

QUANTUM CORE INSTITUTE

QCI-QS1-S6

EU Financial Entities Supplement

DORA Quantum Readiness Alignment

Document ID	QCI-QS1-S6
Version	1.2
Status	Published — For organizational adoption and external reference
Publisher	Quantum Core Institute (QCI)
Normative ref	QCI-QS1 Version 2.3 (September 23, 2026). Clause references are QCI requirement identifiers.
Effective date	September 23, 2026
Companion docs	QCI-QS1-H Practitioner Handbook V2.3 (September 23, 2026) QCI-QS1-S6-P Practitioner Supplement v1.0 (restricted)
Review cycle	Annual, or upon material DORA RTS, ESA oversight, or EU PQC roadmap developments, or a new edition of QCI-QS1

This supplement extends QCI-QS1 for EU financial entities subject to the Digital Operational Resilience Act (DORA). It maps QCI-QS1 requirements to DORA's ICT risk management framework, cryptographic controls mandates, and the EU Coordinated PQC Roadmap milestones. It does not replace QCI-QS1. It translates it for the European regulatory context.

Foreword

DORA is already in force. Financial entities subject to it are not awaiting a future compliance deadline — they are operating under mandatory obligations that include cryptographic controls, crypto agility requirements, and third-party vendor oversight for ICT risk. QCI-QS1 was designed to be auditable, repeatable, and comparable across institutions. This supplement makes that design visible in DORA's language.

The alignment is closer than most entities realize. DORA's RTS Article 6 requires a documented cryptographic controls policy, provisions for updating cryptographic technology based on cryptanalysis developments, and a flexible approach to quantum threats. QCI-QS1's QASI, Q-Risk Score, and governance framework satisfy these requirements directly. This supplement shows where and how.

What changed in version 1.2

Version 1.2 aligns this supplement to QCI-QS1 version 2.3. Clause references are now QCI requirement identifiers. The review-date targets in section 5.2 are restated for the fixed Core profile: the Defensible readiness band begins at 81, gate G60 is fixed at 95 percent validated coverage of both critical systems and critical flows, and gate G70 is no longer satisfied by a documented exception — an entity with an unattested critical third-party provider is capped at 70 whatever else it has done. The RTS Article 6.4 mitigation record maps to the exception register of QCI-4.3-02 rather than a separate vendor register. The crypto agility evidence expected at 2029 to 2030 is the representative end-to-end test of QCI-4.7 that gate G80 requires. Section 2.6 seeds the obligations register QCI-2.2-01 requires, and the EU Coordinated PQC Roadmap is cited as Annex E reference S17.

1. Scope and applicability

This supplement applies to all financial entities within the scope of DORA (Regulation (EU) 2022/2554) and the associated Regulatory Technical Standards (Commission Delegated Regulation (EU) 2024/1774). This includes banks, insurance undertakings, investment firms, payment institutions, electronic money institutions, crypto-asset service providers, central counterparties, central securities depositories, and ICT third-party service providers serving these entities.

The supplement is relevant at two levels. First, for entities completing a QCI-QS1 assessment: it shows how each QCI-QS1 requirement maps to a specific DORA obligation, so that assessment outputs can be used directly in supervisory reporting and examination preparation. Second, for entities that are beginning their DORA cryptographic controls compliance program: QCI-QS1 provides the governance structure, inventory methodology, and scoring mechanism that DORA requires but does not prescribe.

Who this supplement is for

EU financial entities with DORA obligations — including those already past the January 17, 2025 compliance date who are now building evidence for supervisory review. Also relevant for ICT third-party service providers designated or potentially designatable as Critical Third-Party Providers (CTPPs) under DORA's Article 31 oversight framework.

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. They govern cryptographic risk arising from AI systems. They do not govern AI risk generally.

2. DORA regulatory context

2.1 The five DORA pillars and QCI-QS1 relevance

DORA organizes its requirements around five pillars. Quantum readiness and cryptographic controls appear primarily in Pillar 1, but the exposure extends across all five.

DORA pillar	Core obligation	QCI-QS1 relevance
1. ICT risk management	ICT risk framework, encryption policy, crypto key management, certificate register, crypto agility (Articles 5–14, RTS Arts 6–7)	Governance under QCI-4.1; QASI inventory under Clause 5; Q-Risk Score pillars P1–P3; approved profiles and key lifecycle under QCI-4.5 and 4.6
2. ICT-related incident management	Classification, reporting, and root cause analysis of ICT incidents including cryptographic failures (Articles 17–23)	Incident readiness under QCI-4.4-01 and 4.4-02; QRAF domain D7; Q-Risk Score P4 secondary input
3. Digital operational resilience testing	Threat-led penetration testing, resilience testing for critical systems (Articles 24–27)	Test categories and acceptance under QCI-4.7; gate G80 representative end-to-end test; Q-Risk Score P4 Level 4–5 evidence
4. ICT third-party risk management	Vendor contracts, ICT Register of Information, CTPP oversight (Articles 28–44)	Supplier engagement under QCI-7.1 and 7.2 (Annex C request pack); gate G70; Q-Risk Score P5; QASI supplier records
5. Information sharing	Sharing of cyber threat intelligence on voluntary basis (Article 45)	Not directly mapped; informative for threat horizon monitoring

2.2 RTS Article 6: Encryption and cryptographic controls

Commission Delegated Regulation (EU) 2024/1774, Article 6 is the primary DORA obligation for quantum readiness. It requires financial entities to develop, document, and implement a policy on encryption and cryptographic controls. That policy must contain:

- Rules for encryption of data at rest, in transit, and in use
- Provisions for cryptographic key management across the full lifecycle
- Provisions for updating or changing cryptographic technology based on developments in cryptanalysis — which explicitly includes quantum threats per Recital 9
- Criteria for selection of cryptographic techniques based on data classification and ICT risk assessment
- A requirement to record mitigation and monitoring measures where cryptographic technology cannot be updated, with documented justification

The last two points are particularly significant. An entity that cannot migrate a system because of a vendor constraint is not excused — it must document the constraint, implement

compensating controls, and record the rationale. This is the DORA equivalent of the QCI-QS1 exception register (QCI-4.3-02), with its review triggers, expiry and exit path.

QCI-QS1 alignment: Article 6

The QASI directly satisfies the Article 6 inventory and classification requirements. The approved cryptographic profile of QCI-4.5-01 is the Article 6 selection criteria in documentary form. The QASI treatment status (QCI-5.3-02) and the exception register (QCI-4.3-02) map to the RTS requirement to document systems that cannot be updated and the mitigations in place. The Annex C request pack and the attestation of QCI-7.2-02 satisfy the vendor engagement and attestation dimension of Article 6's third-party crypto controls requirements.

2.3 RTS Article 7: Cryptographic key management

Article 7 requires financial entities to identify and implement controls protecting cryptographic keys across their whole lifecycle, and to maintain a register of all certificates and certificate-storing devices for systems supporting critical or important functions. This register must be kept current and certificates must be renewed proactively before expiration.

For QCI-QS1 practitioners, this is the key and trust lifecycle requirement of QCI-4.6-01 and 4.6-02 and the identity records of QCI-5.2-02 in DORA form. The QASI certificate and key records satisfy Article 7 when completed for all systems supporting critical or important functions. An entity with incomplete QASI coverage for those systems is in breach of Article 7, not just short of gate G60. Note also QCI-4.6-03: re-wrapping stored data under a new key does not remediate copies already harvested, and the Article 7 register should not be read as implying that it does.

2.4 CTPP designation and third-party quantum risk

DORA's Critical Third-Party Provider (CTPP) designation framework creates a new category of vendor risk for EU financial entities. The European Supervisory Authorities designated the first cohort of CTPPs in November 2025. Financial entities that rely on a CTPP for ICT services supporting critical or important functions inherit the CTPP's cryptographic posture as a direct regulatory exposure.

The DORA supervisory framework will scrutinize whether financial entities have collected PQC roadmap commitments from their CTPPs. Entities without documented CTPP engagement on quantum readiness are exposed to examination findings regardless of their internal program maturity.

CTPP engagement requirement	QCI-QS1 mechanism
Document all ICT arrangements with CTPPs in the Register of Information	QASI supplier records; map CTPPs to QASI records for critical systems and flows
Assess CTPP crypto agility and PQC roadmap posture	Annex C request pack; adequacy criteria of QCI-7.2-02; QASI PQC support status field
Maintain the mitigation record for CTPPs without adequate roadmaps	Exception register under QCI-4.3-02 with compensating controls, review triggers and exit path; QCI-7.3-01 handling of non-response; Q-Risk Score P5 scoring. The exception does not satisfy gate G70.
Include CTPP exceptions in management body reporting	Governing-body insert (Annex D, QCI-8.1-01); quarterly Q-Risk scorecard supplier readiness field

2.5 The EU Coordinated PQC Roadmap

The EU NIS Cooperation Group published the Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography in June 2025 (QCI-QS1 Annex E, reference S17). This roadmap is not a DORA instrument, but it establishes the supervisory expectation for the timeline of cryptographic migration across the EU financial sector. Supervisory authorities will use it as a benchmark.

EU PQC milestone	What it requires	QCI-QS1 program action
By 31 December 2026	National PQC strategies initiated; inventories begun; pilots launched for high- and medium-risk use cases	QASI validated for critical systems and flows; Q-Risk Score baseline established with assessment type; at least one crypto agility pilot underway under QCI-4.7
By 31 December 2030	High-risk use cases — including critical financial systems — migrated to PQC; quantum-safe upgrades enabled by default for new products	P4 Level 3 or higher achieved for critical systems; PQC migration milestones delivered on the approved profile; supplier attestations current under the annual refresh
By 31 December 2035	Full transition complete for as many medium- and low-risk systems as practicable	P4 Level 4–5 across all scoped systems; representative end-to-end tests passed across all critical trust pathways

The 2030 deadline for high-risk financial systems is the operating assumption for any EU financial entity conducting a QCI-QS1 assessment today. A P4 score below Level 3 for systems handling long-lived regulated data should be treated as a 2030-deadline risk, not a general operational improvement goal.

2.6 Obligations register entries for DORA entities

QCI-2.2-01 requires 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 minimum entries for a DORA entity:

Obligation	Issuer and document	Status	Affected systems and suppliers	Action and deadline
ICT risk management framework; management body accountability; incident management; resilience testing; third-party risk	Regulation (EU) 2022/2554 (DORA), Arts 5–45	Regulation, in application since 17 January 2025	All ICT supporting critical or important functions; all ICT third-party providers	Maintain the evidence pack in section 8; quarterly management body reporting
Encryption and cryptographic controls policy; key management and certificate register	Commission Delegated Regulation (EU) 2024/1774, Arts 6–7	Regulation	All critical or important function systems and their certificates	Policy documented; certificate register current; Art 6.4 mitigation records in the exception register

Obligation	Issuer and document	Status	Affected systems and suppliers	Action and deadline
CTPP oversight; Register of Information	DORA Arts 28–44; ESA CTPP designations (first cohort November 2025)	Regulation; designation list maintained by the ESAs	CTPP-delivered services	Register of Information submitted; Annex C requests to every CTPP with the 60-day deadline
Coordinated PQC transition	NIS Cooperation Group Coordinated Implementation Roadmap, June 2025 (Annex E S17); Commission Recommendation (EU) 2024/1101	Recommendation and roadmap; supervisory benchmark	All quantum-vulnerable systems	Inventory and pilot by end 2026; high-risk migration by end 2030; full transition by end 2035

3. DORA-specific vendor engagement

3.1 How DORA changes the vendor conversation

The US sector supplements frame vendor engagement as a risk management best practice. DORA makes it a legal obligation. Financial entities are legally responsible for their vendors' cryptographic posture for systems supporting critical or important functions. A vendor that cannot provide a PQC roadmap and attestation is not merely a risk gap — it is a documented DORA exception requiring compensating controls and management body visibility, and under QCI-QS1 it holds the entity's score at or below 70 until the attestation arrives.

This changes the leverage dynamic. When issuing an Annex C request to a vendor under DORA, the entity is not making a discretionary request. It is fulfilling a supervisory obligation. The vendor's response — or non-response after the 60-day deadline of QCI-7.2-04 — becomes a regulatory artifact.

3.2 CTPP-specific engagement considerations

For vendors designated as CTPPs, the engagement dynamic is different again. CTPPs are under direct ESA oversight and are aware of the scrutiny on their cryptographic posture. They are more likely to have PQC roadmap documentation than non-designated vendors, but the documentation may be generic and may not address the financial entity's specific products and versions. QCI-7.2-02 sets the test: a response is adequate only if it is product- and version-specific, dated, and attested by an officer.

- Request product-specific PQC roadmaps, not corporate-level statements. A CTPP's enterprise PQC strategy does not constitute a roadmap for the specific product versions in your environment, and it does not pass the adequacy criteria.
- Include the CTPP designation in the attestation request. Ask the CTPP to confirm that the attestation covers the specific products referenced in your ICT Register of Information.
- Set a contractual milestone. DORA Article 30 requires ICT contracts to include provisions for termination rights and exit plans. Use contract renewal as the moment to embed PQC milestone commitments and the notification, evidence-access and annual re-attestation terms QCI-7.1-02 expects.

- Escalate unresponsive CTPPs to your competent authority relationship. A CTPP that will not engage on PQC is a supervisory finding waiting to happen, and early documentation of the outreach protects the entity.

4. DORA-specific QASI field guidance

The QASI record groups in QCI-QS1 Clause 5.2 satisfy DORA's inventory requirements when completed for systems supporting critical or important functions and for the critical flows between them. The fields below require EU-specific interpretation.

QASI field	Standard QCI-QS1 interpretation	DORA-specific guidance
Business criticality	High / Medium / Low against the criteria declared under QCI-1.1-02	Map to DORA's 'critical or important functions' definition. If a function is classified as critical or important under DORA, the system is High criticality for QASI purposes regardless of internal classification.
Confidentiality and verification horizons	Dates by which data must remain confidential, and signatures verifiable	Apply the DORA data classification output. The RTS requires crypto controls to be designed based on approved data classification results. Link each horizon entry to the entity's formal data classification artifact.
Critical flows	Flows between critical systems with protection and authentication at each hop	Payment rails, market data feeds, CTPP-hosted services and intra-group links are flows. Coverage of flows is computed separately from systems (QCI-5.1-03) and gate G60 requires both.
Supplier dependencies	Critical suppliers for crypto or communications	List CTPP designation status explicitly. Mark each CTPP dependency with 'CTPP designated' or 'CTPP assessment pending'. This field is an input to the ICT Register of Information submission.
PQC support status	None / roadmap / pilot / available	Add the vendor roadmap date and the attestation receipt date as sub-fields. Supervisory examination will ask for dated evidence of vendor engagement, not just status labels.
Crypto agility status	None / partial / proven, against the QCI-4.7 test categories	'Proven' means a representative end-to-end test under QCI-4.7 passed within the last 12 months. 'Partial' must specify which test categories are complete and which are outstanding. 'None' requires a treatment entry (QCI-5.3-02) and, where the constraint is external, an exception per RTS Article 6.4 and QCI-4.3-02.

5. Q-Risk Score guidance for EU financial entities

5.1 How DORA maps to Q-Risk Score pillars

The Q-Risk Score's five pillars map to DORA obligations at different levels of specificity. The table below shows the primary DORA article driving each pillar and the examination implication.

Pillar	Primary DORA obligation	Examination implication	Realistic starting band for EU entities
P1. Governance	Arts 5–6 DORA: management body accountability; ICT risk policy; quarterly board reporting	Examiner will ask for evidence of named ownership and reporting cadence. A quantum risk register entry without a named owner fails.	Mobilizing (40–59) for large entities with existing ICT governance; Behind (20–39) for smaller entities
P2. Crypto visibility	RTS Art 6–7: cryptographic policy; certificate register; SBOM-equivalent crypto inventory	Examiner will request the certificate register mandated by RTS Art 7.4. Absence is a direct breach, not a gap.	Behind (20–39) across all entity types — crypto inventory is consistently the weakest starting position
P3. Data horizons	RTS Art 6.2: data classification linked to crypto controls; exposure mapping	Examiner will ask how data classification outputs drove cryptographic control selection. Circular references fail.	Behind to Mobilizing depending on existing data classification program maturity
P4. PQC migration	RTS Art 6.3: provisions for updating crypto on cryptanalysis developments; quantum threat mandate	Examiner will ask for the entity's PQC migration roadmap and evidence of progress against the EU 2026 milestone.	Exposed to Behind (0–39) for most EU entities — the 2026 milestone is the near-term bar
P5. Third-party readiness	Arts 28–30 DORA: ICT vendor contracts; CTPP engagement; ICT Register of Information	Examiner will request evidence of roadmap requests for CTPP and other critical vendors. Non-responses are exceptions requiring documentation, and they cap the score.	Exposed to Behind — CTPP designation is recent and most entities have not yet collected attestations

5.2 Realistic band targets under DORA pressure

Unlike the US sector supplements, where examination pressure is emerging, EU financial entities face supervisory examination that is already active. The band targets below reflect what a competent authority examination team will likely find acceptable at specific review dates. They are planning guidance, not Core-profile thresholds (QCI-6.3-02). No score above 80 is possible unless gates G60, G70 and G80 have all passed, and Defensible readiness begins at 81.

Review date	Minimum defensible Q-Risk Score	What examiners will look for
2026 — Post-DORA first cycle	40 to 55 (Mobilizing)	Named ownership, validated QASI for critical systems and flows, at least one supplier request issued with a deadline, management body insert delivered
2027–2028 — Active oversight period	55 to 70 (Mobilizing to Advancing)	Validated coverage at or near 95 percent for systems and flows; CTPP attestations received, with non-responses in the exception register and escalated; first PQC pilot underway
2029–2030 — Pre-2030 milestone	70 to 80 (Advancing), with Defensible readiness reachable once all three gates pass	Critical system migration underway; every critical supplier attested and refreshed annually (G70); representative end-to-end test passed on critical paths within 12 months (G80)
Post-2030	81 or above (Defensible readiness)	Critical systems migrated or on an active PQC path, full CTPP attestation coverage, crypto agility proven across critical trust pathways, independent assessment where the entity claims level 5 on any pillar

6. Governance model for EU financial entities

DORA places direct accountability for ICT risk on the management body. This is not an IT governance obligation — it is a board-level obligation. The management body must approve ICT risk policies, allocate adequate ICT budgets, and receive regular reporting on ICT risk including cryptographic controls.

The governance requirements of QCI-4.1 satisfy this directly. The mapping of required roles to DORA obligations:

QCI-QS1 required role	DORA obligation	EU-specific note
Governing body (management body)	Management body oversight under DORA Art 5; quarterly ICT risk reporting	DORA uses 'management body' to mean the board or equivalent governing body, which is the term QCI-QS1 v2.3 uses. Supervisory bodies are also included in some entity types. Accepted risk is approved explicitly (QCI-8.2-01).
Executive Sponsor (CISO/CIO/CRO)	Management body delegate for ICT risk per DORA Art 5(4); accountable for ICT risk framework	DORA Art 5(4) allows delegation but not abdication. The management body remains liable.
Quantum Risk Owner	ICT risk management function per DORA Art 6(4)	Map to existing DORA ICT risk function where possible. Avoid creating a parallel governance structure.
Procurement and Vendor Risk	ICT third-party risk management per DORA Arts 28–30; ICT Register of Information maintenance	The Register of Information submission to competent authorities is a mandatory deliverable. Vendor risk must maintain it and the supplier register of QCI-7.1-01 together.
Legal and Compliance	DORA contractual requirements per Art 30; data classification per RTS Art 6.2	EU governing law provisions and DORA-specific contract clauses are required for ICT arrangements. Legal must review all critical vendor contracts for the QCI-7.1-02 terms.

7. The DORA 90-day quick start

EU financial entities that have not yet established a quantum readiness program are operating in breach of DORA's cryptographic controls obligations. The sequence below prioritizes producing the evidence artifacts that a competent authority examination will request, while simultaneously building the program foundation. It adapts QCI-QS1 Clause 9.1 and is a planning aid, not a conformance grace period.

Weeks	Phase	Priority actions	DORA artifact produced
1 to 2	Establish	Assign named Quantum Risk Owner with DORA mandate. Declare the assessment boundary and map DORA 'critical or important functions' to the system list (QCI-1.1-01). Seed the obligations register from section 2.6. Note that coverage is fixed at 95 percent of critical systems and flows (G60); there is no threshold to define.	Written scope statement referencing DORA obligations. Named roles documented. Obligations register started.

Weeks	Phase	Priority actions	DORA artifact produced
3 to 6	Inventory	Build linked QASI records for all systems supporting critical or important functions and the critical flows between them. Validate the certificate register (RTS Art 7.4) as the key and trust records of QCI-4.6. Flag all CTPP dependencies.	Validated QASI satisfying RTS Art 7 certificate register requirement. CTPP list with engagement status. Coverage figures for systems and flows.
7 to 9	Analyze	Map data classification outputs to horizon and profile fields (RTS Art 6.2). Raise exposure flags for regulated data with long horizons. Issue Annex C requests to CTPPs and other critical vendors with the 60-day deadline.	Data classification-to-crypto linkage documented. Requests issued with date record and deadline.
10	Score	Produce the first Q-Risk Score, labelled self-assessment (QCI-1.2-03), with gate results. Be honest. A low score with evidence is a defensible DORA posture. A high score without evidence is a supervisory liability.	Q-Risk Score snapshot with evidence links, assessment type and conformance status. Scoreable against DORA pillar mapping.
11 to 12	Report	Deliver the first management body insert with DORA framing. Record vendor responses; open the exception register (QCI-4.3-02) for non-responses. Build the PQC migration roadmap draft aligned to the 2026 EU milestone with milestone types per QCI-4.2-02. Diary the annual supplier refresh.	Management body insert satisfying DORA Art 5 reporting obligation. Exception register. Migration roadmap.

The DORA evidence posture

DORA supervisory examination will not accept narrative descriptions of intent. It requires dated, retrievable artifacts: the QASI with named owners and evidence links, the certificate register, the supplier request records with dates, the management body minutes showing quantum risk was discussed. Every QCI-QS1 artifact is designed to be that kind of evidence, and QCI-4.8-01 sets the retrievability rule. The 90-day sequence above produces a complete first-cycle evidence pack.

8. DORA examination preparation checklist

The items below reflect what a competent authority examination team, applying DORA's ICT risk management RTS, is likely to request during an on-site or documentary inspection of cryptographic controls. Produce these artifacts before examination, not in response to a request.

Governance artifacts

- Written quantum risk policy statement referencing DORA cryptographic controls obligations
- Named Quantum Risk Owner with documented mandate, including DORA ICT risk function alignment
- Management body or risk committee minutes showing quantum risk was discussed and the Q-Risk Score was reviewed
- Exception register under QCI-4.3-02 with review triggers, expiry and exit path for each entry

Inventory artifacts

- Validated QASI records for all systems supporting critical or important functions and their critical flows, each with a named system owner and a validation date within 90 days

- Certificate register satisfying RTS Art 7.4 — all certificates for critical systems, with owner, expiry date, and renewal status
- CTPP designation status for all supplier dependencies in the QASI
- ICT Register of Information (required for competent authority submission)

Cryptographic controls artifacts

- Documented encryption and cryptographic controls policy per RTS Art 6.1, incorporating the approved cryptographic profile of QCI-4.5-01
- Data classification outputs linked to cryptographic control selections for each QASI record
- Documented mitigation and monitoring measures for any system where cryptographic technology cannot be updated, with rationale (RTS Art 6.4), held in the exception register
- Test and acceptance records under QCI-4.7 for at least one critical trust pathway, including the representative end-to-end test gate G80 requires

Vendor artifacts

- Dated request records for all CTPPs and other critical vendors, with the 60-day deadline
- Supplier attestations received, with signatory name and date, refreshed annually
- Exception register entries for non-responsive or inadequate vendors, with compensating controls documented — noting that these do not satisfy gate G70
- CTPP-specific contract clauses referencing PQC milestones and the QCI-7.1-02 terms where applicable

Management body reporting artifacts

- Quarterly Q-Risk Score snapshots with evidence links and assessment type, archived for minimum five years
- Governing-body insert from each quarter, showing Q-Risk Score movement, gate status and top exposures

9. Summary and engagement

DORA has converted quantum readiness from a risk management best practice into a supervised compliance obligation for EU financial entities. The evidence QCI-QS1 requires — named ownership, validated QASI coverage, supplier attestations, tested crypto agility, quarterly management body reporting — is precisely the evidence a DORA examination will request.

Entities that complete a QCI-QS1 assessment using this supplement will have a defensible, evidence-backed quantum readiness posture that satisfies DORA's cryptographic controls requirements and is aligned to the EU PQC Roadmap milestones through 2030.

Engagement

This supplement provides the framework for EU financial entities to understand and map their DORA quantum readiness obligations. QCI engagements for EU entities provide assessment support, benchmark data against the EU cohort, CTPP-specific vendor engagement guidance, and examination preparation review. Independent assessment under QCI-1.2-03 is available separately. Contact the Quantum Core Institute to discuss scope and timing.

Revision history

Version	Date	Changes
1.2	September 23, 2026	Aligned to QCI-QS1 v2.3: references by requirement identifier; band targets restated for the fixed Core profile (Defensible readiness at 81; G60 at 95 percent for systems and flows; G70 not satisfied by exceptions); RTS Art 6.4 mitigation records mapped to the exception register QCI-4.3-02; crypto agility evidence restated as the QCI-4.7 test categories and gate G80; obligations register section 2.6 added; EU roadmap cited as Annex E S17; flows added to QASI guidance; 60-day deadline and annual refresh; assessment type labelling; governing body terminology; companion documents updated to QCI-QS1-H V2.3 and the restricted practitioner supplement, replacing the retired QCI-QS1-A v2.1.
1.1	June 10, 2026	Aligned to QCI-QS1 v2.2; AI-cryptographic provisions note added.

Independent assessment against QCI-QS1 is performed by the Quantum Core Institute. Scope one at quantumcoreinstitute.com/independent-assessment. An independent assessment is not QCI certification (QCI-1.2-03).