

QUANTUM CORE INSTITUTE

QCI-QS1-S1

Financial Institutions Supplement

Quantum Readiness Guidance for Credit Unions and State-Chartered Banks

Document ID	QCI-QS1-S1
Version	1.2
Status	Public — Free to download and cite
Publisher	Quantum Core Institute (QCI)
Normative ref	QCI-QS1 Version 2.3 (September 23, 2026). Clause references are QCI requirement identifiers.
Applies to	Federally insured credit unions, state-chartered banks, and their technology service providers
Effective date	September 23, 2026
Review cycle	Annual, or upon material NCUA, FFIEC, or state regulatory developments, or a new edition of QCI-QS1

This supplement extends QCI-QS1 for the specific regulatory, vendor, and operational context of credit unions and state-chartered banks. It maps quantum readiness requirements to NCUA examination expectations, FFIEC guidance, and the core banking vendor dependencies that define cryptographic exposure for most institutions in this sector.

Foreword

Credit unions and state-chartered banks face a quantum readiness problem that is mostly not their own to solve — and that is exactly what makes it dangerous.

The cryptographic infrastructure protecting member accounts, payment rails, and loan records sits inside core banking platforms operated by a handful of vendors. Fiserv, Jack Henry, Symitar, FIS, and their peers control the upgrade timeline. Institutions that have not explicitly asked those vendors for a post-quantum cryptography roadmap — and documented the response — are carrying unmanaged third-party quantum risk.

At the same time, NCUA examiners are beginning to ask questions about cryptographic resilience and information security program maturity that will eventually reach quantum readiness. State banking regulators in New York, California, and Texas are moving faster than federal guidance. The institutions that have a documented program when those questions arrive will have a material advantage over those that do not.

This supplement maps QCI-QS1 requirements to the specific context of this sector. It does not replace QCI-QS1. It translates it for institutions that run on core banking platforms, operate under NCUA and state examiner oversight, and hold member data with multi-decade confidentiality obligations.

What changed in version 1.2

Version 1.2 aligns this supplement to QCI-QS1 version 2.3. Three changes matter for this sector. The Defensible readiness band now begins at 81, and a score of 80 is Advancing. Gate G70 is no longer satisfied by a documented exception: an institution cannot score above 70 until every critical supplier, including its core banking platform, has provided an adequate response and an officer-signed attestation. And gate G60 is fixed at 95 percent validated coverage of both critical systems and critical data flows. Section 3.4 explains what the G70 change means for institutions whose exposure sits inside a vendor's platform. Section 2.4 is new: it turns this supplement's regulatory mapping into the obligations register that QCI-2.2-01 requires.

1. Scope and applicability

This supplement applies to:

- Federally insured credit unions of all asset sizes
- State-chartered banks and savings institutions subject to state banking department examination
- Credit union service organizations (CUSOs) that provide technology, payment, or identity services to member institutions
- Technology service providers whose products materially affect the cryptographic posture of institutions in scope

This supplement is organized to follow QCI-QS1's structure. Each section of this supplement corresponds to a clause in QCI-QS1 and provides sector-specific guidance, regulatory mapping, and implementation considerations.

Asset size and proportionality

QCI-QS1 applies proportionally. A \$150 million community credit union is not expected to match the quantum readiness posture of a \$50 billion regional bank. This supplement provides guidance calibrated to institution size throughout. Where requirements differ by asset tier, this is explicitly noted. Proportionality does not change the gates: the 95 percent coverage threshold and the supplier

attestation requirement apply to every institution's declared assessment boundary (QCI-1.1-01), and a small boundary is easier to cover than a large one.

Note on the AI-cryptographic provisions

QCI-QS1 carries conditional AI-cryptographic provisions. Where AI systems fall within the assessment scope, the organization also keeps linked AI artifact records with separate confidentiality and verification horizons (QCI-5.2-03), exercises the D7-AI incident scenarios (QCI-4.4-03), includes AI suppliers' posture in Pillar 5 (QCI-6.4-01), and issues Annex C section G, questions G1 to G5, to suppliers of AI platforms, ML infrastructure, model registries, or key management used with AI artifacts. These provisions have no effect where AI systems are not in scope; a non-AI system records AI applicability as none. They govern cryptographic risk arising from AI systems. They do not govern AI risk generally.

2. Regulatory context

2.1 NCUA examination relevance

The NCUA's Information Security examination procedures assess whether credit unions have identified and managed risks associated with their information systems, including cryptographic controls. While NCUA has not yet issued explicit quantum readiness guidance, the following examination areas are directly relevant:

NCUA examination area	Relevance to quantum risk	QCI-QS1 mapping
Information security program maturity	Crypto dependency inventory and governance ownership are information security fundamentals	Governance, Clause 4 (QCI-4.1-01); Inventory, Clause 5
Vendor management and third-party oversight	Core banking vendors control most institution cryptographic exposure; attestation is the evidence standard	Third-party oversight, Clause 7; Annex C
Business continuity and operational resilience	Cryptographic failure in identity or payment systems creates operational continuity exposure	QRAF D7; incident readiness QCI-4.4-01; Q-Risk Score P4
Data classification and protection	Member data confidentiality obligations extend decades for mortgage and loan records	QASI confidentiality and verification horizons, QCI-5.2-01
Board and management oversight	Quantum risk requires named ownership and board-level reporting	QCI-4.1-01 and 4.1-02; governing-body insert, Clause 8

2.2 FFIEC guidance alignment

The FFIEC Information Technology Examination Handbook addresses encryption, authentication, and third-party risk in terms directly applicable to quantum readiness. Key alignment points:

- The Authentication and Access to Financial Institution Services guidance requires institutions to assess the adequacy of their authentication controls — which depend on cryptographic integrity that quantum computing threatens

- The Outsourcing Technology Services booklet requires institutions to manage vendor risk with the same rigor as internal risk — quantum readiness attestation from core banking vendors satisfies this requirement
- The Management booklet's risk appetite and governance requirements align directly with QCI-QS1's governance model

2.3 State regulatory environment

State banking regulators are moving at different speeds. Institutions should monitor the following:

- New York DFS: Has issued cybersecurity regulations (23 NYCRR 500) that include encryption requirements and are likely to be updated to address post-quantum cryptography. New York-chartered institutions should track DFS guidance closely.
- California DFPI: Has issued guidance on technology risk management that encompasses vendor cryptographic controls. California-chartered institutions should include DFPI examination expectations in their quantum readiness planning.
- CISA and OMB federal guidance: While applicable primarily to federal agencies, Executive Order 14412 (June 22, 2026) and OMB M-26-15 (June 24, 2026) set federal key-establishment and authentication transition deadlines of December 31, 2030 and December 31, 2031, and CISA's post-quantum cryptography guidance provides benchmarks that state examiners may reference. QCI-QS1 Annex E records these as S12 and S13.

2.4 Obligations register entries for this sector

QCI-2.2-01 requires the organization to maintain an applicability register listing each relevant external obligation with its issuer, exact document and revision, date, authoritative URL, applicable sections, status, affected systems and suppliers, required actions and deadlines, exception authority, accountable owner, and last verification date. The mapping in this section is the seed for that register. The entries below are the minimum for an institution in this sector; each institution adds its own state, contractual, and network obligations and verifies every entry against the source before relying on it.

Obligation or profile	Issuer and document	Status	Affected systems and suppliers	Action and deadline
Information security examination	NCUA examination procedures; FFIEC IT Examination Handbook (Outsourcing Technology Services; Authentication and Access; Management)	Examination guidance; binding through the examination process, not a PQC mandate	Core banking platform and supplier; digital banking; payment rails; identity stores	Vendor roadmap request and response on file before the next examination cycle
State cybersecurity regulation	New York DFS 23 NYCRR 500; California DFPI technology risk guidance; other state equivalents	Regulation where applicable by charter	All systems holding member data	Track amendments addressing post-quantum cryptography; record the applicable revision
Federal transition policy	Executive Order 14412; OMB M-26-15	Federal policy; applicability to the institution only by contract or federal interoperation	Federally interoperating systems; federal grant-funded systems	Record as context; verify contractual applicability with counsel

Obligation or profile	Issuer and document	Status	Affected systems and suppliers	Action and deadline
Payment network rules	Visa, Mastercard, NACHA operating rules and PQC migration announcements	Contract	Card processing, ACH, wire	Align internal timelines to network requirements as published
Retention obligations	BSA/AML, mortgage and loan record retention rules, state statutes	Law and regulation	Loan servicing, document management, archives	Set confidentiality horizons in the QASI from the longest applicable retention

Examination preparation posture

An institution that arrives at an NCUA or state examination with a completed QASI, a current Q-Risk Score with its assessment type stated (QCI-1.2-03), conformance status reported beside the score (QCI-1.2-04), and vendor attestations for its core banking providers is in a materially stronger position than one that cannot produce these. Examiners are not yet asking for quantum readiness documentation. When they start, the institutions that already have it will define the standard. Use of QCI-QS1 is not described as QCI certification.

3. Core banking vendor concentration risk

3.1 Why this sector's exposure is different

Most industries face quantum risk distributed across many vendors and internal systems. Financial institutions in this sector face a more concentrated problem: the majority of cryptographic exposure sits inside a small number of core banking platforms that institutions did not build and cannot easily modify.

This creates a specific risk profile: the institution's Q-Risk Score, particularly Pillar 5 (third-party readiness), is largely determined by whether its core banking vendor has a credible post-quantum cryptography roadmap and will attest to it. An institution with excellent internal governance but a vendor with no PQC roadmap is still materially exposed, and under QCI-QS1 v2.3 its score is capped at 70 until that vendor attests.

3.2 Core banking vendor landscape

The following vendors represent the majority of core banking relationships in this sector. Each presents specific quantum readiness considerations. The status column records what each vendor had published as of September 23, 2026; it changes with every release, so confirm the current position with the vendor and record it, with the date, in the QASI supplier record (QCI-5.2-01).

Vendor	Primary platforms	Key crypto exposure	PQC status (reviewed September 23, 2026)	Institution action required
Fiserv	Signature, Premier, Portico, DNA	Core transaction authentication, TLS, digital signing, card services	No public PQC roadmap located for any platform. The only public reference is the August 2023 Signature International modernization white paper, which cites the quantum-safe capability of IBM Power10 hardware — an infrastructure attribute, not an application-layer roadmap.	Issue the Annex C request with a 60-day deadline; request the PQC roadmap and the approved key-establishment and signing profiles by release
Jack Henry	Symitar, SilverLake, Banno	Member authentication, digital banking TLS, certificate management	No public PQC roadmap located. A 2026 PKI and cryptography engineering role posting refers to post-quantum cryptography research; there is no product statement for Symitar, SilverLake or Banno.	Request a scoped CBOM or library inventory meeting QCI-5.4-03; request the PQC roadmap with dates
FIS	IBS, HORIZON, XP2	Payment processing crypto, core authentication, data encryption at rest	No public PQC statement located on fisglobal.com, in FIS insight publications or in press releases for IBS, HORIZON or XP2.	Contractualize PQC milestones at next renewal (QCI-7.1-02); request the officer-signed attestation now
Corelation	Keystone	Member authentication, TLS, digital banking crypto	No public PQC statement located for KeyStone; published security material covers tokenization and encryption generally.	Engage account team at VP level; request the published PQC roadmap and the attestation
Payment networks (Visa, MC, NACHA)	Card processing, ACH, wire	Transaction signing, authentication, nonrepudiation	Mastercard: migration white paper published October 20, 2025, following its earlier quantum-resistant contactless specification. Visa: December 30, 2025 outlook names 2026 as the year to begin preparing and gives no dated commitment. FS-ISAC payment card PQC papers (February 2025) record that EMV's ability to carry quantum-safe certificates is unresolved. NACHA: no statement located.	Monitor network PQC migration announcements; align internal timelines to network requirements; record the network as a supplier in the QASI

Status sources, as reviewed September 23, 2026. Absence of a public statement is recorded as such; it is not evidence of absence of work, and it is not an adequate response under QCI-7.2-02 either way.

- Fiserv, Signature International Modernization on IBM Hybrid Cloud, white paper, August 2023: [fiserv.com/content/dam/fiserv-ent/final-files/marketing-collateral/white-papers/signature-international-modernization-on-ibm-hybrid-cloud-white-paper-1123.pdf](https://www.fiserv.com/content/dam/fiserv-ent/final-files/marketing-collateral/white-papers/signature-international-modernization-on-ibm-hybrid-cloud-white-paper-1123.pdf)
- Jack Henry, Senior Information Security Engineer: PKI/Cryptography, careers posting: careers.jackhenry.com
- Mastercard, Migration to post-quantum cryptography, white paper page dated October 20, 2025: [mastercard.com/global/en/news-and-trends/Insights/2025/post-quantum-cryptography-white-paper.html](https://www.mastercard.com/global/en/news-and-trends/Insights/2025/post-quantum-cryptography-white-paper.html)

- Visa, The quantum unlock: and five more pillars shaping payments in 2026, press release, December 30, 2025: visa.com.au/about-visa/newsroom/press-releases/
- FS-ISAC, The Impact of Quantum Computing on the Payment Card Industry, February 2025: fsisac.com/pqc-payment-card-industry

3.3 Vendor leverage strategies

Institutions often believe they have no leverage over large core banking vendors. This is partially true but not entirely. The following strategies have proven effective:

1. Issue the Annex C request formally, via your account manager, with a named response deadline no later than 60 days after issue (QCI-7.2-04). Vendors who receive informal questions often defer. Vendors who receive a formal written request with a deadline treat it differently.
2. Coordinate with peer institutions. A request from one \$200 million credit union is easy to defer. A coordinated request from 15 institutions using the same platform, facilitated through a league or association, is not. CUNA, NAFCU, and state leagues can facilitate this coordination.
3. Reference regulatory expectations in the request. Language such as 'our NCUA examination program requires us to document vendor cryptographic roadmaps as part of our third-party risk program' changes the conversation from a preference to an obligation.
4. Contractualize at renewal. If a vendor cannot provide a PQC roadmap today, add a contractual requirement to deliver one within 12 months as a condition of contract renewal, with notification terms and evidence-access rights (QCI-7.1-02). This converts a soft expectation into an enforceable obligation.
5. Use the exception register. Every vendor that fails to respond by the deadline, or responds inadequately, goes on the exception register under QCI-4.3-02 and QCI-7.3-01 with treatment, expiry, review triggers, and an exit or replacement strategy or the documented reason none is feasible. This creates an audit trail that demonstrates due diligence regardless of vendor behavior.

3.4 What gate G70 means for this sector

Under QCI-QS1 v2.3, an institution cannot score above 70 until every critical supplier has provided a current, adequate response and an officer-signed attestation on the Annex C form (gate G70, QCI-6.3-01). An approved exception, however well managed, does not lift the cap. For an institution whose core banking platform is operated by a supplier that has not attested, the score stays at 70 and the supplier's name recurs in the governing-body insert every quarter until it does.

That is the rule working as designed. It moves the pressure from the institution, which cannot fix the vendor's cryptography, to the vendor, which can. The leverage strategies in section 3.3 are how the institution gets the attestation; the exception register is where the supplier's name sits in the meantime. An institution that has done everything in its own power and is held at 70 by a vendor has a defensible position with an examiner, and the register is the evidence of it. An institution that reports 74 with an unattested core vendor has a finding.

4. Member data horizons and HNDL exposure

4.1 Why financial institutions face elevated HNDL risk

Harvest-now, decrypt-later (HNDL) attacks are particularly relevant for financial institutions because of the long-lived nature of the data they hold. An adversary who captures encrypted loan records, mortgage documents, or authentication credentials today may be able to decrypt them within the timeline relevant to those records. QCI-QS1 v2.3 records that timeline as a confidentiality horizon, a date or a duration with a start date, and records separately the verification horizon for anything that must remain provably authentic, such as signed loan agreements (Clause 3; QCI-5.2-01).

Data type	Typical retention	HNDL risk level	Rationale
Mortgage and real estate loan records	Life of loan plus 7 years (up to 37 years)	High	Long retention combined with regulated confidentiality creates a sustained exposure window
Member authentication credentials and identity records	Active plus 7 years post-closure	High	Identity compromise has long-tail fraud implications; authentication replay attacks extend exposure
Business and commercial loan documentation	7 to 10 years post-maturity	High	Commercial loan data includes sensitive financial disclosures with extended confidentiality obligations
Transaction and payment records	5 to 7 years	Medium	Shorter retention reduces the window; payment data has high value if decrypted
Card data and tokenization records	Varies by network rules	Medium	Network-managed retention reduces institution exposure; tokenization provides some mitigation
BSA/AML records and suspicious activity reports	5 years minimum, often longer	Medium	Regulatory sensitivity of SAR data makes decryption a significant compliance and reputational risk

4.2 Applying horizons to the QASI

When completing the QASI for financial institution systems, the confidentiality horizon should reflect the full retention obligation, not just the active use period. A mortgage loan originated today may carry a 37-year confidentiality obligation when retention requirements are applied. Any system holding that data under vulnerable protection carries the exposure flag for vulnerable protection of long-lived confidentiality (QCI-5.3-01), and an approved migration plan does not clear the flag; only evidenced mitigation does (QCI-5.3-02).

Institutions should pay particular attention to:

- Core banking systems that hold loan origination and servicing records — these are typically the highest-horizon datasets in the institution
- Document management systems holding mortgage closing packages, commercial loan agreements, and trust documents — these carry a verification horizon as well, because the signatures must remain provable

- Identity and authentication stores — member credentials and biometric data have both horizon and sensitivity characteristics that elevate HNDL risk
- Archive and backup systems — encrypted backups are a primary harvest target because they are often less monitored and may use older key protection than production systems. A backup whose data keys were protected under a classical key envelope remains exposed even after the envelope is replaced; the standard requires that a rewrap is not reported as remediation of copies an adversary may already hold (QCI-4.6-03)

5. QASI record guidance for financial institutions

The following guidance supplements the QASI record groups in QCI-5.2-01 with financial institution-specific context. A field may hold a known value, an explicit unknown with an investigation action, owner and due date, or a justified not-applicable value (QCI-5.1-02). A record with an unknown algorithm, profile, trust dependency, or key-protection mechanism stays outside validated coverage until the unknown is resolved; that is the honest answer for an institution whose vendor has not yet responded, and it is better than a guess.

QASI field	Financial institution guidance
Business criticality	Core banking platform: always High. Digital banking portal: High. Payment processing: High. Internal HR system: Medium or Low. When in doubt, default to High for any system touching member financial data. Criticality follows QCI-1.1-02: a system whose failure could exceed approved risk appetite is critical.
Confidentiality and verification horizons	Use the longest applicable retention period as the confidentiality horizon. For systems holding multiple data types, use the longest. Mortgage systems: 37 years. Transaction systems: 7 years. Authentication systems: 7 years post-closure minimum. Record a separate verification horizon for signed agreements and audit records.
Critical data flows	New in v2.3: flows are a separate coverage denominator (QCI-5.1-03). Inventory at minimum: core-to-digital-banking sessions, payment rail connections (card, ACH, wire), core-to-document-management transfers, and identity provider federation, with protection and authentication at each hop.
Vendor dependencies	Name the core banking platform vendor, product, and deployed release explicitly. Do not write 'cloud provider' — name the platform. This record drives the Annex C request and the G70 determination.
PQC support status	Most core banking platforms will be at 'None' or 'Roadmap' as of late 2026. Distinguish supported, configured, and observed (QCI-4.5-01). Do not accept vendor sales assertions as evidence — require a written roadmap with dated milestones and an attestation before upgrading this field.
Crypto agility status	Most institutions will be at 'None' for core banking systems — algorithm changes require vendor action, not institution action. Document this dependency explicitly rather than leaving the field blank.
Exposure flags	Raise the long-lived-confidentiality flag for any system holding mortgage, loan, or identity data with retention exceeding five years under vulnerable protection. Treatment status is recorded separately (QCI-5.3-02); tokenization or minimization is recorded as treatment, not as removal of the flag, until its effect on the protected path is evidenced.

QASI field	Financial institution guidance
Compensating controls	Tokenization of card data is an effective compensating control. Data minimization for archived records is effective. TLS version upgrades (1.2 to 1.3) reduce some exposure but do not address the underlying public-key cryptography problem. None of these is assumed to remove HNDL risk without analysis of the protected path and its dependencies.

6. Q-Risk Score guidance for financial institutions

6.1 Realistic band targets by asset tier

QCI-QS1 defines score bands from Exposed (0 to 19) through Defensible readiness (81 to 100). A score of exactly 80 is Advancing, and no score above 80 is possible unless gates G60, G70 and G80 have all passed (QCI-6.3-01, QCI-6.5-01). The following targets represent realistic 12-month goals for institutions in this sector, given vendor dependency constraints and resource realities. They are guidance for planning, not Core-profile thresholds; peer comparison uses the Core profile only (QCI-6.3-02).

Institution profile	Starting baseline (typical)	Realistic 12-month target	Primary constraint
Credit union under \$500M assets	8 to 18 (Exposed)	25 to 40 (Behind to Mobilizing)	Limited security staff; vendor dependency on core platform
Credit union \$500M to \$2B assets	12 to 25 (Exposed to Behind)	35 to 55 (Behind to Mobilizing)	Core banking vendor PQC readiness; certificate sprawl
State-chartered bank under \$1B assets	15 to 28 (Exposed to Behind)	40 to 58 (Mobilizing)	Vendor concentration; limited dedicated security resources
State-chartered bank \$1B to \$10B assets	20 to 38 (Behind)	50 to 68 (Mobilizing to Advancing)	Multi-vendor complexity; migration sequencing across legacy systems

No tier reaches 70 within 12 months unless the core banking supplier has attested; see section 3.4. A target in the 60s assumes G60 has passed, which requires the critical-flow inventory as well as the system inventory.

6.2 Pillar-specific guidance

The following notes address how each Q-Risk Score pillar typically presents for institutions in this sector, against the cumulative rubrics of QCI-6.6-01 to 6.10-01:

- P1 (Governance): This is the fastest pillar to improve. Naming an executive sponsor and Quantum Risk Owner, creating a quantum risk register entry, approving the policy and risk appetite, and delivering a governing-body briefing can move P1 from level 0 to level 2 within 30 days. Level 3 requires one full quarterly cycle completed. Most institutions underinvest here because it feels like paperwork. It is not — it is the prerequisite for everything else.
- P2 (Crypto visibility): Institutions that have completed a technology inventory for other purposes (SOC 2, NCUA examination prep) can accelerate QASI completion by cross-referencing existing asset registers. The gap is usually crypto-specific fields — algorithms, libraries, deployed versions, horizons — which require engineering validation, and the

critical-flow inventory, which is new. Level 3 requires 80 percent validated coverage in each category; level 4 requires 95 percent.

- P3 (Exposure management): Financial institutions typically score higher on this pillar than other sectors once they complete the analysis. The retention obligations are well understood from a regulatory perspective — the gap is mapping those obligations to specific systems as horizons and separating exposure from treatment.
- P4 (PQC migration): This pillar will be constrained by vendor timelines for most institutions. Score honestly. Level 3 requires a representative pilot passed under QCI-4.7 and at least one critical production transition accepted; a level 1 with documented vendor engagement is more defensible than a claimed level 3 without evidence.
- P5 (Third-party readiness): This is the pillar where financial institutions can make the most meaningful near-term progress. Issuing Annex C requests to every critical supplier, tracking responses against the 60-day deadline, and maintaining the exception register directly improves this score and creates examination-ready documentation. Level 3 requires 80 percent of critical suppliers with current adequate responses and attestations; G70 requires all of them.

7. Governance model for smaller institutions

QCI-4.1-01 requires named roles including an executive sponsor, a Quantum Risk Owner, documented responsibilities across engineering, system and data owners, procurement, incident response, legal and compliance, and assurance, and a cross-functional steering function. Roles may be combined where conflicts are managed. For smaller institutions with lean staffing, these roles can be mapped to existing positions without creating new headcount:

QCI-QS1 required role	Typical mapping for smaller institution	Minimum time commitment
Executive Sponsor	CISO (if present), VP of IT, or COO — whoever owns the information security program	Quarterly review and governing-body briefing preparation; approval of the assessment boundary
Quantum Risk Owner	IT Director, Security Officer, or senior IT staff member with program coordination capability	Monthly: QASI maintenance, vendor follow-up, score tracking; quarterly obligations register review
Steering function (risk committee)	Existing IT Risk or Enterprise Risk committee; add quantum risk as a standing agenda item	Quarterly review of Q-Risk Score and vendor exception register
Procurement / vendor risk	Existing vendor management function or contract administrator	As needed for Annex C issuance, deadline tracking, and attestation filing
Governing-body oversight	Existing board IT or audit committee; use the governing-body insert format from QCI-QS1 Annex D	Quarterly, as part of the existing board pack

The staffing reality

A credit union with two IT staff cannot run a full quantum readiness program at the same depth as an institution with a dedicated security team. What they can do is document what they know, record what they do not know as explicit unknowns, name an owner, issue vendor requests, and produce an honest self-assessed Q-Risk Score labelled as such. That documented effort is the difference

between a finding and a commendation in an examination. QCI engagements are specifically designed to supplement internal capacity for institutions in this position.

8. Financial institution 90-day quick start

This sequence is adapted from the QCI Practitioner Handbook's establishment sequence and QCI-QS1 Clause 9.1 for the specific starting point of most credit unions and state-chartered banks, where vendor engagement is the critical early action. It is a planning aid, not a conformance grace period.

Timeframe	Phase	What to accomplish	Output
Week 1	Assign and bound	Name the executive sponsor and Quantum Risk Owner. Map to existing roles using section 7. Declare the assessment boundary (QCI-1.1-01). Seed the obligations register from section 2.4.	Signed role assignment. Approved boundary. Obligations register started.
Week 2	Issue vendor requests	Issue Annex C requests to your top three vendors: core banking platform, digital banking provider, and primary certificate authority. Do this before inventory — vendor response timelines are long and the clock needs to start.	Three requests issued with a 60-day response deadline (QCI-7.2-04). Logged in the vendor management system.
Weeks 3 to 5	Inventory core systems and flows	Build linked QASI records for the five highest-criticality systems: core banking platform, digital banking portal, payment processing, identity and authentication, and primary document management. Inventory the critical flows between them and to payment rails.	Five system records and their flows completed, validated with owners and a technical reviewer. Unknowns recorded explicitly. Long-lived-confidentiality flags raised where horizons exceed 5 years.
Weeks 6 to 8	Expand and analyze	Extend the QASI to remaining critical systems and flows toward the 95 percent threshold. Set horizons using section 4. Identify top exposures and set treatment status.	Coverage computed per QCI-5.1-03 for systems and flows. Horizon analysis complete. Top 10 remediation targets identified.
Week 9	Score	Produce the first Q-Risk Score using the Annex B worksheet and the QCI-6.1-02 formula. Record the assessment type. Apply the sector band targets from section 6 as planning context. Be honest.	Self-assessed Q-Risk Score snapshot with evidence links, gate results, and pillar gaps documented.
Weeks 10 to 12	Report and follow up	Deliver the first governing-body insert (QCI-8.1-01). Follow up with vendors as the 60-day deadline passes. Place non-responding or inadequate vendors on the exception register.	Insert delivered. Exception register active. PQC migration roadmap draft begun with milestone types per QCI-4.2-02.

9. Examination preparation checklist

The following checklist documents what a well-prepared institution should be able to produce when an examiner asks about quantum risk and cryptographic resilience. None of these require a fully mature program — they require a documented, honest program.

Governance documentation

- Named executive sponsor for quantum readiness program — in writing
- Approved assessment boundary with exclusions and rationale (QCI-1.1-01)
- Quantum risk register entry with current risk rating and owner
- Obligations register with the entries in section 2.4, verified and dated (QCI-2.2-01)
- Governing-body insert from the most recent quarterly risk pack
- Quantum Risk Policy Statement or equivalent section in the information security policy

Inventory and visibility

- QASI covering all critical systems and critical flows — with coverage computed for each, numerator and denominator shown
- System owners and technical reviewers confirmed for each record; unknowns explicit
- Horizon analysis completed for mortgage, loan, and identity systems
- Exposure flags identified and tracked with treatment status and owners
- Discovery evidence, where used, with the provenance elements of QCI-5.4-01

Vendor management

- Annex C requests issued to core banking platform, digital banking provider, and certificate authority, with deadlines
- Vendor responses received and filed with adequacy determinations (QCI-7.2-03), or non-responses documented in the exception register
- Vendor exception register with treatment, expiry, review triggers, and exit strategy for each exception
- Any vendor attestations received on the Annex C form, officer-signed and filed; refresh dates tracked

Scoring and progress

- Q-Risk Score snapshot — current quarter — with evidence links, gate results, assessment type, and conformance status reported separately
- Score movement since the prior quarter, with reasons, and restatement where the edition changed (QCI-1.3-02)
- PQC migration roadmap draft with milestones, even if early stage

What examiners are not yet asking for — but will

Crypto agility test results. A documented test that the institution can change a cryptographic profile on at least one critical trust pathway without full platform replacement. QCI-QS1 v2.3 defines the test in QCI-4.7-01: interoperability end to end, actual algorithm negotiation, authentication and trust validation, invalid inputs, downgrade and fallback, message and certificate size, resource exhaustion, capacity and latency, backup and restore, failover, and authorized rollback, in an environment representative of the pathway, with acceptance under QCI-4.7-02. No financial institution in this sector can run that test on a core banking platform today — that is a vendor constraint. But institutions can run it on pathways they control directly, such as an internal identity system or a web application's TLS configuration, provided the pathway is critical under QCI-1.1-02. Passing it on one such pathway within the last twelve months passes gate G80 and creates a documented foundation for the vendor

conversations that are coming. QCI-T2 is the protocol.

10. Summary and engagement

This supplement translates QCI-QS1 into action for credit unions and state-chartered banks. The core message is straightforward: most of your quantum risk sits in vendors you did not build and cannot easily replace, your retention obligations make harvest-now, decrypt-later exposure material and long-lived, and your examiners will eventually ask questions you should already have answers to. Under version 2.3 the standard says the vendor part plainly: until the vendor attests, the score is capped, and the register is where that is recorded.

The institutions that act now are not over-preparing. They are building the documentation, vendor relationships, and governance habits that will define the examination standard for this sector when quantum readiness moves from best practice to expectation.

QCI engagement support for financial institutions

QCI works with credit unions and state-chartered banks to deliver calibrated assessments against QCI-QS1, facilitate peer-coordinated vendor engagement for core banking platforms, benchmark Q-Risk Scores against sector peers on the Core profile, and build examination-ready documentation packages. Independent assessment under QCI-1.2-03 is available separately. Contact QCI to discuss how an engagement is structured for institutions of your size and complexity.

Revision history

Version	Date	Changes
1.2	September 23, 2026	Aligned to QCI-QS1 v2.3; vendor status table refreshed against supplier publications as of September 23, 2026, with sources listed: references by requirement identifier; band targets restated for the 81-point Defensible readiness threshold; gate G70 no longer satisfied by exceptions (new section 3.4); G60 fixed at 95 percent for systems and flows, with critical-flow guidance; obligations register section 2.4 added; horizons replace data longevity; supplier deadline and attestation rules; federal policy references updated to EO 14412 and OMB M-26-15; agility test described per QCI-4.7; references to the retired QCI-QS1-A guide replaced.
1.1	June 10, 2026	Aligned to QCI-QS1 v2.2; AI-cryptographic provisions note added.