryptograms and their enforcement rather than by irreversibility. PCI SSC's guidance on EMV payment tokens and domain controls settles the point. This edition states the protection as resting on the symmetric cryptography and the access controls around the vault or the key (Challenge 8).

Standards currency runs to September 2026: RFC 9954 and RFC 10024 for hybrid key establishment in TLS (X25519MLKEM768 Recommended=Y), which the payment API and scheme-interface pilots deploy; RFC 10042 for hybrid key establishment in SSH on the management plane; RFC 9964 for ML-DSA in JOSE and COSE, which token signing in payment APIs and 3DS 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 firmware-signing action.

The subsections below read each element for payment organizations. 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 payment organizations as written, with one note: the counterparty coordination pattern (Activity 7.6) is the general case of the scheme, network and SWIFT coordination this extension already specifies. Where the two overlap, this extension's guidance governs.

Two-Track Migration Model in Payments

Track A (Confidentiality / Key Exchange): SWIFT messaging channel encryption, correspondent banking host-to-host connections, payment API TLS endpoints, acquirer-to-processor connections, and card network management links. This track addresses HNDL, and the horizon it protects against is the attacker's: account numbers and track data keep their value to an attacker for the life of the card and beyond, whatever the organization is permitted to retain (PCI DSS prohibits storing sensitive authentication data after authorization).

The Universal states HNDL as inference from demonstrated capability, never as observed harvesting. This extension plans on that inference. Every Track A migration on a Tier-1 interface counts toward Coverage only when the negotiated hybrid outcome is observed in production traffic and classical-only refusal is tested where policy requires it; capability that arrived through a library or gateway default is reported on the incidental line until then.

Track B (Integrity / Signatures / PKI): ISO 20022 Business Application Header signatures, RTGS settlement instruction authentication, card network CA hierarchies, EMV offline data authentication signatures, and payment HSM root key signing. Symmetric MACs (including SWIFT message authentication), PIN translation keys, and DUKPT hierarchies are critical inventory items and are tracked under symmetric key management rather than grouped with Shor-vulnerable public-key signatures. This track addresses TNFL.

Payment organizations should start Track A immediately (hybrid key exchange on SWIFT connections, payment APIs, and acquirer links) and launch Track B within 90 days. Both tracks run as parallel workstreams with separate milestones. Their dependency profiles differ: Track A is largely within the organization's control, while Track B depends heavily on external parties (card networks, SWIFT, central banks). A Track B entry that waits on a scheme CA, on Swift's release 8.0 or on an EMV specification change keeps the tier the ordered test gives it, takes the delivery state dependent with the counterparty's date and firmness grade, and appears on the roadmap against that date. It is never demoted for waiting (Activity 3.2).

Validation Decided Per Product, Per Operation and Per Certificate

Payment infrastructure operates predominantly in FIPS-required or FIPS-aware environments, and a payment HSM answers to two certification regimes at once: FIPS 140-3 for the module, and PCI PTS HSM for the payment operations.

The obligation is checked at its source, never assumed from the sector:

- The PCI PTS HSM requirement comes from the scheme rules and PCI PIN Security.
- A SWIFT interface's comes from the Customer Security Programme.
- 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
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, not 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

Property	Certificate #5247	Certificate #5497
		parameter sets, and LMS

Three qualifications from #5497's Security Policy apply to every citation of it:

- §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.
- HSS key generation, signing and verification are vendor-affirmed, not CAVP-tested.
- The module's firmware-update verification service uses ECDSA and HSS.

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.

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

- the governing requirement
- the exact module and firmware family
- both certificate numbers and their status
- the approved services each 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.

A PQC firmware that breaks the PCI PTS HSM certification is not deployable until re-certified, whatever its FIPS status. PCI PTS HSM v5.0 (May 18, 2026) is the current major version of the Modular Security Requirements. The v4 Security Requirements remain open for new device security approvals until June 30, 2027, under the Council's twelve-month minimum overlap between major versions (PCI SSC bulletin, March 2, 2026). An approval obtained before that date may have been granted under either version, and the register records which.

Sequence the rollout in three steps:

1. **Pilots**, now, in unrestricted environments: development, staging and test HSMs outside the validated boundary.
2. **FIPS-aware systems**, with documented risk acceptance on CAVP-tested algorithms.
3. **FIPS-required and PCI-scoped 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.

It 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 scheme, supervisory and contractual policy, not from a CMVP prohibition; whether an existing deployment on a Historical certificate may continue is decided under the applicable scheme, supervisory or contractual risk policy, and the two questions are assessed separately. Payment organizations 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 Payment Web Infrastructure

For public-facing payment portals, consumer-facing digital wallet endpoints and merchant-facing APIs, 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. Checked for this edition: public root CAs have issued no ML-DSA roots that chain into the major browser and operating-system trust stores. Payment organizations 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).

Internal payment PKI (SWIFT mTLS, HSM certificate chains, card network CA hierarchies, EMV CA hierarchies, terminal and ATM device certificates) continues on X.509 with PQC algorithms. One dated dependency reaches the merchant and processor interfaces 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 acquirer-to-processor links, 3DS server connections and host-to-host channels 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).

Hybrid and Composite Signatures Under Payment Message Constraints

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, and the Financial Services Extension reads it for the broader banking estate in "Hybrid and Composite Signatures as the Track B Default". Payments is where the position meets its hardest constraint: a composite signature is larger than the ML-DSA signature that already exceeds every ISO 8583 field and that Project Leap Phase 2 could carry in the ISO 20022 header only through new components, and Project Leap could not test a hybrid signature at all because the verification software accepts one algorithm at the header level.

Payments resolves this constraint by sequencing the composite rollout to match each format's revision timeline. A dual-signed settlement instruction is hedged only when the receiving system accepts it solely if both signatures validate. The verifier acceptance policy is recorded with the message format. Where message formats are being revised anyway (ISO 20022 buffer work, BAH accommodation), engineer for composite from the start.

The format revision is the gating effort, and carrying the classical component alongside ML-DSA is marginal once buffers are being resized. Where dual certificates are operationally simpler than composite structures (settlement message signing, where Project Leap showed static reference data is the fragile layer), parallel dual-signing achieves the same defense-in-depth. Where neither fits (constrained EMV offline authentication, legacy formats pending revision) solo PQC deployment should be documented as a risk decision per the Universal position, with the implementation-maturity exposure that motivates hybrid weighed explicitly.

Algorithm Weighting and the EMV ECC Transition

The Universal's algorithm-specific vulnerability weighting (Activity 3.1) applies in Phase 3: quantum attack cost scales with key size, not classical strength. A 256-bit ECC key is therefore 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. Payments must read this against its own modernization path. The EMV

specifications' addition of ECC as the successor to RSA for offline data authentication, 3DS signing on ES256, and P-256 credentials in wallets and secure elements are classical-security and performance wins that increase relative quantum exposure.

Organizations mid-transition from RSA to ECC in EMV and card network infrastructure should not book that work as quantum progress, and should not deprioritize ECC-protected payment systems behind RSA-legacy ones in Phase 3 scoring. None of that assigns a tier: the ordered test of Activity 3.2 reads dimension scores and factor values from the record, and neither the algorithm nor the key size is among them. The record feeds the sequencing inside a tier instead, where the attack-cost evidence separates entries that tie on the composite score. Record algorithm and key size per entry in the payment CBOM so that separation reads one recorded value rather than a judgment re-debated per system.

The Identity Stack in Payments (Track B)

The Universal brings the identity stack explicitly into Track B scope, and payments is further along this curve than most sectors. The Financial Services Extension gives the banking-wide reading. This subsection covers the payment surface. Payment passkeys (FIDO credentials replacing OTPs in 3DS flows and Click to Pay) typically assert with ES256 on P-256 or RS256, and the inventory records the algorithm actually enrolled per credential population: long-lived classical credentials being enrolled at scale right now. 3DS directory server and ACS signing, OAuth/OIDC token signing in payment APIs, wallet device-bound keys in secure elements, and terminal and ATM device certificates belong in the same Track B inventory slice.

Two payment-specific actions follow: include the issuer ACS, wallet platforms, and passkey infrastructure in the identity CBOM slice during Phase 1, and put the credential migration question (how enrolled passkeys and device-bound keys will be re-enrolled or migrated when signature algorithms change) into Phase 7 vendor governance for ACS providers, wallet platforms, and authentication vendors, asked as the Universal's second agility question.

For a WebAuthn assertion the customer's authenticator holds the private key and signs, and the relying party verifies against the enrolled public key. In payments that relying party is the issuer ACS, the wallet platform or the Click to Pay participant. Its verification implementation is server-side and updatable. Phase 3 scores that implementation on verifier updatability and reaches Medium or Low. What cannot be updated is the credential on the customer's device, whose algorithm changes only by re-enrollment.

Phase 3 records that as a separate constraint, scored Hard on the Universal's control-posture factor in Dimension 3, with the delivery state blocked until the re-enrollment path exists. The entry reaches the agility-debt register through the control-posture score, not through verifier updatability.

SP 800-208 Firmware Signing as the Deploy-Now Track B Action

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), and the payments estate is where the action has the longest reach. Terminal and ATM fleets have 7-to-15-year replacement cycles. The firmware update verification keys provisioned into hardware shipping today must survive into the CRQC era, and a terminal whose verifier cannot follow an algorithm change is the clearest agility-debt entry in the sector.

LMS and XMSS are standardized, conservative, and recommended by CNSA 2.0 for signing software and firmware, with ML-DSA-87 approved under CNSA 2.0 for all signature use cases including firmware (Universal, Two-Track Migration Model). 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. The CMVP search form offers no filter for LMS or XMSS, so the validated population cannot be enumerated, and this extension makes no broader claim in either direction. The HSM firmware the June 2026 edition named as supporting these schemes is in Tool and Vendor References, verified there for the general-purpose line only. The deploying organization verifies parameter-set coverage on the specific certificate rather than inferring it from the algorithm's presence.

"Deploy now" carries SP 800-208's own conditions, in section 8 of that publication: key and signature generation inside a hardware module with at least Level 3 physical security, no export of the private key in any form, and signing state managed inside the module so that backup, replication and failover designs cannot reuse a state. A signing service that does not meet section 8 is not a conforming deployment, and the terminal and ATM 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, and tested backup, replication, crash-recovery and concurrent-signing behavior. The action: move terminal, ATM, and HSM firmware signing pipelines to SP 800-208 signatures now, dual-signed with classical during transition, operated from HSM-backed signing infrastructure whose module certificates, parameter-set coverage and entropy validation are recorded in the Phase 6 register.

The state-management constraint that makes these schemes unsuitable for general-purpose use is met where the section 8 evidence above exists. The controlled signing ceremonies payment organizations already run are the operating context for that evidence, not a substitute for it, and the quarterly HSM-partition failover exercises the

state-management design as well as the failover, recorded as a failover and state-management result rather than as an algorithm-change rehearsal.

Securing the Payment CBOM

The Universal's Activity 2.5 (Secure the CBOM and Program Artifacts) applies with particular force in payments. A complete payment CBOM maps HSM locations and key hierarchies, DUKPT-to-terminal-population relationships, unmigrated external interfaces, and the certificate chains that authenticate settlement. An adversary with a copy of the CBOM – from a payment fraud operation to a nation-state – would have a pre-built target map of the HSM estate and its trust hierarchy.

PCI workflows widen the exposure: 12.3.3 documentation, QSA assessments, PIN security assessments, and acquirer or network due diligence all create standing requests for exactly this data. The default answer to each of them is the rule the Financial Services Extension states in "Securing the CBOM Against Examination and Due-Diligence Requests": attest, do not send. The QSA, the PIN assessor, the scheme or the acquirer receives a signed commitment to the snapshot, a coverage statement with its denominator and discovery method, and the predicate the request needs ("every PCI-scoped cipher suite and protocol is inventoried and was reviewed within twelve months"; "no scheme-facing Tier-1 interface negotiated classical-only key establishment during the observation window"), in place of the document.

Where an assessment requires the record itself, it is a point-in-time extract scoped to the assessment, delivered through a controlled channel, never standing access to the queryable inventory. The CBOM is marked AMBER or RED at generation, and the repository joins the SOC's high-sensitivity exfiltration watch list.

Verification and Decommissioning in Multi-Party Payment Networks

The Universal's Migration Verification & Program Closure section defines what "done" means, and payments needs its discipline more than most because configuration and reality diverge across counterparty boundaries. Verification in payments means observed negotiation on the wire: SWIFT connections, card network links and payment APIs showing hybrid or PQC algorithms in production traffic, not in configuration files. Once schemes set classical-refusal dates, it also means negative testing that classical-only counterparties are refused.

For Track B, evidence comes from endpoint telemetry, the certificate inventory and authorized active tests, because TLS 1.3 encrypts the certificate and signature algorithm. For Tier-1 systems, evidence includes the rehearsal record showing that the algorithm was changed by configuration in staging and rolled back, with the elapsed time per segment. Decommissioning in payments is complicated by trust-store persistence. Retired EMV CA certificates and superseded signing keys remain in terminal trust stores for years.

A key is retired only when no device still trusts it. Plan trust-store cleanup across the terminal and ATM estate as an explicit migration wave. Log key destruction with certificates for HSM-held material per the Universal evidence standard.

Closure reads three things against the payments estate. First, a verification disposition for every Tier-1 and Tier-2 service, one of four: migrated with no agility debt outstanding; migrated with agility debt and a funded closure date; enclosed or compensated under an accepted exception; retired. Second, 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.

Third, the agility-debt register at zero unaccepted debt: every remaining entry has a funded treatment with a date or a SteerCo-signed exception. In payments the expected entries are the terminal and PIN-pad populations whose verifiers cannot be updated in the field, the ATM fleets on legacy remote key loading, the enrolled passkey and device-bound credential populations, the scheme and SWIFT interfaces whose algorithm the network sets, and the payment HSM firmware families with no configuration-driven algorithm selection.

Each closes as migrated with agility debt against a dated vendor, scheme or network release with a firmness grade, as enclosed under the Encapsulate Strategy with a bridge end date or a signed exception, or as retired on the refresh roadmap. A terminal population that will not follow its refresh cycle inside the roadmap is an exception the SteerCo signs with a re-evaluation date, not a line that disappears from the register. At closure the program hands three things into business as usual: the Cryptographic Record owner retains the CBOM. The Crypto-Agility workstream transfers with its owner, its budget and the rehearsal cadence on the gateways, the issuers and the signing services as its standing cadence, with the quarterly HSM-partition failover reported beside it as a failover and state-management exercise; and algorithm transitions on the organization's own gateways, HSMs and signing services enter routine change management.

The Agility Criterion and Rehearsal in Payments

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 payments the first two conditions are met on the external payment API gateway, the acquirer-to-processor links and the host-to-host channels the organization controls. The third and fourth are met on those layers, on the internal payment service mesh, on the internal PKI and on the firmware-signing pipelines, and they fail on the terminal and ATM fleets, on the scheme and SWIFT interfaces whose algorithm the network sets, and on payment HSM firmware that changes algorithms only with a release.

A payment organization is crypto-agile, in those terms, when it can change the algorithm on its own gateways, its own HSM estate and its own signing services on a planned date; and when it can name the date on which each scheme, network and terminal population will follow. Every wave includes an algorithm-change rehearsal on at least one system in the wave, chosen from the layer the organization controls: a parameter-set change (ML-KEM-768 to ML-KEM-1024) on the external payment API gateway; a hybrid-to-composite switch on the firmware-signing pipeline; a certificate-signature-algorithm change on the internal issuer that signs terminal and device certificates; for the payment HSM estate, one of those three run on the HSM-backed signing service, 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, and is scheduled outside the month-end, quarter-end and peak-season change 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.

It 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 terminal firmware release, a scheme cutover or a Swift release 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 Payments

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 payments the distribution is split by ring. Passive monitoring on the external payment API gateway, the acquirer links and the SWIFT connection produces E1 for the traffic it sees. The payment HSM estate yields E3 from the HSM management console exports and E4 from the vendor's firmware and certificate statements.

The terminal and ATM fleets are E3 from the terminal management system and E4 from the terminal vendor. Their offline data authentication is E5 until a device is examined. The card platform SDK and SWIFT Alliance software are E2 for the binaries that can be analyzed and E4 otherwise. Counterparty cryptography (schemes, SWIFT, correspondents, RTGS operators) is 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 travels with the finding into the CBOM and into Phase 3, where 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, the terminal management system's device census and the PCI DSS

12.3.3 documentation the organization already maintains, never from what the tools found. A coverage figure states its denominator ("88 percent of the 1,240 external TLS endpoints enumerated from the API-gateway and load-balancer 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, and the terminal fleet's offline authentication is named as unobserved with its coverage recorded as unknown, not zero. The same denominator is the one the PCI 12.3.3 evidence, the PIN security assessment and the Inventory Completeness KRI (Universal, GRC Implementation) all read.

Vendor Dates and Questions in Payments

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. At this edition Swift's release 8.0 date is announced. The Visa and Mastercard CA migration dates and every EMV specification date are unknown.

The payment HSM certification dates are graded per vendor from the questionnaire. The questionnaire opens with the two agility questions and the firmness question (Activity 7.2). In payments the answer to the first agility question sets the migration path for the payment HSM estate and the acquiring platform. The answer to the second sets it for the terminal and ATM fleets, the enrolled credential populations and the mobile wallets with pinned certificates, which are the sector's verifier populations.

The four certificate-authority questions go to every issuer the organization depends on: its public CAs, the scheme CAs, the EMV CA hierarchies, the SWIFT PKI, the domestic scheme CAs and the internal issuer that signs terminal and ATM device certificates. The non-standardized-algorithm rule and its one-afternoon test (Activity 7.3) apply to every terminal, HSM or gateway 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 HSM, payment-as-a-service and tokenization provider: the provider's completion date is the date its half of the boundary migrates, and the carve-outs in its footnotes are unmigrated components. The Phase 7 adaptations place the whole set inside the third-party risk management cycle the organization already runs.

PHASE-BY-PHASE FRAMEWORK ADAPTATIONS FOR PAYMENTS

This section specifies the adaptations required for payment infrastructure for each Universal Framework phase. Organizations should implement these alongside the Universal Framework and the Financial Services Extension. 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

Payment-Specific Business Case Arguments

- **Settlement disruption risk:** Reference the BIS Project Leap Phase 2 report (December 2025) to demonstrate that PQC works in a settlement system and introduces measurable performance overhead: a 7.5× signature verification slowdown on the T2 test environment, on a system class that settles many multiples of GDP per year, gives the board a measured performance cost on a named system.
- **Systemic cascading-loss scenario:** The Hudson Institute's April 2023 analysis (Butler and Herman, "Prosperity at Risk"), as relayed in the Project Leap Phase 2 report, estimated that a quantum-enabled attack on Fedwire alone could reduce US real GDP by 10 to 17 percent, with $2 to $3.3 trillion in indirect losses measured as GDP at risk. The June 2026 edition attributed the figures to a joint Citi Institute analysis. The attribution is corrected to the Hudson Institute study.

The six-month-recession framing was not an addition: Hudson's own abstract describes the analysis as running through the resulting six-month recession. The GDP range and the dollar figures are conditional estimates in the study's scenarios, not forecasts.

- **Regulatory convergence:** Map PCI DSS 12.3.3 (required after March 31, 2025), the G7 Cyber Expert Group roadmap (critical systems within 2030–2032), the EU coordinated roadmap (high-risk use cases by 2030), Swift's Alliance Release 8.0 (planned for end July 2027) and the Singapore CII milestones (plan by March 31, 2027; procure quantum-safe-ready from January 1, 2028) into a single timeline, each date with its firmness grade, showing that the investment is scheduled by parties the organization does not control.
- **Hardware lead times:** HSM certification cycles (12–24 months), card reissuance (3–5 years for fleet turnover), and terminal replacement cycles (7–15 years) mean decisions deferred today constrain options for years. The delivery state of each hardware-bound entry says which decisions are already blocked.
- **Readiness and agility as one charter:** The charter states both outcomes in the Universal's dual-outcome form: readiness against the dated obligations above, and crypto-agility as the capability that makes the next algorithm change on the organization's own gateways, HSMs and signing services a planned date rather than a program. A payment organization that migrates its scheme interfaces once will migrate them again when the scheme moves. The agility outcome ensures the second move requires only a configuration change on the organization's own infrastructure.

Governance Adaptation for Payments

Payment PQC governance must include representation from acquiring, issuing, terminal management, payment HSM operations, SWIFT administration and settlement, in addition to IT security and compliance. The Financial Services Extension's recommended Quantum Readiness Working Group should include a dedicated payments sub-group. Two owners are named at chartering (Activity 0.3): the Crypto-Agility workstream owner, placed in the function that controls the payment gateways, the HSM estate and the firmware-signing pipelines, with a budget line from Year 1 and the agility-debt register as scope; and the Cryptographic Record owner, the permanent owner of the payment CBOM, separated from Discovery because discovery ends and the record does not.

The three lines apply by function: the program under the CISO delivers as first line, the risk function challenges the scoring model, the gate decisions and closure as second line, and internal audit is third line. The same mapping the Financial Services Extension places inside the bank's existing model.

Phase 1 – Discovery & Inventory

Payment-Specific Inventory Tracks

In addition to the Universal Framework's three parallel inventory tracks (cryptographic inventory, sensitive data, systems and assets) and the Financial Services Extension's broader sector tracks, payment organizations should add the tracks below. Every finding

on every track has an evidence grade E1 to E5 attached to the claim (Activity 1.2), and the coverage denominator for each track is enumerated before discovery runs (the alignment section's evidence subsection names the sources):

- **Payment message format analysis:** Inventory every format in use (ISO 8583, ISO 20022, SWIFT MT/MX, domestic scheme formats). Map field-level cryptographic dependencies and identify fixed-size fields that cannot accommodate PQC payloads.
- **Payment HSM estate mapping:** Inventory all payment HSMs into the four-field register of Activity 6.2 (visible platform, firmware family, manufacturer of origin, certificate reference, the last as both the FIPS 140-3 and the PCI PTS HSM certificate), with the vendor PQC roadmap graded for firmness. Classify each as PQC-ready, PQC-upgradeable, or PQC-blocked, and record the delivery state that follows.
- **Card and terminal estate:** Inventory card platforms by chip type, RAM capacity, supported algorithms. Map offline versus online authentication reliance by card program. Inventory terminals and PIN pads by firmware version, PCI PTS certification status, remote-update capability and verifier updatability. Record for each population who can change its cryptography: the vendor's firmware, the terminal management system, or an in-field key-injection process. The population that no one can change remotely is the one the Encapsulate Strategy will enclose.
- **SWIFT infrastructure:** Inventory the Alliance deployment model and release level (7.7, 7.9 or later), SWIFT-facing HSMs, PKI certificates, and CSP control compliance. Assess the path to Alliance Release 7.9 and then 8.0, and the compatibility of the message-handling systems with release 8.0 requirements as Swift publishes them.
- **Third-party payment interfaces:** Map every external cryptographic interface: SWIFT, card network links, clearing house integrations, correspondent banking channels, payment APIs, 3DS directory server connections.
- **Certificate authority hierarchies:** Map all CA hierarchies: internal PKI, card network CAs, SWIFT PKI, domestic payment scheme CAs, EMV CA hierarchies.
- **PCI-scoped system cryptography:** Structure the inventory to satisfy PCI DSS 12.3.3 simultaneously, producing both PQC readiness assessment and PCI compliance evidence from the same data collection, on the same denominator.
- **ATM and remote key loading:** Inventory ATM fleet by model, remote key loading protocol version (TR-34), key-block format (TR-31 or ANSI X9.143, symmetric and inventoried under key management), and PQC hardware feasibility.

Phase 2 – CBOM & Documentation

Payment CBOM Complexity

Build the payment CBOM in concentric rings on the Universal's minimum record (Activity 2.1). The first ring documents cryptography the organization controls directly: HSM key material, internal application encryption, owned certificate hierarchies. The second ring

documents vendor-consumed cryptography: payment HSM firmware implementations, card platform SDK functions, SWIFT Alliance software. The third ring documents dependencies on counterparties and networks: card network CA certificates, SWIFT PKI, RTGS authentication, correspondent bank channel encryption.

The third ring will be incomplete, and the accepted-gaps register says so with the readiness-inquiry date for each counterparty. In the Universal's CBOM layers, the first ring is CBOM Layers 1 and 2 (infrastructure and platform cryptography, the HSM estate first), the second ring is CBOM Layer 4 (vendor and embedded cryptography) and the third ring is the counterparty dependency the standard CBOM model does not address. Organizations that keep the CBOM in the Applied Quantum CBOM Profile (v1.0-RC or later) record the same facts as Profile properties, the payment HSM register fields as `custody:*` and the counterparty context as `fs:*`. The Profile is informative carriage and is never required.

PCI DSS 12.3.3 as CBOM Accelerator

PCI DSS 12.3.3 already mandates documentation of all cryptographic cipher suites and protocols for PCI-scoped entities, reviewed annually. The CBOM effort should be structured to produce PCI 12.3.3 evidence artifacts as a standard output, as attestations and scoped extracts rather than the queryable inventory (alignment section, Securing the Payment CBOM). The CBOM effort thereby satisfies the PCI 12.3.3 documentation obligation as a standard output, without a separate work package.

Phase 3 – Risk Scoring & Prioritization

Payment-Specific Risk Scoring Dimensions

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 Financial Services Extension restates its systemic criticality and multi-party dependency dimensions as factors inside Dimensions 2 and 3. The June 2026 edition of this extension added two more dimensions for payments.

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. The tier is assigned by the Universal's ordered test (Activity 3.2), read from Dimensions 1, 2 and 4.

The first condition that matches assigns the tier. The composite score orders entries inside a tier and plays no part in the assignment. Dimension 3 and the delivery state place no tier.

- **Settlement chain position (a factor inside Dimension 2, read with the Financial Services systemic-criticality factor):** Does a forged instruction or a compromised trust anchor on this element reach settlement? RTGS access, clearing-house and scheme settlement interfaces = Critical; interbank messaging and acquirer-to-network links = High; acquirer and merchant interface layer = Medium; internal only = Low.
- **Hardware constraint severity (a factor inside Dimension 3, the Universal's control-posture and system-age factors read for the sector):** Is migration blocked by hardware limitations? Card chip RAM, terminal processor or an ATM platform that cannot support PQC = Hard; a payment HSM whose PQC operation waits on a certificate = Medium, with the delivery state dependent; software-upgradeable = Easy. The factor sets the remediation strategy (refresh, enclosure or replacement) as well as the score.
- **Verifier updatability (the Universal's Dimension 2 factor, read for the sector):** Verifiers that cannot be updated (the terminal and PIN-pad populations no terminal management campaign reaches, which are the verifiers of offline data authentication; ATM firmware the operator cannot change; wallet apps with pinned certificates that no release reaches) = Critical; updatable by a terminal management campaign or a scheduled app release = Medium; centrally managed trust stores = Low.

A scheme's, a network's or a counterparty'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. A credential held by the signer is not a verifier. For enrolled passkeys, device-bound wallet credentials and card credentials that change only by reissuance, this factor scores the implementation that actually checks the signature: the relying party's server for a passkey assertion, the terminal population for offline data authentication.

The difficulty of re-enrolling or reissuing the credential population is scored Hard on the Universal's control-posture factor in Dimension 3 and recorded in the delivery state. It is the strongest single indicator of agility debt in the payments estate.

- **Weighting:** The Universal's default weights (HNDL 0.35, TNFL 0.25, regulatory 0.25, feasibility 0.15) stand for payments. HNDL on external payment interfaces is the most immediately exploitable threat in this sector, and Dimension 4 scores the scheme and PCI gates at enforcement tier 1. The SteerCo ratifies the dimensions, the weights and the appeals rule before the first scoring run (Activity 0.3).

Algorithm-specific weighting: Apply the Universal Framework's algorithm weighting (Activity 3.1): quantum attack cost tracks key size, not classical strength, so ECC-protected payment systems score at least as urgent as RSA-2048 estates. See the Alignment section for the EMV ECC transition implications.

Delivery state and the agility-debt register. Every scored entry records 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 payments the dependent and blocked Tier-1 entries are the SWIFT interfaces waiting on Alliance Release 8.0 (announced), the scheme interfaces waiting on a CA migration date (unknown), and the FIPS-required and PCI-scoped HSM operations waiting on a certificate.

The agility-debt register lists every Tier-1 and Tier-2 entry scored Hard on control posture, system age or hardware constraint, or Critical on verifier updatability. Each entry states the reason. In payments the expected entries are the terminal and ATM populations whose verifiers cannot be updated in the field, the enrolled credential populations (which reach the register on control posture, not on verifier updatability), the scheme-set interfaces, and the payment HSM firmware families with no configuration-driven algorithm selection.

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

Payment Infrastructure Priority Tiers

Priority	System Category	Rationale	Typical Delivery State
Tier 1	Internet-facing entries: external payment APIs, merchant-facing gateway endpoints, consumer-facing wallet and 3DS challenge endpoints. Settlement-chain and network entries: RTGS and settlement connections, scheme settlement interfaces, SWIFT interfaces, and correspondent banking encryption on links whose recorded confidentiality	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 settlement-chain factor reaches for RTGS access and scheme settlement interfaces, the trust-scope and key-lifetime factors reach	Available for the organization's own channel encryption, API gateway and host-to-host links; dependent for SWIFT and RTGS interfaces, on the network's release with a firmness grade; dependent or blocked for FIPS-required and PCI-scoped HSM operations, on the module certificate; blocked for offline data authentication and the non-updatable terminal

Priority	System Category	Rationale	Typical Delivery State
	horizon exceeds 15 years. Trust anchors and long-lifetime keys: payment HSM root key material, the internal issuer's root, and the card network, EMV and SWIFT CA hierarchies the organization participates in. Keys whose verifiers cannot be updated: smart card offline data authentication, the terminal and PIN-pad populations no terminal management campaign reaches, ATM fleets on legacy remote key loading whose firmware the operator cannot change	for HSM roots and the scheme, EMV and SWIFT trust anchors, and verifier updatability reaches for the terminal and ATM populations whose verifiers cannot be updated; or Dimension 4 Critical on a mandatory deadline within 2 years, which no payment instrument reaches for PQC at this edition. Swift's Alliance Release 8.0 (planned for availability at end July 2027) is a mandatory software release and not a published requirement to use PQC by a date, so the Dimension 4 factor scores from the participant requirement when Swift publishes one. The SWIFT interfaces hold this tier on Dimension 1 where the recorded confidentiality horizon of the message content exceeds 15 years, and on Dimension 2 where a forged instruction on the	and ATM populations, on the card and terminal refresh cycle or the ATM replacement cycle. A dependent or blocked entry keeps this tier and runs under a bridging pattern until the dependency lands: enclosure under the Encapsulate Strategy at the acquirer host, the terminal management system or the estate gateway for the terminal and ATM channels (Challenge 3); manual key injection or enclosure behind the host for legacy remote key loading (Challenge 10); tokenization that takes the cardholder data out of the exposed path (Challenge 8); PQC key-wrapping around a payment HSM whose operation waits on a certificate (Activity 7.4). Where no bridge reaches the verifier (offline data authentication on the chip), the residual exposure is recorded under Activity 7.4's documented risk

Priority	System Category	Rationale	Typical Delivery State
		entry reaches settlement or where the SWIFT CA hierarchy is the trust anchor the entry depends on; an entry that reaches neither sits in Tier 2 on Dimension 2 High. Difficulty places nothing here or anywhere: a hardware-constrained population sits in the tier its risk gives it, with the delivery state recording the constraint.	acceptance with a re-evaluation date
Tier 2	Partner-facing links carrying cardholder data with a recorded horizon of 15 years or less: acquirer-to-processor and host-to-host links on private circuits, 3DS directory-server connections. Shared signing keys and intermediates with updatable verifiers: 3DS access control server and directory-server signing keys, OAuth/OIDC token signing in payment APIs, the internal issuer's intermediates for terminal and device certificates.	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-requirement factor. Multi-party coordination and consumer-facing reputational risk follow from the same facts and place nothing on their own.	Available for the gateway, the acquiring platform and the internal issuer; dependent for the scheme's directory-server connections and signing requirements, on the scheme's date (unknown at this edition), and for the campaign-updatable terminal and ATM populations, on the campaign; blocked for the enrolled passkey and device-bound wallet credential populations, on the re-enrollment path;

Priority	System Category	Rationale	Typical Delivery State
	The enrolled passkey and device-bound wallet credential populations, placed by Dimension 2 High on the credential-lifetime and trust-scope factors, with the re-enrollment difficulty scored Hard on control posture; a population whose recorded remaining credential life reaches 15 years moves to Tier 1 on the key-lifetime factor. The terminal and PIN-pad populations updatable by a terminal management campaign and the ATM fleets whose firmware the operator can update (verifier updatability Medium), placed by Dimension 1 on the acquirer channel they use. Internal stores holding cardholder data with a recorded horizon over 10 years: payment databases and message archives not yet tokenized. Entries under a contract that requires PQC or a mandatory deadline		the entry keeps its tier and shows the unblocking dependency

Priority	System Category	Rationale	Typical Delivery State
	within 5 years		
Tier 3	Internal services whose data horizon is 10 years or less and whose keys are relied on by one application: the internal payment service mesh, transaction monitoring encryption, fraud detection data stores, payment databases and archives whose cardholder data is tokenized or whose horizon is 10 years or less, single-application signing verified through centrally managed trust stores	Any applicable risk dimension (1, 2 or 4) Medium or above, none higher. Internally controlled; migrates on the organization'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	Entries with no remaining confidentiality need and no trust dependency: message archives past their confidentiality horizon that hold no cardholder data, session keys and short-lived credentials verified only by the system that issued them, test and development	Every applicable risk dimension Low. Monitor; compensating controls; migrate when feasible. A blocked migration does not place an entry here: smart card offline authentication, the non-updatable terminal populations and legacy ATM remote key loading are hardware-	Blocked entries are shown in the tier the ordered test gives them, not in this one

Priority	System Category	Rationale	Typical Delivery State
	estates holding no production data	constrained and sit in Tier 1 on their risk with the delivery state blocked.	

Phase 4 – Roadmap & Governance

External Dependency Timeline Map

Payment roadmaps must incorporate external timelines that the organization does not control. Every date below is graded for firmness (Activity 7.5: committed, forecast, announced, unknown), as of September 2026. 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.

Availability, prerequisite deployment, end of support and mandated PQC use are four separate dates on this dependency, recorded separately. The Dimension 4 deadline factor scores from the last of them and never from the availability date.

- **Card network PQC timelines:** Visa and Mastercard CA migration timelines: no dated public roadmap found for either scheme; grade: unknown as of September 2026. EMV specification changes: none published; EMVCo's stated position (January 30, 2026) expects no practical threat to the EMV infrastructure before 2040, maybe never; grade: unknown.
- **HSM vendor certification:** FIPS 140-3 Level 3 CMVP validation with the PQC operation as an approved service, and PCI PTS HSM v5.0 evaluation of the same firmware, tracked per product and per firmware family; grade per vendor from the questionnaire (product names in Tool and Vendor References). CMVP certificate #5247 (April 2026) lists ML-KEM at ML-KEM-768 and ML-KEM-1024 in a Level 1 software module, and CMVP certificate #5497 (August 2026) lists ML-KEM, ML-DSA, SLH-DSA and LMS inside the approved boundary of a Level 3 hardware module, each with the qualifications the validation subsection states; whether a payment

HSM firmware offers the PQC operation in approved mode under both of its certificates is read per product from the CMVP validated-modules list and the PCI Approved PTS Devices list.

- **Smart card silicon:** PQC-capable 28 nm smart card silicon announced for 2026 mass production and next-generation secure microcontrollers (supplier and product names in Tool and Vendor References). Grade: announced.
- **Central bank RTGS upgrades:** T2, Fedwire, Bank of England RTGS and BOJ-NET modernization timelines for PQC adoption. Grade: unknown at this edition; obtained through the counterparty pattern (Activity 7.6), with the Project Leap Phase 2 report as the Eurosystem's published evidence of intent.
- **Domestic payment schemes:** ACH, SEPA, Faster Payments, BACS, UPI, PIX scheme-level PQC adoption decisions. Grade: unknown at this edition.
- **Regulatory milestones:** PCI PTS HSM v5.0 published (May 18, 2026), with the v4 Security Requirements open for new device security approvals until June 30, 2027 and the v4 and v3 device approval expirations extended to April 2033 and April 2028 (PCI SSC bulletin, March 2, 2026); PCI SSC standalone PQC guidance: none published at this edition; the Singapore CII milestones (plan by March 31, 2027; procure quantum-safe-ready from January 1, 2028; complete by December 31, 2031) for CII-designated payment operators; the plan-by dates of the national supervisors in the Universal's roster and on the Global PQC Migration Clock page.

These external dependencies are visualized on a single timeline map with their grades and reviewed quarterly. Where an external date slips, the organization's roadmap adapts through the Re-Baseline Protocol (Activity 4.8): Swift or a scheme moving a 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 organization 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). An external payment API that passes on protection and whose gateway can change its algorithm by configuration exits as migrated; a scheme interface that passes on protection with the algorithm set by the network exits as migrated with agility debt, with the entry and its closure date in the Phase 3 register; a terminal population protected by enclosure exits as enclosed under an accepted exception or as a bridge with an end date.

Neither result stands in for the other, and the Coverage and Agility KPIs read them separately. Gate records are filed to the evidence dossier in the form the QSA, the PIN assessor and the scheme read.

Recommended Year-1 Plan for Payments

- **Q1:** Establish the payment PQC governance sub-group and name the Crypto-Agility workstream owner and the Cryptographic Record owner. Begin the PCI 12.3.3 aligned cryptographic inventory on PCI-scoped payment systems with evidence grades and the denominator stated. Initiate payment HSM vendor engagement, agility questions first. Commission the SWIFT readiness assessment against Alliance Release 7.9 and 8.0.
- **Q2:** Expand the inventory to payment message format analysis (ISO 8583/20022 field-level mapping), the card and terminal estate with verifier updatability recorded, the ATM fleet, and the 3DS infrastructure. Begin CBOM construction for Tier-1 systems on the minimum record. Conduct the tokenization coverage assessment. Sign the accepted-gaps register at gate G1 → G2, with the counterparty ring and the terminal fleet's offline authentication on it.
- **Q3:** Ratify the scoring model, weights and appeals rule at the SteerCo; complete Tier-1 risk scoring with the payment factors and delivery states; produce the agility-debt register. Produce the initial Quantum Readiness Assessment for board consumption, with the terminal-fleet and scheme-dependency debt stated on its own. Begin Tier-1 pilot design (SWIFT test interface or external payment API with hybrid X25519MLKEM768).
- **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 for the HSM hardware refresh, the terminal refresh and enclosure plan, expanded pilot scope and the agility milestones on it.

Phase 5 – Pilots & Migration Execution

Payment Pilot Targets

The Universal's first-layer selection table (Activity 5.2) names the API gateway and its mutual TLS as the first layer for API-driven financial services: counterparties reach one enforcement point, and the gateway holds the negotiation policy. The payment pilots follow that row:

- **External payment API with hybrid TLS:** Enable hybrid X25519MLKEM768 on a non-critical external payment API at the gateway. Lowest-risk, highest-learning pilot. Force a fresh handshake on a defined interval for persistent connections, require the hybrid group on resumption and disable 0-RTT for the flows in scope; count the endpoint toward Coverage only once the negotiated outcome is observed and the policy is tested.

- **SWIFT test environment:** Pilot PQC message signing in the non-production SWIFT environment as Swift's pilot and sandbox programs open. Measure ISO 20022 BAH signature size impacts and certificate distribution requirements, and record the verifier acceptance policy for dual signatures.
- **Settlement performance benchmarking:** Replicate the BIS Project Leap Phase 2 method on the organization's own infrastructure, with the HSM in the loop and certificates rather than raw keys, which the report left for future testing. Benchmark ML-DSA verification throughput at peak volumes.
- **Payment HSM PQC key generation:** Pilot PQC key generation on test HSMs, including where the module performs it as a service that is not approved under its validation. Validate key ceremony procedures and dual-key management. Record the module and its version, the cryptographic boundary and the service as separate fields in the Phase 6 register, and record the operating mode, the algorithm validation and the governing policy beside them, with the firmware family and the entropy validation as before.
- **Internal payment service mesh:** Enable hybrid key exchange in the internal TLS mesh between payment microservices from the mesh control plane for production-scale performance data.
- **Terminal firmware signing:** Dual-sign one terminal or PIN-pad firmware release with an SP 800-208 signature alongside the classical signature, from the HSM-backed signing service, and verify acceptance on a sample of each verifier generation in the fleet. The sample is what shows which populations the verifier can follow.

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 organization controls: a parameter-set change from ML-KEM-768 to ML-KEM-1024 on the external payment API gateway; a hybrid-to-composite switch on the firmware-signing pipeline; a certificate-signature-algorithm change on the internal issuer that signs terminal and device certificates; for the payment HSM estate, one of those three run on the HSM-backed signing service, or a key ceremony that generates a PQC-authorized signing key and retires it.

The rehearsal is timed across assessment, decision, change and verification, with the rollback exercised. It is scheduled outside the change advisory board's month-end, quarter-end and peak-season freezes. The four elapsed times feed the rehearsed time-to-change KPI. The quarterly failover to the backup HSM partition is recorded beside them as a failover and state-management exercise, not as a rehearsal. Its timing does not feed that 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 organization applies the counterparty pattern: published dual-stack windows on acquirer and host-to-host interfaces, interoperability test events before enforcement, and the refusal decision recorded in the risk register for the counterparty that will not move. Wave 5 (long tail) is the terminal and ATM estate, where the exit record states enclosure or refresh per population.

Tokenization Coverage Assessment

Before designing data-at-rest migration pilots, conduct a tokenization coverage assessment identifying which payment data categories are already quantum-defended, which use FPE warranting further analysis, and which remain exposed to HNDL. Expanding tokenization scope may be faster and cheaper than end-to-end PQC for certain data stores.

Hybrid Architecture Planning

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. Plan for hybrid as an architectural change requiring duplicate PKI infrastructure, extended certificate handling, modified verification logic, expanded message format buffers, and updated reference data at all counterparties.

The hybrid period will last years and must be managed as a sustained operational state. 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 verifies that the switch required no code release, recompilation or hardware replacement.

Phase 6 – Infrastructure Modernization & Performance

Payment HSM Modernization Strategy

The Universal's Activity 6.2 register is the instrument for the payment HSM estate. 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. For a payment HSM the certificate reference is both the FIPS 140-3 certificate and the PCI PTS HSM certificate, each with the version of the standard the approval falls under and its status.

For PCI PTS HSM that version is v3, v4 or v5.0. A v4 approval can still be obtained until June 30, 2027. The v3 and v4 device approval expiration dates now run to April 2028 and April 2033 (PCI SSC bulletin, March 2, 2026). The installed base the register covers therefore outlives this edition by years. Two products under two names can be one

firmware family. A cloud or hosted payment HSM is recorded as a dependency boundary rather than as a manufacturer.

The boundary-verification rule of Activity 7.7 applies to those 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 in the register. A "quantum" label on a randomness product is not a requirement of this framework or of any standard it cites.

Organizations 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, cross-referenced from the register. Model, firmware and certification references as the June 2026 edition listed them are in Tool and Vendor References.

- **Firmware versus hardware replacement:** Classify the HSM estate from the register and the vendor questionnaire. Current firmware generations include initial ML-KEM, ML-DSA and LMS support on some payment HSM product lines. On others PQC arrives as an in-field application package. Older units require hardware replacement with 12 to 24 month lead times. 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, for FIPS 140-3 and for PCI PTS HSM as two independent dependencies. 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 and PCI-scoped classes. A PQC firmware that breaks the PCI PTS HSM certification is not deployable until re-certified. Monitor the CMVP Modules in Process list and the PCI Approved PTS Devices list for the modules the estate depends on.
- **Key ceremony adaptation:** PIN translation keys, and most payment-HSM master and key-wrapping keys, are symmetric. A PQC transition changes the asymmetric key transport, signatures and key establishment around them. It does not replace a PIN-encryption key with a KEM or with a PQC signing key. Inventory each key the ceremony touches by function and by algorithm, not by ceremony. Track the symmetric-strength changes, TDEA to AES and the key-block format versions, on their own schedule and separately from PQC.

Update ceremony procedures for the asymmetric dependencies the ceremony actually involves: the key transport, the certificate-based authentication of the participants and the signatures over the key blocks. Record how each of those relates to the symmetric keys it protects. Define "root key" by the role it plays, whether that is the local master key, the top key-encryption key of a wrapping hierarchy or an issuer signing root,

because the term names a position and not an algorithm. Rehearse in test environments before production. The rehearsal is timed and filed like any other (Activity 5.2).

- **Dual-key management:** During hybrid transition, HSMs must manage both classical and PQC key material. Dual-algorithm operation is not twice the key-storage bytes: it adds a second key lifecycle (generation, backup, rotation, destruction) with its own ceremonies for the asymmetric keys it introduces, its own backup, replication and failover design, and, for stateful firmware-signing keys, state handling the classical estate never needed.
- **Partition failover as the standing exercise:** The quarterly failover to the backup HSM partition exercises state management, failover and the SP 800-208 state design, changes no algorithm, and is recorded and reported in the register as a failover and state-management result. Its timing does not feed the rehearsed time-to-change KPI. The estate's algorithm-change rehearsal is a key ceremony that generates a PQC-authorized key and retires it, or one of the three rehearsals of Activity 5.2 run on the HSM-backed signing service, timed across the four segments with the rollback exercised.

Settlement Performance Benchmarking

- **Signature verification throughput:** Benchmark ML-DSA at peak volumes. Use the Project Leap Phase 2 figure (7.5× on software verification, the one step it timed) as the software baseline. Test with hardware acceleration and with the HSM in the loop.
- **Certificate chain validation:** Test full PQC chain validation including OCSP/CRL with enlarged certificates.
- **Network bandwidth impact:** Model bandwidth increase from PQC signatures and certificates at peak volumes. Include archive storage growth projections.
- **End-to-end transaction timing:** Measure complete transaction lifecycle (authorization, clearing, settlement) with PQC at each stage.

Phase 7 – Vendor & Supply Chain Governance

Payment-Specific Vendor Classification

The Universal classifies vendors by PQC impact (Activity 7.1). The table below groups them by their role in the payments infrastructure; entities a reader deals with regardless of choice (the schemes, SWIFT, the domestic schemes, the RTGS operators, the wallet platforms cardholders choose) 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 reduces exposure only when the second vendor's product runs on a different firmware family:

Vendor Category	Examples	Engagement Approach

Vendor Category	Examples	Engagement Approach
Network operators	SWIFT, Visa, Mastercard, domestic schemes (ACH, SEPA, Faster Payments), central bank RTGS operators	Strategic C-suite engagement through the counterparty pattern (Activity 7.6). Participate in forums and pilots. Align the roadmap to published timelines, each graded for firmness; the four certificate-authority questions to every scheme and network CA.
Payment HSM vendors	The payment HSM product lines (Tool and Vendor References)	The two agility questions and the firmness question first. Quarterly PQC roadmap reviews. FIPS 140-3 and PCI PTS HSM tracked as two certificate references per firmware family. Early PQC firmware access for lab testing.
Card and terminal vendors	Card manufacturers, secure-element silicon suppliers, terminal and PIN-pad manufacturers (Tool and Vendor References)	The second agility question (verifiers updatable in the field) first. Monitor PQC chip availability. Track EMVCo's position. Plan terminal replacement cycles and the enclosure of the populations that will not migrate.
Payment processors and gateways	Acquiring processors, issuer processors, payment gateways and payment-as-a-service providers (Tool and Vendor References)	PQC readiness questionnaires in the Universal's order. Message format testing. Hybrid TLS interoperability validation. Both halves of the roadmap disclosure for hosted services (Activity 7.7).
Digital wallet platforms	The handset and wallet platforms cardholders use, and regional wallets	Monitor platform PQC adoption. Coordinate certificate pinning updates; the credential migration question for device-bound

Vendor Category	Examples	Engagement Approach
		credentials.

HSM Concentration, the Profile's Sector Fields and the CCF Cross-Reference

Most of the sector runs on a small number of payment HSM product lines. The count of vendors an organization contracts with can overstate its diversity. Two acquirers that bought different products may run one firmware family, and two processors that source from separate vendors may verify with one implementation. The Universal's Activity 6.2 register makes the sharing visible per module. Two further questions belong to the Cryptographic Concentration Framework's Payments extension (CCFramework.org): how many distinct firmware families, implementations and key-generation designs execute beneath the sector's payment HSMs, and what one certification delay or one implementation flaw would reach.

That framework aligns to this framework's sector taxonomy and measures concentration per layer per service. This extension cross-references the CCF result in the Quantum Readiness Assessment and in alternative-sourcing decisions, and does not compute a concentration figure of its own. Organizations that keep the CBOM in the Applied Quantum CBOM Profile (v1.0-RC or later) record the payment context the CCF consumes in the Profile's financial-services fields: `fs:paymentContext` (swift, card-network, rtgs, ach, instant, correspondent, securities or none), `fs:interopConstraint` (whether changing the algorithm requires coordination with external parties) and `fs:crossBorder` (whether the usage involves counterparties in other jurisdictions), written here as shorthand for the fully qualified `appliedquantum:fs:*` names the Profile specifies.

The Financial Services Extension's Phase 3 subsection on multi-party dependency records the same three fields for the broader banking estate and cross-references the CCF's Financial Services extension. This extension does the same for the HSM-concentration question and the Payments extension of the CCF. The record stands without the Profile: an organization on plain CycloneDX records the same three facts in its own fields.

Questionnaire Order, the Certificate-Authority Questions and the One-Afternoon Test

The vendor PQC readiness questionnaire of Activity 7.2 enters the third-party risk management cycle the organization 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.

For a terminal or PIN-pad vendor the second agility question decides the migration path: the answer says whether the fleet follows an algorithm change by a terminal management campaign or by replacement. The four certificate-authority questions go to every issuer in the Phase 1 hierarchy map, the scheme CAs, the EMV CA hierarchies and the SWIFT PKI included, because an issuer that cannot issue on the roadmap's dates gates every Track B migration behind it (Activity 3.3).

The Universal's procurement clause (Activity 7.3) warrants configuration-driven algorithm change, and the acceptance test turns the clause into evidence: before a terminal, HSM or gateway product enters production, the organization's own team executes a rehearsed algorithm change on it, with the elapsed times recorded and the rollback exercised. 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: a public specification, published cryptanalysis, a standards-body track and a validated implementation. A product that fails the first two is excluded. Every cloud HSM, hosted payment and tokenization provider is asked for both halves of the roadmap disclosure (Activity 7.7).

Industry Coordination Forums

- **BIS Innovation Hub:** Central bank PQC experiments (Project Leap Phase 2, December 2025, and successors). Early insight into RTGS timelines.
- **EMVCo:** Its security position statement on quantum computing and EMV chip cryptography and its 2026 industry engagement on post-quantum cryptography. The source for any EMV specification change, none published at this edition.
- **X9 Accredited Standards Committee:** PQC in financial messaging (ISO 8583, ISO 20022 accommodation); the Post-Quantum Cryptography Financial Readiness Needs Assessment.
- **Swift PQC program:** Alliance Release 7.9 and 8.0 preparation. Sandbox and pilot participation as the programs open.
- **PCI SSC:** PCI PTS HSM v5.0 (May 18, 2026) and its evaluation program; monitor for standalone PQC guidance, none published at this edition.
- **Europol QSFF / FS-ISAC:** Cross-sector coordination and the January 2026 prioritization methodology; FS-ISAC's payment card guidance.

PAYMENTS REGULATORY ALIGNMENT MAP

Payment infrastructure answers to overlapping bodies, 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.

PCI PTS HSM v5.0 (May 18, 2026) is the product-evaluation type: the current major version of the standard a payment HSM firmware is evaluated against, now including post-quantum considerations, with the v4 Security Requirements open for new device security approvals until June 30, 2027 under the Council's twelve-month overlap between major versions (PCI SSC bulletin, March 2, 2026), whose effect reaches the organization as the certificate reference, with its version, in its Phase 6 register.

The Singapore Quantum-Safe Migration Handbook (CSA, GovTech and IMDA, July 16, 2026) is the dated national instrument: for owners of designated Critical Information Infrastructure, a migration plan to CSA by March 31, 2027, procurement of quantum-safe-ready systems from January 1, 2028, and completion by December 31, 2031. The handbook is guidance, and the dates it states for CII owners are requirements it reports rather than requirements it creates.

For each CII date the organization records the operative provision or written direction under the Cybersecurity Act that imposes it, and the class of owner bound by it. That record, not the handbook's own status, sets the enforcement tier the Dimension 4 factor reads. Two supervisory instruments are announced and not issued at this edition and are recorded as verify-first items rather than rows. MAS stated at its Annual Report FY2025/2026 media conference (July 28, 2026) that it will issue supervisory expectations later in 2026 with progressive timelines toward quantum resilience before the end of the decade.

The ECB's Supervisory Board pre-announced a quantum-specific letter to significant institutions alongside its July 7, 2026 letter on AI-enabled cyber threats (action plans

due October 31, 2026). Neither the MAS expectations nor the ECB letter had published when checked in September 2026. Jurisdiction rows that repeat the Universal's roster (NIST IR 8547, the EU coordinated roadmap, the G7 Cyber Expert Group 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 Financial Services Extension covers the banking supervisors (DORA, FINMA, HKMA). The instruments that bind a given organization are recorded in its Regulatory Horizon Report (Universal, GRC Implementation).

The table is a dated snapshot of the sector bodies and the one national instrument that sets a sector date, 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 organization before planning against a row.

Instrument	Requirement and dates	Status at this edition (enforcement tier)	Framework phases and payments 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 evidence as attestations and scoped extracts. PCI SSC had published no standalone PQC guidance at this edition; re-checked at each release.
PCI PIN Security (PCI SSC)	PIN block encryption and DUKPT key management requirements; TDEA phase-out on the Council's schedule	In force (tier 1: PIN security assessments are a condition of processing PIN transactions)	Phase 1 and Phase 6: symmetric material inventoried under symmetric key management; the TDEA-to-AES key hierarchy work at the terminal and HSM layers is scheduled with the PQC

Instrument	Requirement and dates	Status at this edition (enforcement tier)	Framework phases and payments implication
			migration, not after it.
PCI PTS HSM v5.0 (PCI SSC, May 18, 2026)	Modular Security Requirements for payment HSMs, revised from v4.0: post-quantum cryptography considerations and definitions; device-security keys of at least 128-bit effective strength; TDES no longer permitted for device security; new modules for key transfer, remote administration and HSM-as-a-service; the v4 Security Requirements open for new device security approvals until June 30, 2027, the v4 device approval expiration extended to April 2033 and the v3 expiration to April 2028 (PCI SSC bulletin, March 2, 2026)	Published; new evaluations run against v5.0 or, until June 30, 2027, v4 (tier 1: an approved device is a scheme and PCI PIN condition of use)	Phase 6 and Phase 7: the second certificate reference in the Activity 6.2 register; a PQC firmware that breaks the approval is not deployable until re-evaluated; the vendor questionnaire asks for the version each approval sits under, the v5.0 evaluation date and its firmness grade.
Swift Customer Security Programme and Alliance Release 8.0 / SwiftNet 8.0 (Swift)	Release 7.9 as the foundation for 8.0 and PQC readiness, needed by the majority of the community because	Announced (firmness grade: announced; the participant PQC requirement and its date unknown) (tier 1 once mandated for	Phase 5 and Phase 7: the SWIFT pilot and the counterparty pattern; the dates set the delivery state of every SWIFT-

Instrument	Requirement and dates	Status at this edition (enforcement tier)	Framework phases and payments implication
	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	the community: a market-access gate on the network)	dependent Tier-1 entry.
EMVCo security position statement on quantum computing and EMV chip cryptography and the January 30, 2026 statement of its Board of Managers chair	No practical threat to the EMV infrastructure expected before 2040, maybe never, an assessment reasoned from offline data authentication and the chip's own cryptography; industry engagement on post-quantum cryptography through 2026; no specification change and no date published	Published position; no instrument (tier 5, advisory; a specification change would bind at tier 1 through the schemes)	Phase 4 and Phase 5: every EMV specification date graded unknown; offline data authentication sits in Tier 1 under the ordered test with the delivery state blocked on the refresh cycle; the HNDL exposure of the transaction channel is unaffected by the statement.
Singapore Quantum-Safe Migration Handbook, Version 1.0 (CSA, GovTech, IMDA, July 16, 2026)	For CII owners: quantum-safe migration plan to CSA by March 31, 2027; new CII systems procured from January 1, 2028 to support quantum-safe algorithms or be quantum-safe ready; migration complete	Published as CSA's requirements for CII owners; the Handbook's own disclaimer states it is not mandatory or prescriptive, and no Code of Practice or written direction under the Cybersecurity Act	Phase 0, Phase 4 and Phase 7: the plan-by, procure-by and migrate-by dates for CII-designated payment system operators; the Phase 7 procurement clause satisfies the 2028 procure-by date.

Instrument	Requirement and dates	Status at this edition (enforcement tier)	Framework phases and payments implication
	and vulnerable cryptography out of use by December 31, 2031	setting the dates was found at this edition (tier 4 until such an instrument issues, then tier 3)	
BIS Innovation Hub, Project Leap Phase 2 report (December 11, 2025) and BIS Papers No. 158 (July 2025)	Post-quantum signatures on T2 liquidity transfers tested with the Eurosystem central banks, Nexi-Colt and Swift; the quantum-readiness roadmap for the financial system	Published (tier 5, advisory; the authors' views, not necessarily the BIS's)	Phase 0 and Phase 6: the settlement-system evidence for the business case and the benchmarking method; RTGS operators' own dates through the counterparty pattern.
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); FS-ISAC payment card guidance	Prioritization methodology scoring quantum risk against migration time; the payment card impact analysis that states it is not known whether EMV can accommodate quantum-safe certificates	Published (tier 5, advisory)	Phase 3 and Phase 7: cross-reference the Phase 3 outputs for supervisory defensibility; the coordination channel.
FIPS 140-2 to the CMVP Historical list (NIST CMVP)	Every remaining FIPS 140-2 certificate moved to the Historical list on September 21, 2026; CMVP supports the purchase and use of Historical modules for existing systems and recommends	Past event (the maintained prose of the CMVP transition page; its 2021 table prints September 22, 2026) (tier 1 where a scheme, supervisor or contract requires currently validated modules for new	Phase 6: the FIPS 140-3 and PQC refresh of the HSM estate planned as one.

Instrument	Requirement and dates	Status at this edition (enforcement tier)	Framework phases and payments implication
	that purchasers consider modules validated against either standard while the FIPS 140-3 selection is limited	systems, an exclusion that follows from CMVP's scoping to existing systems and from that policy, not from a CMVP prohibition)	

Enforcement tiers the Universal does not assign are recorded here as this extension's reading, by who enforces. PCI DSS 12.3.3, PCI PIN Security and PCI PTS HSM v5.0 are tier 1. Swift release 8.0 is tier 1 from the date a published participant requirement names and not before, so the July 2027 availability date scores no Dimension 4 deadline. The EMVCo position is tier 5. The Singapore Handbook's general guidance is tier 4, with the CII requirements it reports tagged at the tier of the operative provision or direction that imposes them on the designated owner, recorded per organization.

The BIS, Europol and FS-ISAC publications are tier 5. The CMVP Historical move is tier 1 where scheme, supervisory or contractual policy requires currently validated modules for new systems. The June 2026 edition's "EMVCo Quantum Working Group", "PCI PTS HSM v4" and "SwiftNet 8.0, target around 2027, 12-to-18-month window" rows are replaced by the rows above, and its NIST IR 8547, EU coordinated roadmap and G7 rows by the pointer.

PCI SSC had published no standalone PQC guidance when checked in September 2026. Requirement 12.3.3 mandates cryptographic documentation (which surfaces quantum vulnerability) but does not mandate remediation. Payment organizations should anticipate that PCI SSC PQC guidance will follow and build their processes to produce the evidence artifacts that future requirements will demand.

PAYMENTS 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 payment infrastructure indicators are read beside them.

Level	Universal Level	Payment Infrastructure 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	No inventory of payment HSMs, card platforms, or message format cryptographic dependencies. No engagement with SWIFT, the card networks or EMVCo on quantum readiness. PCI 12.3.3 compliance may be ad hoc.
2	Initiated: formal program chartered; budget allocated; discovery underway; initial CBOM in development	Charter states both outcomes; Crypto-Agility and Cryptographic Record owners named. Payment HSM estate in the four-field register with both certificate references. Message formats analyzed for PQC payload constraints. SWIFT release level and card network readiness assessed; readiness inquiries issued.

Level	Universal Level	Payment Infrastructure Indicator
		Terminal and ATM fleets inventoried with verifier updatability recorded. Tokenization coverage quantified. Priority A inventory complete with evidence grades and a stated denominator; accepted-gaps register signed. Initial QRA produced.
3	Progressing: CBOM operational; risk scoring complete; hybrid pilots in production; vendor engagement active; KPIs reported	Scoring model ratified with the payment factors; agility-debt register produced with the terminal, ATM, credential and scheme-interface entries. External dependency timeline map maintained with firmness grades (Swift release 8.0, the card networks, the HSM vendors, the central banks). Year-1 plan in execution. HSM vendor PQC reviews quarterly, agility questions answered. Industry forum participation active. First algorithm-change rehearsal run on the external payment API gateway and timed; first quarterly HSM-partition failover run and recorded as a failover and state-management result.
4	Advanced: Tier-1 systems migrated to hybrid/PQC; PKI modernized; crypto-agility demonstrated; vendor commitments secured	Hybrid key exchange deployed on Tier-1 systems (external payment APIs, acquirer and host-to-host links) with the negotiated outcome observed; SWIFT and scheme interfaces pass

Level	Universal Level	Payment Infrastructure Indicator
		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. Payment HSM PQC operations in validated or risk-accepted mode per product, both certificate references recorded. Terminal and ATM populations classified as refresh, enclosure or exception with dates. Firmware signing on SP 800-208 from the HSM-backed service. Two results in every gate and wave-exit record. An algorithm change rehearsed on the gateway and on the internal issuer inside the agility window. Settlement performance benchmarked with the HSM in the loop.
5	Optimized: estate-wide PQC migration substantially complete; crypto-agility is organizational capability; continuous monitoring and posture management operational	All payment channels quantum-safe or hybrid; every scheme, network and SWIFT interface has followed its network or has a SteerCo-signed exception. Payment HSMs validated under FIPS 140-3 and PCI PTS HSM with PQC in approved mode. Card platforms PQC-capable; enclosed terminal populations on bridge end dates or signed exceptions with re-evaluation dates. Full

Level	Universal Level	Payment Infrastructure Indicator
		CBOM exchange with network operators and Tier 1 vendors. Standing rehearsal cadence on the gateways, the issuers and the signing services, with the quarterly HSM-partition failover recorded beside it as a failover exercise; 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.

PAYMENTS KPI SUPPLEMENT

The Universal Framework defines board-level, operational, agility and evidence-dossier KPIs (Metrics, KPIs & Reporting). The following additional KPIs are recommended for payment organizations, supplementing the Universal Framework and Financial Services Extension KPIs.

Board-Level KPIs (Quarterly)

- **Payment HSM PQC readiness:** Percentage of payment HSMs with PQC-capable firmware installed and the certificates (FIPS 140-3 and PCI PTS HSM) that cover the operation / total payment HSM estate. Track validated, risk-accepted and non-approved capability as separate lines.
- **External payment interface quantum exposure:** Number of external payment interfaces (SWIFT, card network, payment APIs, acquirer and host-to-host links) operating without hybrid or PQC key establishment observed / total external interfaces, with the incidental line reported separately (Universal, enforcement counting rule).
- **Settlement PQC performance baseline:** PQC signature verification latency as a multiple of the classical baseline, with the HSM in the loop (target: a multiple that fits inside the scheme's authorization and settlement latency budget for that system, set from the benchmark; hardware acceleration narrows the multiple, and no overhead-free target is assumed for new hardware).
- **HNDL data-at-risk volume:** Payment data in transit across external interfaces whose confidentiality horizon, read as the attacker's horizon, exceeds 10 years, not yet protected by hybrid or PQC key exchange or tokenized. The risk-weighted companion to Coverage.
- **Terminal and ATM fleet disposition:** Share of the terminal, PIN-pad and ATM estate classified as refresh on a dated roadmap, enclosure with a bridge end date, or exception signed by the SteerCo, with the unclassified share reported as its own line.

Operational KPIs (Monthly)

- **Payment vendor PQC roadmap alignment:** Critical payment vendors (HSM, terminal, processor, gateway) with dated PQC roadmaps, by firmness grade / total critical payment vendors. A date graded unknown does not count.
- **Counterparty readiness:** Share of scheme, SWIFT, RTGS and correspondent 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).
- **Message format PQC readiness:** Payment message formats analyzed for PQC accommodation / total formats in active use.
- **Tokenization coverage:** Percentage of high-sensitivity payment data categories protected by tokenization.
- **Card/terminal fleet PQC readiness:** Percentage of estate with PQC-capable hardware and updatable verifiers / total estate. Long-term fleet turnover metric.

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 organization controls, and the terminal fleets and the scheme-set interfaces whose algorithm the network sets are reported beside them, never inside them.

KPI	Payments measurement	Threshold
Configuration-driven share	Percentage of Tier-1 and Tier-2 systems (the external payment API gateway, the acquirer and host-to-host endpoints, the internal payment service mesh, the internal issuers, the firmware-signing service, the payment HSM estate) whose key-establishment and signature algorithms change by configuration, verified by rehearsal; the terminal and ATM fleets and the scheme, SWIFT and RTGS 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	Inside the agility window; a

KPI	Payments measurement	Threshold
	assessment, decision, change and verification on the most recent rehearsal, per track: on the external payment API gateway for Track A, on the firmware-signing service or the internal issuer for Track B, and on a key ceremony generating a PQC-authorized key, or a rehearsal on the HSM-backed signing service, for the payment HSM estate (Activity 5.2; the quarterly HSM-partition failover is reported beside this KPI and does not feed it), scheduled outside the change advisory board's freezes	rehearsal whose change segment cannot run without a terminal firmware release, a scheme cutover or a Swift release 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 terminal and ATM, the enrolled-credential and the scheme-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 terminal, HSM and gateway procurements 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 payment organizations 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 10 are the sector's inventory, coordination and pilot actions; actions 11 and 12 are its agility actions.

#	Action	Timeline	Phase
1	Map the complete payment HSM estate into the four-field register with both certificate references (FIPS 140-3 and PCI PTS HSM) and the vendor PQC roadmap graded for firmness. Initiate vendor engagement on PQC firmware and certification timelines, agility questions first.	0–3 months	Phase 1/6/7
2	Inventory all payment message formats (ISO 8583, ISO 20022, SWIFT MT/MX, domestic formats) and map field-level cryptographic dependencies.	0–3 months	Phase 1
3	Conduct the tokenization	0–3 months	Phase 3/5

#	Action	Timeline	Phase
	coverage assessment to quantify which payment data is already quantum-defended.		
4	Assess the SWIFT interface's path to Alliance Release 7.9 and 8.0 and its readiness for release 8.0 requirements as Swift publishes them. Register for Swift's PQC pilot and sandbox programs as they open.	0–6 months	Phase 5/7
5	Inventory the card and terminal estate by chip generation, RAM capacity, PQC feasibility, verifier updatability, and replacement cycle, and record who can change each population's cryptography.	0–6 months	Phase 1/4
6	Inventory the ATM fleet by model, RKL protocol version, and PQC hardware feasibility.	0–6 months	Phase 1
7	Structure the PCI 12.3.3 cryptographic inventory to simultaneously produce the PQC readiness assessment, with	0–3 months	Phase 1/2

#	Action	Timeline	Phase
	evidence grades and the denominator stated before the tools run.		
8	Follow the coordination forums relevant to the organization's role and join those it is eligible for: the BIS Innovation Hub's published experiments and their successors (participation runs through the central banks and operators that join them), EMVCo's industry engagement, X9, Swift's PQC program, FS-ISAC and the Europol Quantum Safe Financial Forum; name an owner who reads each forum's output into the external dependency timeline map.	0–3 months	Phase 0/7
9	Enable hybrid key exchange (X25519MLKEM768) on at least one external payment API endpoint, and count it toward Coverage only once the negotiated outcome is observed and the policy is tested.	3–9 months	Phase 5

#	Action	Timeline	Phase
10	Replicate the BIS Project Leap Phase 2 settlement benchmarking on the organization's own infrastructure, with the HSM in the loop.	3–9 months	Phase 6
11	Name a Crypto-Agility workstream owner in the function that controls the payment gateways, the HSM estate and the firmware-signing pipelines, with a budget line from Year 1 and the agility-debt register as scope; name the Cryptographic Record owner beside it.	0–1 month	Phase 0
12	Schedule the first rehearsal on the pilot endpoint of action 9 (change the key-establishment parameter set by configuration, time the four segments, roll it back) and file its timings as the first agility KPI reading and the first entry in the closure evidence; run the first quarterly failover to the backup HSM partition in the same period and record it as a failover and state-management	3–9 months	Phase 5/6

#	Action	Timeline	Phase
	result, outside the KPI.		

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.
- **BIS Project Leap Phase 2 – https://postquantum.com/security-pqc/bis-leap-2-pqc-payments/ –** Analysis of the first real-world PQC test on production payment settlement infrastructure.
- **The Cryptographic Iceberg Inside a Mobile Banking Transaction – https://postquantum.com/post-quantum/cryptography-cbom-mobile-banking/ –** Layer-by-layer reconstruction of ~320 cryptographic function calls 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 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.
- **Evaluating Tokenization in the Context of Quantum Readiness – https://postquantum.com/post-quantum/tokenization-quantum-readiness/ –** Tokenization as scope-reducer and blast-radius limiter.
- **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.
- **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.

- **Singapore Tells Its Critical Infrastructure to Finish Quantum-Safe Migration by 2031 – https://postquantum.com/security-pqc/singapore-cii-quantum-safe-milestone/ –** The CSA Handbook's three CII milestones and the question of their legal footing under the Cybersecurity Act.
- **MAS Targets Quantum Resilience for FIs by End of Decade – https://postquantum.com/security-pqc/mas-quantum-resilience-supervisory-expectations/ –** The July 2026 announcement of supervisory expectations with progressive timelines, read against the 2024 advisory.
- **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.
- **BIS Project Leap Phase 2 report – https://www.bis.org/publ/othp107.htm –** The primary source (December 11, 2025) for every Project Leap figure and finding this extension cites.

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 Payments Requires Its Own Extension, Hardware Fleet with Decade-Long Replacement Cycles.* It must be physically manufactured, distributed, certified, and installed, creating migration timelines that are constrained by logistics and certification bureaucracy.
2. *Payment-Specific Challenges, Archive and Storage Multiplication.* Organizations must model this storage impact during Phase 6 capacity planning.
3. *Payment-Specific Challenges, Archive and Storage Multiplication.* Framework Impact: Phase 1 (Discovery) must include message format analysis as a distinct inventory track, identifying every fixed-size field carrying cryptographic data.
4. *Payment-Specific Challenges, Archive and Storage Multiplication.* Phase 3 (Risk Scoring) must weight message-format-constrained systems separately.
5. *Payment-Specific Challenges, Archive and Storage Multiplication.* Phase 5 (Pilots) must include message-format-specific testing with realistic payload sizes.
6. *Payment-Specific Challenges, Archive and Storage Multiplication.* Phase 6 (Infrastructure) must model archive storage growth.
7. *Payment-Specific Challenges, The Double Certification Problem.* Payment HSMs must satisfy two independent certification regimes.
8. *Payment-Specific Challenges, Payment HSM Vendor Concentration.* Framework Impact: Phase 6 (Infrastructure) must include HSM certification tracking as a gating dependency, with FIPS 140-3 and PCI PTS HSM recorded as two certificate references per module in the Activity 6.2 register.

9. *Payment-Specific Challenges, Payment HSM Vendor Concentration.* Phase 7 (Vendor Governance) must establish structured quarterly engagement with HSM vendors on certification timelines and early access to PQC firmware for lab testing, with the two agility questions asked first and every date graded for firmness.

10. *Payment-Specific Challenges, Terminal Fleet Scale and the Mastercard Ecos Approach.* Framework Impact: Phase 4 (Roadmap) must incorporate hardware refresh cycles for cards and terminals as hard constraints on migration timelines, with each population's delivery state recorded.

11. *Payment-Specific Challenges, Terminal Fleet Scale and the Mastercard Ecos Approach.* Phase 5 must include a triage strategy separating online authentication (protectable with symmetric cryptography now) from offline data authentication (dependent on asymmetric PQC on constrained hardware), with enclosure per the OT extension's Encapsulate Strategy for the populations that will never migrate natively.

12. *Payment-Specific Challenges, Terminal Fleet Scale and the Mastercard Ecos Approach.* Phase 1 must inventory the card and terminal estate by chip generation, RAM capacity, PQC feasibility and verifier updatability.

13. *Payment-Specific Challenges, BIS Project Leap Phase 2 Performance Data.* RTGS systems (T2, Fedwire, BOJ-NET, CHAPS), real-time payment networks (FedNow, TIPS, Faster Payments, UPI), and high-frequency trading venues all operate within tight latency budgets where PQC overhead must be engineered out through hardware acceleration or architectural changes.

14. *Payment-Specific Challenges, Certificate Chain Overhead and Hardware Acceleration.* However, hardware-accelerated PQC modules must themselves pass FIPS 140-3 validation and PCI PTS HSM evaluation before production deployment on a payment HSM, so the certification dependency of Challenge 2 sits on the performance optimization path as well.

15. *Payment-Specific Challenges, Certificate Chain Overhead and Hardware Acceleration.* Framework Impact: Phase 6 (Infrastructure) must include settlement-system-specific performance benchmarking.

16. *Payment-Specific Challenges, SWIFT Alliance Architecture and PQC Readiness.* For institutions using Alliance Gateway in a high-availability configuration, the PQC migration must be coordinated across primary and backup sites.

17. *Payment-Specific Challenges, SwiftNet 8.0 Migration Planning.* Alliance Release 7.9 lays the foundations for release 8.0 and PQC readiness and must be deployed by the majority of the community, because there is no upgrade path from release 7.7 to 8.0.

18. *Payment-Specific Challenges, SwiftNet 8.0 Migration Planning.* The institution's SWIFT-facing HSMs must generate and use PQC keys within the validated boundary by the time release 8.0 requires them, on the certificate date of the module that

covers them; and the message-handling systems must process PQC-signed ISO 20022 messages with enlarged signature payloads.

19. *Payment-Specific Challenges, SWIFT PKI and Certificate Management.* The transition from classical to PQC certificates in SWIFT's PKI requires coordinated action: SWIFT must update its root and intermediate CA certificates to PQC, member institutions must deploy the new PQC certificates on their Alliance infrastructure, and message verification logic must be updated to handle PQC signatures.

20. *Payment-Specific Challenges, SWIFT PKI and Certificate Management.* Certificate provisioning at every counterparty must therefore be sequenced before – not after – production deployment of the PQC signature.

21. *Payment-Specific Challenges, The Correspondent Banking Chain.* Framework Impact: Phase 0 (Executive Mandate) must establish cross-industry coordination mechanisms from the outset.

22. *Payment-Specific Challenges, The Correspondent Banking Chain.* Phase 4 (Roadmap) must map SWIFT, card network, domestic scheme, and central bank timelines as hard constraints, each graded for firmness, with the delivery state of every dependent entry read from them.

23. *Payment-Specific Challenges, The Correspondent Banking Chain.* Phase 7 must include strategic-level engagement with SWIFT on the release 8.0 requirements and timeline through the counterparty pattern.

24. *Payment-Specific Challenges, PCI PIN Security and DUKPT Key Hierarchy.* Organizations must track the intersection of PCI's TDEA deprecation timeline with their PQC migration timeline, as both require key hierarchy updates at the terminal and HSM layers.

25. *Payment-Specific Challenges, PCI Point-to-Point Encryption (P2PE).* Framework Impact: Phase 1 (Discovery) must include PCI-scoped systems as a priority inventory track, structured to satisfy both PCI 12.3.3 and PQC readiness.

26. *Payment-Specific Challenges, PCI Point-to-Point Encryption (P2PE).* Phase 3 (Risk Scoring) must score PCI and scheme requirements at enforcement tier 1 on Dimension 4 and the attacker's horizon on Dimension 1.

27. *Payment-Specific Challenges, PCI Point-to-Point Encryption (P2PE).* Phase 7 (Vendor Governance) must include 3DS network providers and P2PE solution providers in vendor PQC readiness assessment.

28. *Payment-Specific Challenges, Continuous Availability and Migration Windows.* PQC migration for RTP must be executed through rolling upgrades with hybrid cryptography, maintaining backward compatibility throughout the transition.

29. *Payment-Specific Challenges, Latency Sensitivity at Scale.* Phase 6 (Infrastructure) must include RTP-specific hardware acceleration planning.

30. *Payment-Specific Challenges, Challenge 9: Mobile and Digital Wallet Cryptography.* Framework Impact: Phase 1 must include mobile payment app cryptographic dependencies as a distinct inventory track.

31. *Payment-Specific Challenges, Challenge 9: Mobile and Digital Wallet Cryptography.* Phase 5 must coordinate server-side PQC deployment with mobile app update cycles.

32. *Payment-Specific Challenges, Challenge 9: Mobile and Digital Wallet Cryptography.* Phase 7 must include mobile platform vendors as dependencies for SE/TEE PQC support.

33. *Payment-Specific Challenges, Challenge 10: ATM Network Security and Remote Key Loading.* Framework Impact: Phase 1 (Discovery) must include ATM network cryptographic dependencies and RKL protocol versions.

34. *Payment-Specific Challenges, Challenge 10: ATM Network Security and Remote Key Loading.* Phase 4 (Roadmap) must incorporate ATM replacement cycles as hardware constraints.

35. *Alignment with Universal Framework v3.0, Algorithm Weighting and the EMV ECC Transition.* Payments must read this against its own modernization path.

36. *Alignment with Universal Framework v3.0, SP 800-208 Firmware Signing as the Deploy-Now Track B Action.* The firmware update verification keys provisioned into hardware shipping today must survive into the CRQC era, and a terminal whose verifier cannot follow an algorithm change is the clearest agility-debt entry in the sector.

37. *Alignment with Universal Framework v3.0, SP 800-208 Firmware Signing as the Deploy-Now Track B Action.* A signing service that does not meet section 8 is not a conforming deployment, and the terminal and ATM verifiers must accept the parameter set chosen.

38. *Phase 0 adaptation, Governance Adaptation for Payments.* Payment PQC governance must include representation from acquiring, issuing, terminal management, payment HSM operations, SWIFT administration and settlement, in addition to IT security and compliance.

39. *Phase 4 adaptation, External Dependency Timeline Map.* Payment roadmaps must incorporate external timelines that the organization does not control.

40. *Phase 5 adaptation, Hybrid Architecture Planning.* The hybrid period will last years and must be managed as a sustained operational state.

41. *Phase 6 adaptation, Payment HSM Modernization Strategy.* - Dual-key management: During hybrid transition, HSMs must manage both classical and PQC key material.

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