QUANTUM CORE INSTITUTE

# QCI-QS1-S1 · Regulatory Crosswalk

**Mapping the QCI-QS1 Standard to the NCUA's Current Examination Framework**

Financial Institutions Supplement — Credit Unions and State-Chartered Banks

| | |
|---|---|
| **Document ID** | QCI-QS1-S1 Annex R (Regulatory Crosswalk) |
| **Version** | 1.2 |
| **Status** | Public — free to download and cite |
| **Normative reference** | QCI-QS1 Quantum Readiness and PQC Governance Standard, v2.2 |
| **Applies to** | Federally insured credit unions, state-chartered banks, CUSOs, and their technology service providers |
| **Regulatory currency** | Reflects the NCUA Information Security Examination (ISE) program and FFIEC IT Handbook as of June 2026 |
| **Review cycle** | Annual, or upon material NCUA, FFIEC, or state regulatory developments |

## 1. Purpose and scope

This crosswalk shows how the QCI-QS1 standard satisfies the controls and expectations a credit union faces in an NCUA examination. It is built for one job. A compliance officer should be able to walk into an exam and point to the QCI-QS1 artifact that answers each examiner question.

QCI-QS1 is not a regulation. It is a governance standard that produces the evidence regulators ask for. This document maps that evidence to the NCUA's live examination references, not to deprecated guidance.

> **What this anchors to**
> The NCUA examines credit unions using the Information Security Examination (ISE) program, supported by 12 CFR Parts 748 and 749, the FFIEC IT Examination Handbook, and the agency's own supervisory letters. This crosswalk maps to those sources. It does not rely on Appendix A to Part 748, which the NCUA proposed to remove in December 2025. See the currency note in Section 6.

## 2. The NCUA examination framework in 2026

The NCUA standardized its information security examinations in 2023. The ISE program replaced the older patchwork of review approaches. It scales by asset size and risk across three tiers.

| ISE tier | Who it applies to and what it covers |
|---|---|
| SCUEP | Small Credit Union Examination Program. Credit unions under $50 million in assets. Focuses on the core security program and records preservation under 12 CFR Parts 748 and 749. |

| ISE tier | Who it applies to and what it covers |
|---|---|
| CORE | Credit unions over $50 million in assets. The baseline risk-focused exam. This is where cybersecurity governance, vendor management, and operational resilience controls are assessed. |
| CORE+ | Extended review applied based on risk. Adds deeper coverage of data governance, change and configuration management, logging and monitoring, and vulnerability and patch management. |

Examiners draw on a defined set of references during an ISE review. The crosswalk in Section 3 maps QCI-QS1 to these.

| Reference | Role in the current examination |
|---|---|
| ISE procedures | The live examination workflow since 2023. Organized into control statements and components across the three tiers. |
| 12 CFR Part 748 | Security program rule. Includes the 72-hour cyber incident reporting requirement at 748.1(c), effective September 2023. |
| 12 CFR Part 749 | Records preservation rule. Sets retention obligations that drive data longevity exposure. |
| FFIEC IT Examination Handbook | Reference material examiners use. Key booklets include Architecture, Infrastructure, and Operations (2021) and Development, Acquisition, and Maintenance (2024). |
| ACET | Automated Cybersecurity Evaluation Toolbox. A voluntary maturity self-assessment that prepares a credit union for the ISE. |
| Supervisory Letter 07-01 | Evaluating Third Party Relationships. The anchor for vendor and service-provider oversight expectations. |
| NIST, CIS, CISA | Industry frameworks the ISE references for control selection and testing. |

## 3. Crosswalk: NCUA expectations to QCI-QS1

Each row pairs an examination expectation with the QCI-QS1 component that satisfies it and the artifact that proves it. Read it left to right. The examiner asks. The standard answers. The artifact is the evidence.

| NCUA examination expectation | What the examiner looks for | QCI-QS1 component | Evidence artifact |
|---|---|---|---|
| Board governance over information security (ISE objective; Part 748 security program) | Named accountability, board reporting cadence, approved risk appetite | QRAF Clause 4.1 governance ownership; Board Insert Clause 8 | Quantum risk policy statement; quarterly board briefing insert |
| Documented information security program and risk assessment (ISE CORE; Part 748) | A program that identifies, assesses, and controls information system risk | QRAF Clause 4.2 governance artifacts; QASI Clause 5 inventory | QASI inventory; quantum risk register section |

| NCUA examination expectation | What the examiner looks for | QCI-QS1 component | Evidence artifact |
|---|---|---|---|
| Data governance and classification (ISE CORE+ data governance component) | Data identified, classified, and protected across its lifecycle | QASI Clause 5.2 data classification and longevity fields | QASI rows with classification and data longevity values |
| Third-party and vendor management (ISE CORE+; Supervisory Letter 07-01) | Due diligence and ongoing oversight of technology service providers | QRAF D5 third-party exposure; Vendor Pack Clause 7 | Vendor Roadmap Request Pack responses; signed attestations; exception register |
| Operational resilience and business continuity (ISE CORE) | Resilience of identity, payment, and member-facing systems to disruption | QRAF D7 incident and resilience; Q-Risk Score Pillar 4 | Incident runbook; crypto agility test evidence |
| Cyber incident reporting (12 CFR 748.1(c), 72-hour rule) | A response program able to detect and report a reportable cyber incident | QRAF D7 detection and response; crypto incident scenario | Incident playbook covering cryptographic failure and mass certificate events |
| Security testing of key controls (ISE testing requirement; GLBA safeguards) | Evidence that key controls are tested and function as expected | Q-Risk Score comparability controls (agility test before scoring above 80) | Crypto agility proof; test reports for a critical trust pathway |
| Reporting to the board (ISE; safeguards expectation, at least annually) | Evidence-driven reporting that informs board oversight | Board Insert Clause 8; Q-Risk Score quarterly snapshot | Quarterly board insert; Q-Risk Score snapshot with deltas |
| Records preservation (12 CFR Part 749) | Retention of vital records, with confidentiality obligations that can span decades | QASI data longevity fields; HNDL risk flag | Data longevity mapping; harvest-now-decrypt-later exposure analysis |

## 4. FFIEC IT Handbook booklet mapping

ISE CORE+ procedures echo the FFIEC booklets directly. These are the booklets most relevant to quantum and cryptographic risk, with the QCI-QS1 components that align to each.

| FFIEC booklet | Examiner focus relevant to cryptographic risk | QCI-QS1 support |
|---|---|---|
| Architecture, Infrastructure, and Operations (2021) | Change and configuration management, logging and monitoring, vulnerability and patch management, and the interconnectedness of assets, processes, and third parties | QASI crypto visibility (D2); crypto agility (D4, Pillar 4); Vendor Pack third-party exposure (D5) |

| FFIEC booklet | Examiner focus relevant to cryptographic risk | QCI-QS1 support |
|---|---|---|
| Development, Acquisition, and Maintenance (2024) | System development lifecycle and supply chain risk management for software and third-party platforms | QASI crypto library and SBOM fields; Vendor Pack SBOM and roadmap questions |
| Information Security (2016) | Encryption, key management, and authentication controls within the information security program | QASI crypto function, key management, and identity dependency fields (D2, D6) |

## 5. The records and longevity hook

This is the point that lands hardest in a credit union exam. A 30-year mortgage creates a confidentiality obligation measured in decades. Part 749 governs records preservation. Member authentication data, transaction records, and identity verification tied to that loan must stay protected long after the loan closes.

Harvest-now-decrypt-later turns that obligation into a present-tense problem. An adversary can collect encrypted member data today and decrypt it later. The data created in 2026 that must remain confidential until 2056 is exposed the moment it crosses a network, not the day a quantum computer arrives.

> **Why this maps cleanly**
> QASI already captures data longevity and an HNDL risk flag for every system. That is the exact field an examiner needs to see when assessing whether long-lived member data sits on a non-PQC cryptographic path. The standard was built to answer this question before it was asked.

## 6. A note on regulatory currency

Two recent developments shape how this crosswalk is anchored.

- The NCUA proposed removing Appendix A to Part 748, the Guidelines for Safeguarding Member Information, from the Code of Federal Regulations in December 2025. The safeguards substance persists in the ISE program and the Part 748 rule, so this crosswalk anchors there rather than to the appendix text.
- The FFIEC Cybersecurity Assessment Tool was retired in 2025. The NCUA's ACET, which was based on that tool, remains available as a voluntary maturity self-assessment. This crosswalk anchors to the ISE program, which is the live examination workflow.

QCI-QS1 maps to disciplines, not to a single citation. Governance ownership, cryptographic inventory, data longevity assessment, vendor attestation, and evidence-backed reporting outlast any individual rule revision. When a reference changes, the mapping is reviewed and updated. The underlying evidence does not move.

## 7. Using this in an examination

Bring this crosswalk and the QCI-QS1 artifacts to the exam together. The crosswalk tells the examiner where to look. The artifacts are the proof. Three practical notes:

- Lead with the Q-Risk Score snapshot and the QASI coverage metric. They answer the examiner's first two questions: where are you, and how do you know.
- Have the vendor exception register ready. Core banking vendor concentration is the most common gap an examiner finds, and the register shows it is managed, not ignored.
- Treat the board briefing insert as the cover sheet. It proves the board receives evidence-driven reporting, which is the governance expectation behind the entire ISE.