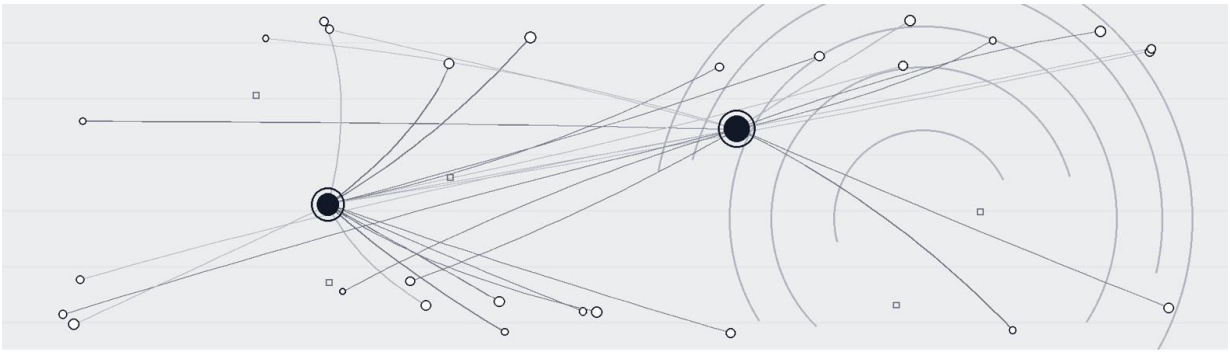
AUGUST 2026

APPLIED QUANTUM

THE APPLIED QUANTUM CRYPTOGRAPHIC CONCENTRATION FRAMEWORK

FINANCIAL SERVICES EXTENSION



Banking, capital markets and insurance

Version 1.0-RC – August 2026

Steve Vaile and Marin Ivezic, Applied Quantum

Disclosure: Applied Quantum provides post-quantum migration advisory services. This work is published openly under CC BY 4.0 and is computable without engaging Applied Quantum.

"Switching vendors moves the contract, not the dependency."

COPYRIGHT AND LICENSE

DISCLAIMER

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

The regulatory instruments, certification records, standards and vendor capabilities referenced in this document reflect the state of the landscape as of August 2026, and that landscape moves. Readers should verify current status against primary sources (regulators and supervisory authorities, NIST, EMVCo and PCI SSC, the CycloneDX specification, public certification listings, vendor documentation) before making decisions.

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

This is a v1.0 release candidate: v1.0 final publishes in November 2026 after a pilot cycle. Open items are public on the roadmap at CCFramework.org, and corrections are published as dated entries on its errata page.

ABOUT THIS DOCUMENT

Document type	Sector extension to the CCF Universal Framework
Parent document	The Cryptographic Concentration Framework – Universal – v1.0-RC (August 2026)
Intended audience	Risk analysts assessing banking, capital markets and insurance services, and the infrastructure specialists supplying them with data
Assumed knowledge	The Universal Framework and its phase definitions; familiarity with the institution’s service architecture
Scope	Banking, capital markets and insurance enumerations, the sector consequence-threshold template, and the correspondent-banking worked example. Banking is practitioner-tested; capital markets and

	insurance validate toward v1.0 final, and the document states this on its face. Not a standalone document.
Status	Version 1.0-RC – release candidate; v1.0 final November 2026 after pilot

VERSION HISTORY

Version	Date	Changes
1.0-RC	August 2026	First public release, as a release candidate; drafted through four external review rounds and a family-wide line-edit pass.
1.0-RC	7 September 2026	Cloud-collapse note aligned to the Universal's cloud-custody determination; FS.7 layer 6 profile-node known reach corrected to 15.4% per Universal A.4, tolerance label corrected.
1.0-RC	8 September 2026	FS.7 layer-2 OpenSSL bound includes the undisclosed cloud-library assets, 41.5% in place of 33.8%; the largest failure domain reported per layer including standalone units, the service's largest being the mainframe generation design at 71.5%; the unresolved cloud boundary counts as one unit at its known population. Prose revised throughout. No index, band or flagged-only figure changed.

HOW TO USE THIS DOCUMENT

This document is a companion to the CCF Universal Framework. It does not replace it: for each service family it enumerates what to examine and maps the findings onto the Universal's phases, units and determinations. Readers should have the Universal Framework open alongside this document and cross-reference its phase definitions, evidence standards and templates.

ACCOMPANYING RESOURCES

The framework family publishes at CCFramework.org: the Universal Framework, the Payments and Financial Services extensions, the payments whitepaper, the CBOM Conformance Statement, the Technical Companion and the instruments, together with the public roadmap, the errata and corrections page, the provenance survey and the frontier-census methodology.

Every canonical figure in the family comes from the reference implementation, with ten canonical test vectors that fix each one exactly. Both are open under Apache-2.0 on the Applied Quantum GitHub, and any implementation that reproduces the fixtures is conformant.

The Applied Quantum CBOM Profile, the input data contract, publishes at CBOMProfile.org. The Applied Quantum PQC Migration Framework, whose sector taxonomy the extensions follow,

publishes at PQCFramework.org. Practitioner background and adjacent analysis sits on PostQuantum.com, as further reading rather than a normative source.

TABLE OF CONTENTS

Requires the CCF Universal Framework **v1.0-RC.** This extension names what to enumerate at each of the six layers. It does not restate the computation, the interpretation bands, or the reporting rules, which are defined in the Universal Framework.

Relationship to the Payments extension. Payment services are assessed under the Payments extension. An institution operating both runs each extension against its own service list rather than merging them, because the counterparty classification differs – the classes are the same everywhere; the membership is not.

FS.1 SERVICES IN SCOPE

This extension applies the Universal Framework to banks, insurers, market infrastructure and related financial-service functions. It identifies where to look for relevant cryptographic dependencies and how to connect them to service ownership, tolerances, counterparties and existing risk processes. It does not prescribe a financial-sector weighting different from the Universal method.

Banking. The scope includes deposit-taking and account servicing; lending origination and credit decisioning; correspondent banking; treasury and liquidity management; customer authentication and digital channels; and data-at-rest protection and backup.

Capital markets. The scope includes trading and market access; custody and safekeeping; post-trade processing and settlement instruction; and collateral management.

Insurance. The scope includes policy issuance and contract execution; claims settlement authorisation; and long-term document retention and archive.

Scope status at v1.0-RC. The banking service list and its enumerations are practitioner-tested. The capital-markets and insurance lists are scoped and published for use, with practitioner validation completing at v1.0 final. This work is tracked at ccframework.org/roadmap. Findings against those two lists carry that status until then.

Start from the institution's approved service or critical-function taxonomy. Retail payment execution, treasury operations, settlement submission, trading, custody, customer authentication and regulatory reporting can share technology while remaining distinct assessment services. Map the chosen scope to applicable legal definitions; DORA's critical or important functions and the UK important-business-service taxonomy should not be treated as identical merely because both support operational-resilience work.

A shared HSM, PKI service or mainframe cryptographic facility is counted in every service it supports under the Universal rule. Within each service, de-duplicate the

persistent assets and declare the counted classes. An unallocated infrastructure service inherits the most stringent relevant supported-service tolerance where a defensible mapping exists, or is `NOT MAPPED`.

FS.2 WHAT TO ENUMERATE AT EACH LAYER

Commercial product names and contractual legal entities are retained as context, not used indiscriminately as cryptographic units. A shared ancestor does not collapse distinct executing families in the CCI; it creates a reach domain. A common manufacturer does not automatically establish one firmware family, and a managed service does not reveal its underlying module merely through its provider name.

Layer 1 – Algorithm

Enumerate quantum-vulnerable public-key material: RSA and elliptic-curve material in enterprise TLS, code signing, document and contract signing, customer authentication, correspondent messaging and key wrapping over symmetric estates. Exclude symmetric material at adequate key length from the layer-1 denominator and report it in the estate profile.

Wrapped estates. Database and backup encryption are symmetric at rest and frequently use asymmetric keys to wrap the data keys. Those wrapping keys belong in layer 1 and bring the otherwise-symmetric estates into scope. Their compromise retroactively exposes everything wrapped beneath them.

A layer-1 baseline of 10,000 describes the concentration of the remaining specified public-key class. It does not determine the probability of a quantum attack or imply that every sound hybrid loses confidentiality when its classical component is broken. Coverage and scenario consequences retain that distinction.

Layer 2 – Implementation lineage

Identify the executing families and resolve their relevant code to upstream ancestors. Enumerate core banking platform cryptographic modules; mainframe cryptographic services, including z/OS ICSF and the Crypto Express family; and Java Cryptography Extension providers across application estates.

Include TLS stacks on customer channels, branch connectivity, interbank links and vendor integrations; database transparent data encryption modules; backup and archive encryption; trading platform and market gateway cryptographic modules; HSM firmware modules; and cloud provider libraries where key operations execute in the provider's environment. Browser/mobile integrations and vendor platforms also remain within the selected service scope.

Mainframe concentration. One cryptographic facility on one hardware family commonly serves dozens of services. It therefore appears as a single dependency across a large share of the service inventory. That is an accurate reading of the shared dependency, not an artefact of the calculation.

Layer 3 – Trust root

Enumerate internal enterprise certificate authorities and their hierarchy; public web PKI roots on customer channels; code-signing roots; document-signing and qualified trust service provider roots where a qualified regime applies; and the relevant verifier trust stores.

Include SWIFT PKI; central bank and market infrastructure PKI, including central securities depositories and central counterparties; and correspondent bank PKI. Resolve the roots and policies accepted for the relevant service function.

Qualified trust service providers. A qualified trust service provider appears at this layer and again in the counterparty classification. Recording the same object in the trust-root and counterparty views is expected: the views describe different aspects of the dependency.

Layer 4 – Key custody platform

Enumerate general-purpose hardware security modules, payment HSMs within the selected service scope, mainframe cryptographic coprocessors, cloud key management and cloud HSM services, and enterprise key management systems. Include cryptographic modules embedded in core banking and trading platforms, and customer authentication devices and tokens issued by the institution. Resolve custody platforms to firmware family.

Cloud boundaries. Where key generation or key operations execute in a cloud provider's environment and the underlying module is undisclosed, layers 2, 4 and 6 meet the same unresolved boundary. Apply the Universal Framework's cloud-custody determination: count the boundary as one primary unit at its known population and carry its uncertainty in reach. The provider's identity is never written into the lineage, firmware-family or generation fields. Second line computes the reach bounds. One cloud relationship can therefore produce three simultaneous bounded readings that a vendor-layer assessment does not surface.

Layer 5 – Protocol and negotiation

Record the TLS protocol, version and key-establishment group negotiated on customer channels, branch links, interbank connections and vendor integrations. Include IPsec negotiated proposals on branch and site connectivity, SSH negotiated key exchange on administrative and file-transfer paths, and database and backup transport encryption as negotiated per connection.

For authentication and federation, record the TLS beneath OAuth, OpenID Connect and SAML exchanges, and the authenticator algorithms negotiated in FIDO ceremonies. Identify what is selected and enforced in operation, including fallback behaviour.

Messaging and authentication context. For SWIFT and FIX messaging, ISO 20022, message-oriented middleware and strong-customer-authentication flows, record the security profile negotiated per path and map the relevant dependencies to layers 2 to 4. A message standard or authentication framework is context, not a dependency unit.

Layer 6 – Key generation: entropy source and generation design

Enumerate hardware random number generators in each custody platform and generation-algorithm designs used outside a custody platform, including application-side and mainframe key generation. Include mainframe entropy sources, cloud provider entropy, server-side entropy in application key generation, and random number generation in issued customer authentication devices.

Trace central key ceremonies, platform generators, issued credentials, managed services and imported keys to the point that produced the material. Record the entropy-source design, generation design and certification profile. Current custody does not by itself establish generation origin.

FS.3 COUNTERPARTY CLASSIFICATION

Class	Members
Blocking	SWIFT; central bank rails and RTGS operators; central securities depositories; central counterparties; automated clearing house operators; qualified trust service providers; regulators mandating specific formats
Contractual	Corporate and institutional clients; third-party providers under open banking access; vendors and outsourced processors; syndicate participants under agreement
Peer	Correspondent banks; bilateral trading counterparties; other institutions on shared market infrastructure
Population	Retail customer endpoints; issued authenticator and token estates; branch

Class	Members
	device estates

Assess each counterparty's practical remediation route for the scoped service. Retain the relationship between the counterparty, the service and the change required.

Map actual paths and cryptographic functions. A messaging interface can use several transport, message-signature and trust mechanisms. A supported message standard does not identify all of them. A successful bilateral key-establishment test does not prove that all intermediary hops, signature functions or relevant fallback configurations meet the service target.

FS.4 CRITICALITY TEST 2

The Universal Framework's test 2 covers material authorising an irreversible action or supporting a finality or non-repudiation guarantee. For financial services, the relevant functions and material include:

- Payment release and funds transfer authorisation.
- Securities settlement instruction.
- Contractual execution under qualified electronic signature.
- Irrevocable credit commitment.
- Claims settlement authorisation.
- Any signing key whose output must remain verifiable beyond the migration horizon.

Apply the five criticality tests to persistent assets or the explicitly selected endpoint/configuration class. Functions certifying or deriving other keys, authorising irreversible instructions, supporting finality, or lacking an operational equivalent may qualify. The institution must identify the relevant function and evidence rather than flag every financial record by category alone.

Availability, confidentiality and integrity require distinct consequence reasoning. A settlement-signing service may recover processing within a four-hour tolerance while still failing an approved integrity threshold. A certificate reissuance may restore a channel without resolving the status of an earlier signature. Where the necessary threshold or operational facts are unavailable, retain Not assessable and identify the accountable owner.

FS.5 SECTOR NOTES

Long-lived verification

Qualified-regime signatures on mortgage documentation, custody records, insurance policies and archived contracts must remain verifiable for decades. Each such asset triggers criticality test 4 under its verification-validity reading. The exposure is forgery, so it requires the signature side of the migration rather than only the key-establishment side.

Separate contemporary cryptographic protection from long-term verification. A document or instruction may continue to require authenticity after the signing system or certificate has changed. The service owner should identify that verification horizon, relevant preservation controls and the actual consequence of forged acceptance.

Data at rest and harvest exposure

Backup and archive estates hold the institution's longest-lived confidential data. For these wrapped estates, the exposure is the asymmetric wrapping keys rather than the symmetric encryption itself.

Internal services

Data-at-rest encryption, internal key management and backup encryption typically have no external counterparties. Under Universal Framework C.6, Effective Coverage then reduces to own-state coverage and counterparty counts report zero. That zero means the institution can close the gap alone; it is not a missing counterparty count.

FS.6 CONSEQUENCE-THRESHOLD TEMPLATE (NON-NORMATIVE)

The institution defines the consequence threshold under Universal Framework C.5.3. Use one row for each in-scope service. The service owner maintains the row and reviews it with the tolerance.

Field	Prompt
Service	The important business service the threshold protects
Failure shape	Confidentiality exposure, forgery, or both – per the layer scenarios in Universal C.5.2
Threshold statement	The exposure or forgery consequence the service treats as intolerable, stated as a

Field	Prompt
	quantity or a named category. "Per risk appetite" is not a statement.
Anchored to	The obligation or harm that makes it intolerable – scheme rules, notification duties, finality guarantees, contract law
Owner	The named individual who defends it in challenge
Review	Date, aligned to the tolerance review

Two illustrative statements show how to record a threshold. "A single forged qualified contract signature is intolerable" anchors the forgery threshold to non-repudiation. "Exposure of client positions held past the confidentiality horizon is intolerable" anchors the confidentiality threshold to criticality test 4's horizon.

An undefined consequence threshold is Not assessable, never Pass. Record the missing threshold as a governance finding.

FS.7 WORKED EXAMPLE – CORRESPONDENT BANKING

Scope and inputs

This illustrative, synthetic example is computed by the reference implementation (`compute_ccf.py --fs-example`). It shows mainframe concentration and the cloud-collapse effect in a mid-size universal bank's correspondent banking service.

The assessment covers 2,600 cryptographic assets, of which 140 are flagged. Criticality test 2 covers the SWIFT signing and payment-release material. Test 4 covers contract-signing keys whose validity extends beyond the horizon. The service has a four-hour tolerance, based on intraday settlement cutoffs.

Estate profile, reported and not scored: 2,450 assets are quantum-vulnerable (94.2%), 150 are quantum-safe symmetric (5.8%), and there is no post-quantum public-key material. Layer 1 is the 10,000 baseline for its applicable public-key population and is excluded from the reported service maximum.

The unit counts are synthetic inputs, not measurements of an institution or market. The example demonstrates arithmetic and interpretation; it does not assert that a complete institution-specific CBOM or independent validation has been supplied. The unresolved

cloud boundary counts as one primary unit at its known population. Its uncertainty is carried in reach, not in alternative CCI assignments.

Layer results

Layer	Units (assets)	CCI	Largest share	Band	Flagged-only	Largest failure domain (bound)	Largest upstream node (bound)	Tolerance
1 Algorithm *(baseline, excluded from the reported figure)*	one class	10,000	100%	Single-source-equivalent	10,000	–	–	Fail
2 Lineage	1180/640/340/240/200	2,981	45.4%	Concentrated	–	45.4% evid (standalone unit)	24.6% evid · 41.5% bound	Fail, on the bound
3 Trust root	980/760/320/300/240	2,645	37.7%	Concentrated	6,633	37.7% evid (standalone unit)	–	Fail, flagged
4 Custody	1800/420/280/100	5,185	69.2%	Highly concentrated	5,918	69.2% evid (standalone unit)	0.0% evid · 10.8% bound	Fail
5 Protocol	1120/900/340/240	3,310	43.1%	Concentrated	–	43.1% evid (standalone unit)	–	Pass
6 Key generation	1860/400/240/100	5,454	71.5%	Highly concentrated	–	71.5% evid (standalone unit)	15.4% evid · 24.6% bound	Fail

A flagged-only cell shows a dash where the illustration places no flagged material at that layer. An upstream-node cell shows a dash where no upstream node is named. The largest-failure-domain column includes standalone units as well as reach nodes and identifies the kind of endpoint reported. Tolerance results follow the failure-impact determination in Universal Framework C.5; the CCI and asset share do not themselves supply a recovery time.

Mainframe concentration

One coprocessor family holds 69.2% of custody, and one generation design produces 71.5% of the service's key material. This is the concentration described in the mainframe note in FS.2. Custody fails tolerance because migrating key material off the family takes longer than four hours.

Key generation fails on the same family's generation design. Re-keying 71.5% of the service's key material exceeds four hours, and keys already generated remain exposed regardless of the recovery time. The mainframe generation design is a standalone unit at layer 6, not the smaller profile-only design node reported in the upstream column.

That profile-only design node comprises the HSM family and the cloud entropy source conforming to one certification profile. It has 15.4% known reach and a 24.6% upper bound. The known figure is the largest conformant point's own design, a floor by construction rather than evidence that both points share a design.

The mainframe family also accounts for 45.4% of layer 2 because its cryptographic facility is an executing lineage. The reported service CCI is 5,454, at key generation.

Cloud boundary and lineage

The provider-boundary node appears at layers 2, 4 and 6 at 7.7%, 10.8% and 9.2% of the service respectively. These are bounds because the underlying modules are undisclosed. In each layer, the boundary counts as one primary unit at its known population. The provider is recorded as the boundary, never as the module behind it.

At layer 2, the same 200 cloud-library assets also fall within the OpenSSL-lineage bound. Reach overlaps by design, so reach shares must not be summed. Recording these assets against the cloud boundary does not exclude them from a possible shared implementation ancestor.

The largest upstream node is the OpenSSL-lineage bound at layer 2. Known reach covers the 640-asset distributed stack, or 24.6% of the service. The upper bound is 41.5% after including the HSM firmware family's undisclosed ancestry (240 assets) and the cloud provider's undisclosed library (200 assets). The 16.9 reach points between the known figure and the bound arise because two suppliers have not disclosed lineage. The Supplier Lineage Disclosure Request is issued to narrow that bound.

Layer 2 remains Fail, on the bound. The OpenSSL bounded domain fails the four-hour tolerance, while the mainframe facility's own 45.4% domain passes on its recoverability. The cell takes the worst result among the tested domains.

Trust-root criticality

Layer 3 has a headline CCI of 2,645, with the enterprise CA as the largest anchor. Across the 140 flagged assets, the CCI is 6,633. The SWIFT signing keys and qualified contract-signing keys resolve to two anchors at 78.6% and 21.4% respectively.

Revocation and reissuance under the SWIFT anchor exceed four hours. The cell therefore fails on the flagged view, even though the headline is one band lower. The difference identifies concentration in the qualifying functions that the overall trust distribution does not show as clearly.

Service result, coverage and counterparties

The service's largest failure domain is the mainframe generation design: 71.5% evidenced, a standalone unit at layer 6. This is distinct from its largest upstream node, the OpenSSL-lineage bound at layer 2. The reported CCI remains 5,454, the maximum across layers 2 to 6.

Effective Coverage is 0%. This is the result for the assessed population, not a numerical zero inferred from the classical baseline. If the required path facts were unavailable, the appropriate result would be EC-0/not computable rather than zero.

Second line organises remediation by counterparty class: 3 blocking counterparties – SWIFT, the home RTGS operator and the qualified trust service provider anchoring contract signatures; 14 peer correspondents; and 180 contractual respondents and vendors. There is no population class because the service has no retail endpoints. Attribute the affected paths to their actual parties rather than assuming that every asset depends on all three blocking counterparties.

FS.8 INTEGRATION INTO FINANCIAL-SERVICES GOVERNANCE

Use the service matrix to supplement RCSA, third-party concentration and operational-resilience assessments. A capital or loss model may consume relevant scenarios under separate governance, but the CCI itself does not produce a monetary loss or capital charge.

The procurement response should identify the dependency to be changed and the operational benefit. A different provider can improve contractual resilience while retaining the same code or firmware lineage. Conversely, a well-evidenced independent implementation may offer a genuine common-mode reduction but introduce testing, maintenance or transition costs. Document the trade-off rather than assume more vendors is always the correct remedy.

Use the framework instruments as a connected process: the Data Request obtains internal records; the Supplier Lineage Request addresses external provenance; the Determination Log preserves interpretation; the Model Documentation Pack records review; and the Board Report carries the service findings and qualifiers into a decision. For card and payment-specific asset details, also use the Payments Extension.

The UK NCSC migration timeline sets staged planning guidance through 2035; NIST IR 8547 is a transition draft. US Executive Order 14412 addresses specified federal systems and directs additional procurement rulemaking. These instruments must not be presented as interchangeable obligations for every financial institution. Record each applicable requirement, status, jurisdiction and function, and distinguish an adopted internal horizon from a binding external deadline.

UK CTP oversight began for the first four designated providers from 13 July 2026. That development does not turn a CCF score into a supervisory designation or a prescribed regulatory metric. CCF can provide cryptographic dependency evidence within broader third-party-risk and resilience work.

Canonical source. Published at ccframework.org under CC BY 4.0. Cite as: *The Applied Quantum Cryptographic Concentration Framework, Financial Services Extension v1.0-RC, Steve Vaile and Marin Ivezic / Applied Quantum, ccframework.org.*