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	1.1
Status	Public — Free to download and cite
Publisher	Quantum Core Institute (QCI)
Normative ref	QCI-QS1 Version 2.2
Applies to	Federally insured credit unions, state-chartered banks, and their technology service providers
Effective date	June 10, 2026
Review cycle	Annual, or upon material NCUA, FFIEC, or state regulatory developments

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.

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.

Note on QCI-QS1 v2.2 AI-cryptographic provisions

QCI-QS1 v2.2 adds conditional AI-cryptographic provisions to the parent standard. Where AI systems fall within the assessment scope, the organization also captures the conditional QASI AI fields (Clause 5.2), covers the D7-AI incident scenarios (Clause 4.4), applies the Pillar 5 AI-cryptographic posture check (Clause 6.4), and issues Vendor Roadmap Request Pack Section G 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. 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	QRAF Clause 4, QASI Clause 5
Vendor management and third-party oversight	Core banking vendors control most institution cryptographic exposure; attestation is the evidence standard	Vendor Pack Clause 7
Business continuity and operational resilience	Cryptographic failure in identity or payment systems creates operational continuity exposure	QRAF D7, Q-Risk Score P4
Data classification and protection	Member data longevity obligations extend decades for mortgage and loan records	QASI data longevity fields, Clause 5.2
Board and management oversight	Quantum risk requires named ownership and board-level reporting	QRAF Clause 4.1, Board 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 QRAF 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, CISA's post-quantum cryptography guidance and OMB memoranda on migration timelines provide useful benchmarks that state examiners may reference.

Examination preparation posture

An institution that arrives at an NCUA or state examination with a completed QASI, a current Q-Risk Score, 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.

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. An institution with excellent internal governance but a vendor with no PQC roadmap is still materially exposed.

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:

Vendor	Primary platforms	Key crypto exposure	Institution action required
Fiserv	Signature, Premier, Portico, DNA	Core transaction authentication, TLS, digital signing, card services	Issue Vendor Roadmap Request Pack; request PQC roadmap and hybrid mode timeline
Jack Henry	Symitar, SilverLake, Banno	Member authentication, digital banking TLS, certificate management	Request SBOM extract for cryptographic libraries; request PQC roadmap with dates
FIS	IBS, HORIZON, XP2	Payment processing crypto, core authentication, data encryption at rest	Contractualize PQC milestones at next renewal; request attestation now
Corelation	Keystone	Member authentication, TLS, digital banking crypto	Engage account team at VP level; request published PQC roadmap

Vendor	Primary platforms	Key crypto exposure	Institution action required
Payment networks (Visa, MC, NACHA)	Card processing, ACH, wire	Transaction signing, authentication, nonrepudiation	Monitor network PQC migration announcements; align internal timelines to network requirements

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 vendor roadmap request pack formally, via your account manager, with a named response deadline. 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. This converts a soft expectation into an enforceable obligation.
5. Use the exception register. Every vendor that fails to respond goes on the exception register with compensating controls documented. This creates an audit trail that demonstrates due diligence regardless of vendor behavior.

4. Member data longevity 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.

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 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 window; payment data has high value if decrypted
Card data and tokenization records	Varies by network rules	Medium	Network-managed retention reduces institution exposure;

Data type	Typical retention	HNDL risk level	Rationale
			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 data longevity to the QASI

When completing the QASI for financial institution systems, the data longevity field 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 with non-PQC encryption and no migration roadmap should carry a High HNDL risk flag.

Institutions should pay particular attention to:

- Core banking systems that hold loan origination and servicing records — these are typically the highest-longevity datasets in the institution
- Document management systems holding mortgage closing packages, commercial loan agreements, and trust documents
- Identity and authentication stores — member credentials and biometric data have both longevity 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 encryption configurations than production systems

5. QASI field guidance for financial institutions

The following guidance supplements the QASI field definitions in QCI-QS1 Clause 5.2 with financial institution-specific context.

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.
Data longevity required	Use the longest applicable retention period. For systems holding multiple data types, use the longest. Mortgage systems: 37 years. Transaction systems: 7 years. Authentication systems: 7 years post-closure minimum.
Vendor dependencies	Name the core banking platform vendor and version explicitly. Do not write 'cloud provider' — name the platform. This field drives the Vendor Roadmap Request Pack process.
PQC support status	Most core banking platforms will be at 'None' or 'Roadmap' as of early 2026. Do not accept vendor sales assertions as evidence — require a written roadmap with dated milestones 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.

QASI field	Financial institution guidance
HNDL risk	Default to High for any system holding mortgage, loan, or identity data with retention obligations exceeding five years. Medium only where compensating controls (tokenization, data minimization) materially reduce exposure.
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.

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 (80 to 100). The following targets represent realistic 12-month goals for institutions in this sector, given vendor dependency constraints and resource realities:

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

6.2 Pillar-specific guidance

The following notes address how each Q-Risk Score pillar typically presents for institutions in this sector:

- P1 (Governance): This is the fastest pillar to improve. Naming an executive sponsor, creating a quantum risk register entry, and scheduling a board briefing can move P1 from Level 0 to Level 2 within 30 days. 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, and longevity data — which require engineering validation.
- P3 (Data longevity): Financial institutions typically score higher on this pillar than other sectors once they complete the analysis. The data longevity obligations are well understood from a

regulatory perspective — the gap is mapping those obligations to specific systems and cryptographic controls.

- P4 (PQC migration): This pillar will be constrained by vendor timelines for most institutions. Score honestly. A Level 1 here 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 vendor roadmap requests and maintaining an exception register for non-responses directly improves this score and creates examination-ready documentation.

7. Governance model for smaller institutions

QCI-QS1 Clause 4 requires named roles including an executive sponsor, Quantum Risk Owner, and cross-functional risk committee. 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 information security program	Quarterly review and board briefing preparation
Quantum Risk Owner	IT Director, Security Officer, or senior IT staff member with program coordination capability	Monthly: QASI maintenance, vendor follow-up, score tracking
Risk Committee	Existing IT Risk or Enterprise Risk committee; add quantum risk as 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 vendor request pack issuance and attestation tracking
Board oversight	Existing board IT or audit committee; use Board Briefing Insert format from QCI-QS1	Quarterly, as part of 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, name an owner, issue vendor requests, and produce an honest Q-Risk Score. 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 QCI-QS1-A for the specific starting point of most credit unions and state-chartered banks, where vendor engagement is the critical early action.

Timeframe	Phase	What to accomplish	Output
Week 1	Assign	Name executive sponsor and Quantum Risk Owner. Map to existing roles using Section 7 of this supplement.	Signed role assignment. Added to information security program documentation.
Week 2	Issue vendor requests	Issue vendor roadmap request packs 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 vendor requests issued with 60-day response deadline. Logged in vendor management system.
Weeks 3 to 5	Inventory core systems	Build QASI for five highest-criticality systems: core banking platform, digital banking portal, payment processing, identity/authentication, and primary document management system.	Five QASI rows completed, validated with system owners. HNDL risk flagged where data longevity exceeds 5 years.
Weeks 6 to 8	Expand and analyze	Extend QASI to remaining critical systems. Map data longevity obligations using Section 4 of this supplement. Identify top risk flags.	Full QASI for critical systems. Data longevity analysis complete. Top 10 remediation targets identified.
Week 9	Score	Produce first Q-Risk Score using QCI-QS1-A worksheet. Apply sector band targets from Section 6 of this supplement. Be honest.	Q-Risk Score snapshot with evidence links. Pillar gaps documented.
Weeks 10 to 12	Report and follow up	Deliver first board briefing insert. Follow up with vendors on roadmap request responses. Place non-responding vendors on exception register.	Board insert delivered. Vendor exception register active. PQC migration roadmap draft begun.

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
- Quantum risk register entry with current risk rating and owner
- Board briefing insert from most recent quarterly risk pack

- Quantum Risk Policy Statement or equivalent section in information security policy

Inventory and visibility

- QASI covering all critical systems — with coverage percentage calculated
- System owners confirmed for each QASI row
- Data longevity analysis completed for mortgage, loan, and identity systems
- Risk flags identified and tracked with remediation owners

Vendor management

- Vendor roadmap requests issued to core banking platform, digital banking provider, and certificate authority
- Vendor responses received and filed, or non-responses documented in exception register
- Vendor exception register with compensating controls for each exception
- Any vendor attestations received, signed and filed

Scoring and progress

- Q-Risk Score snapshot — current quarter — with evidence links
- Score movement since prior quarter, if applicable
- 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 proof that the institution can change a cryptographic algorithm on at least one critical system without full platform replacement. QCI-QS1-A v2.1 Section 4 defines five required components for a passing proof: (1) algorithm change capability demonstrated in a staging environment with documented steps; (2) a written, version-controlled operational runbook covering the change and rollback procedure; (3) a tested rollback with recorded completion time; (4) a performance impact measurement showing latency and throughput before and after the change in a load-representative environment; and (5) trust chain validation confirming downstream systems remain functional after the change. No financial institution in this sector can demonstrate all five components for core banking systems today — that is a vendor constraint. But institutions can demonstrate them for systems they control directly, such as internal identity systems or web application certificate configurations. Completing the proof on even one such system clears the score ceiling at 80 and creates a documented foundation for the vendor conversations that are coming.

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 data longevity obligations make harvest-now, decrypt-later exposure material and long-lived, and your examiners will eventually ask questions you should already have answers to.

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, and build examination-ready documentation packages. Contact QCI to discuss how an engagement is structured for institutions of your size and complexity.