

QUANTUM CORE INSTITUTE

QCI-QS1-S7

EU Critical Infrastructure and Essential Entities Supplement

NIS2 Quantum Readiness Alignment

Document ID	QCI-QS1-S7
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-S7-P Practitioner Supplement v1.0 (restricted)
Review cycle	Annual, or upon material NIS2 implementing act, transposition, or EU PQC roadmap developments, or a new edition of QCI-QS1

This supplement extends QCI-QS1 for essential and important entities subject to the Network and Information Security Directive 2 (NIS2). It maps QCI-QS1 requirements to NIS2's cybersecurity risk management obligations, cryptographic controls mandates, and supply chain security requirements. It does not replace QCI-QS1. It translates it for the NIS2 regulatory context.

Foreword

NIS2 is in force. Essential and important entities across eighteen sectors are operating under mandatory cybersecurity risk management obligations that took effect October 17, 2024. Article 21 of NIS2 specifically requires policies on the use of cryptography and encryption. The Commission Implementing Regulation 2024/2690, which entered into force January 7, 2025, defines the technical and methodological requirements in detail — including asset inventories, cryptographic key lifecycle management, and supply chain security measures.

QCI-QS1 was designed to be auditable, repeatable, and comparable across institutions. This supplement makes that design visible in NIS2 language. The alignment is direct. NIS2's cryptographic controls requirements, supply chain security obligations, and incident response mandates map precisely onto the QCI-QS1 governance requirements, the QASI inventory standard, and the Q-Risk Score pillars. 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 3.2 are restated for the fixed Core profile: Defensible readiness 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 — a supplier on the exception register still caps the score at 70. The supply chain mapping in section 2.4 now points to the supplier requirements of QCI-7.1 and 7.2 and the exception register of QCI-4.3-02. The crypto agility evidence 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. The 2026 amendment proposal COM(2026) 13 is noted as proposed.

1. Scope and applicability

This supplement applies to essential and important entities within the scope of NIS2 (Directive (EU) 2022/2555) and the associated Commission Implementing Regulation (EU) 2024/2690. NIS2 covers entities in eighteen sectors:

- Highly critical sectors (Annex I): energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, ICT service management (B2B), public administration, and space.
- Other critical sectors (Annex II): postal and courier services, waste management, manufacture and distribution of chemicals, food production and distribution, manufacturing of medical devices, computers, electronics, machinery, motor vehicles, and digital providers.

The supplement is relevant at two levels. For entities completing a QCI-QS1 assessment: it shows how each QCI-QS1 requirement maps to a specific NIS2 obligation, so that assessment outputs can be used directly in competent authority reporting and incident notification preparation. For entities beginning their NIS2 cybersecurity risk management program: QCI-QS1 provides the governance structure, inventory methodology, and scoring mechanism that NIS2 requires but does not prescribe.

Who this supplement is for

Essential and important entities with NIS2 obligations across any of the eighteen covered sectors — including those that have not yet established a documented cybersecurity risk management program and are building evidence for competent authority review. Also relevant for ICT service providers and managed security service providers that supply services to NIS2 entities, as NIS2 Article 21(2)(d)

makes supply chain security a mandatory measure.

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. NIS2 regulatory context

2.1 NIS2 structure and quantum relevance

NIS2 organizes cybersecurity obligations around risk management measures (Article 21), incident reporting (Articles 23–24), supply chain security (Article 21(2)(d)), and supervisory accountability (Articles 31–36). Quantum readiness and cryptographic controls appear primarily in Article 21 but the exposure extends across the framework.

NIS2 area	Core obligation	QCI-QS1 relevance
Article 21: Risk management measures	Cryptographic policies, encryption, key management, asset inventory, crypto agility (Art 21(2)(h) and Implementing Reg Arts 4, 7–9)	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
Article 21(2)(d): Supply chain	Security of supply chain including ICT service providers and software suppliers; vendor security practices and contractual requirements	Supplier engagement under QCI-7.1 and 7.2 (Annex C request pack); gate G70; Q-Risk Score P5; QASI supplier records
Articles 23–24: Incident reporting	Significant incident notification within 24 hours (early warning), 72 hours (notification), and 1 month (final report)	Incident readiness under QCI-4.4-01 and 4.4-02; QRAF domain D7; crypto-specific incident scenarios exercised annually
Article 21(2)(c): Business continuity	Backup management, disaster recovery, crisis management including crypto key backup and recovery procedures	QRAF D7; key and trust lifecycle records under QCI-4.6; rollback and fallback documentation under QCI-4.5-03 and 4.7
Articles 31–36: Supervision	Competent authority oversight, peer reviews, on-site inspections, evidence-based compliance demonstration	Q-Risk Score as evidence-backed metric with assessment type (QCI-1.2-03); governing-body insert as governance record

2.2 Implementing Regulation Article 7: Cryptographic controls

Commission Implementing Regulation 2024/2690, Article 7 is the primary NIS2 obligation for quantum readiness. It requires essential and important entities to establish and apply a policy on the use of cryptography and cryptographic controls. That policy must address:

- Selection of cryptographic algorithms, protocols, and key lengths based on current best practice and the entity's risk assessment

- Management of cryptographic keys across the full lifecycle — generation, storage, archival, retrieval, distribution, retirement, and destruction
- Provisions for updating or replacing cryptographic mechanisms as cryptanalysis develops, which the implementing regulation's recitals explicitly include quantum computing threats
- Encryption of data at rest, in transit, and where applicable in use, based on data classification
- Documentation and review of systems where cryptographic technology cannot be updated, with compensating controls and rationale

QCI-QS1 alignment: Article 7

The QASI directly satisfies the Article 7 inventory and classification requirements. The approved cryptographic profile of QCI-4.5-01 is the Article 7 selection policy in documentary form. The QASI treatment status (QCI-5.3-02) and the exception register (QCI-4.3-02) map to the implementing regulation's 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 supply chain cryptographic controls dimension of Article 7 when applied to critical ICT service providers.

2.3 Implementing Regulation Article 8: Key management and certificate lifecycle

Article 8 requires entities to maintain documented procedures for cryptographic key management and certificate lifecycle management. 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. The QASI certificate and key records satisfy Article 8 when completed for all systems supporting essential functions. An entity with incomplete QASI coverage for those systems has a direct Article 8 gap, not just a scoring weakness.

Article 8 also requires entities to monitor certificate expiry proactively and to renew certificates before expiration in a controlled manner. This is directly relevant to quantum readiness: as PQC certificate standards mature, entities will need to execute coordinated certificate lifecycle transitions. The QASI certificate inventory is the prerequisite for managing that transition without operational disruption, and QCI-4.6-02 requires the migration path for each trust anchor to be recorded.

2.4 Article 21(2)(d): Supply chain security

NIS2 Article 21(2)(d) makes supply chain security a mandatory cybersecurity risk management measure. Entities must address security in their supply chain, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers. The implementing regulation requires entities to assess their ICT service providers' security practices, including cryptographic controls.

This provision creates a direct regulatory mandate for the QCI-QS1 supplier request. When an entity issues an Annex C request under NIS2, it is not making a discretionary risk management choice — it is fulfilling a mandatory supervisory obligation. A vendor's failure to respond or provide an adequate roadmap becomes a documented exception requiring compensating controls and management body visibility. It also caps the entity's Q-Risk Score at 70 (gate G70); the documented exception is the right record, but it does not lift the cap.

NIS2 supply chain requirement	QCI-QS1 mechanism	Evidence artifact
Assess ICT service provider cryptographic practices	Annex C request pack: standardized question set covering crypto footprint and PQC roadmap (QCI-7.2-01)	Dated supplier request records and responses
Contractual security requirements for critical suppliers	QCI-7.1-02 contract terms; attestation format requiring officer signature (QCI-7.2-02)	Signed supplier attestations and contract amendments
Vendor exception management for non-responsive suppliers	QCI-7.3-01 handling of non-response after the 60-day deadline; exception register under QCI-4.3-02 with compensating controls, review triggers and exit strategy	Exception register with management body visibility
Monitor supplier security posture on ongoing basis	Q-Risk Score P5 quarterly reassessment; annual attestation refresh (QCI-7.2-04); QASI supplier record currency checks	Quarterly Q-Risk scorecard showing P5 movement and gate G70 status

2.5 The EU Coordinated PQC Roadmap and NIS2

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 sets the supervisory expectation for the timeline of cryptographic migration across NIS2-covered sectors. While it is not a legally binding NIS2 instrument, competent authorities will use it as a benchmark when assessing whether entities have taken appropriate and proportionate technical measures under Article 21. A proposed amendment to NIS2, COM(2026) 13 of January 20, 2026, would anchor the directive to the roadmap and reaffirm its 2030 and 2035 targets; it is proposed, and should be recorded in the obligations register as such until adopted.

EU PQC milestone	What it requires	QCI-QS1 program action
By December 31, 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 December 31, 2030	High-risk use cases — including critical infrastructure 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 December 31, 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

2.6 Obligations register entries for NIS2 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 NIS2 entity; each entity adds its Member State transposition and any sector-specific instrument:

Obligation	Issuer and document	Status	Affected systems and suppliers	Action and deadline
Cybersecurity risk management measures; management body accountability; incident reporting; supervision	Directive (EU) 2022/2555 (NIS2), Arts 20–24, 31–36, as transposed	Directive in application since 17 October 2024; cite the national transposition	All network and information systems supporting essential or important functions	Maintain the evidence pack in section 8; management body reporting; 24-hour, 72-hour and one-month incident timelines
Cryptographic policy; key and certificate lifecycle; asset inventory; supply chain	Commission Implementing Regulation (EU) 2024/2690, Arts 4, 7–9	Regulation, in force since 7 January 2025 (applies directly to the entity types it names)	All systems supporting essential functions and their ICT service providers	Policy documented; certificate inventory current; supplier assessments with Annex C requests
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
NIS2 amendment	COM(2026) 13, proposed 20 January 2026	Proposed; not yet adopted — verify status at each review	Scope additions as adopted	Track; no action until adoption
Sector layering (where applicable)	Network Code on Cybersecurity, Implementing Regulation (EU) 2024/1366 (electricity); MDR/IVDR (medical devices)	Regulation	Sector-specific systems	Record alongside NIS2 with the sector regulator as issuer

3. Q-Risk Score in the NIS2 context

3.1 How NIS2 supervision reads the Q-Risk Score

NIS2 competent authorities do not have a standardized quantum readiness scoring framework. The Q-Risk Score provides a structured, evidence-backed metric that entities can use to demonstrate systematic risk management. The five pillars map to NIS2's Article 21 measures in a way that makes the score auditable and defensible in a supervisory context, provided it is reported with its assessment type and conformance status beside it (QCI-1.2-03, QCI-1.2-04).

Q-Risk pillar	NIS2 alignment	Examination signal	Typical NIS2 starting band
P1. Governance	Art 21(1): management body accountable; Art 20: cybersecurity training for management	Competent authority will look for named accountability and evidence of management body engagement	Behind (20–39) — most entities have general cyber governance but no quantum-specific ownership

Q-Risk pillar	NIS2 alignment	Examination signal	Typical NIS2 starting band
P2. Crypto visibility	Implementing Reg Art 7–8: cryptographic policy; certificate register; asset inventory	Competent authority will request the cryptographic asset inventory. Absence of any crypto-specific inventory is a direct Art 7 gap.	Behind (20–39) — general asset inventories exist but crypto-specific fields are systematically absent
P3. Data horizons	Implementing Reg Art 7.2: data classification linked to crypto selection; exposure mapping	Competent authority will ask how data classification outputs drove cryptographic control selection. Circular references fail.	Behind to Mobilizing — data classification programs exist but the crypto linkage is absent
P4. PQC migration	Implementing Reg Art 7.1(c): provisions for updating crypto on cryptanalysis developments; EU 2026 milestone	Competent authority will ask for the entity's PQC migration roadmap and evidence of progress against the 2026 EU milestone.	Exposed to Behind (0–39) — the 2026 milestone is the immediate bar for most entities
P5. Third-party	Art 21(2)(d): supply chain security; ICT service provider assessment	Competent authority will request evidence of vendor cryptographic controls assessment. Non-responses are exceptions requiring documentation, and they cap the score.	Exposed to Behind — vendor crypto assessments are rarely conducted systematically

3.2 Band targets under NIS2 supervision

NIS2 applies a proportionality principle: essential entities face higher expectations than important entities. The band targets below reflect what a competent authority supervision team will likely find defensible at specific review dates, differentiated by entity tier. They are planning guidance, not Core-profile thresholds (QCI-6.3-02); the gates and the 81-point Defensible readiness threshold apply equally to both tiers.

Review date	Essential entity minimum	Important entity minimum	What supervisors look for
2026 — First NIS2 cycle	40 to 55 (Mobilizing)	30 to 45 (Behind to Mobilizing)	Named ownership, validated QASI for critical systems and flows, at least one supplier request issued with a deadline, management body briefing delivered
2027–2028 — Active oversight	55 to 70 (Mobilizing to Advancing)	45 to 60 (Mobilizing)	Validated coverage at or near 95 percent for systems and flows; supplier attestations received, with non-responses on the exception register and escalated; first PQC pilot underway
2029–2030 — Pre-2030 milestone	70 to 80 (Advancing), Defensible readiness reachable once all three gates pass	60 to 75 (Advancing)	Critical system migration underway; every critical supplier attested (G70); representative end-to-end test passed on at least one critical path within 12 months (G80)
Post-2030	81 or above (Defensible readiness)	75 or above (Advancing, into Defensible readiness on passing the gates)	Critical systems migrated or on active PQC path, full supplier attestation coverage, crypto agility proven across critical trust pathways

4. Governance model for NIS2 entities

NIS2 Article 20 places direct accountability for cybersecurity risk management on the management bodies of essential and important entities. Management bodies must approve cybersecurity risk management measures, oversee their implementation, and can be held personally liable for infringements. This is not a delegation to the IT function — it is a board-level obligation with individual accountability.

The governance requirements of QCI-4.1 satisfy this directly. The mapping of required roles to NIS2 obligations:

QCI-QS1 required role	NIS2 obligation	EU-specific note
Governing body (management body)	Management body oversight and approval under NIS2 Art 20; personal liability for infringements	NIS2 uses ‘management body’ broadly — covers directors, senior management, and supervisory boards depending on entity structure. Personal liability is explicit in Art 20(2). Accepted risk is approved explicitly (QCI-8.2-01).
Executive Sponsor (CISO/CIO/CRO)	Management body delegate for cybersecurity risk management; accountable for Art 21 measure implementation	Art 20(1) allows the management body to delegate specific cybersecurity tasks. The management body remains liable regardless of delegation.
Quantum Risk Owner	Named accountability for quantum-specific risk within the Art 21 cybersecurity risk management framework	Map to existing NIS2 cybersecurity function where possible. Avoid creating a parallel governance structure that complicates supervision.
Procurement and Vendor Risk	Supply chain security under Art 21(2)(d); ICT service provider assessment and contractual requirements	NIS2 requires systematic assessment of supplier security practices, not point-in-time reviews. Vendor risk must treat quantum readiness as an ongoing assessment dimension, with the annual refresh of QCI-7.2-04.
Legal and Compliance	Incident reporting obligations under Arts 23–24; competent authority engagement; contractual requirements for ICT service providers	NIS2 incident reporting timelines are strict: 24-hour early warning, 72-hour notification, 1-month final report. Legal must be integrated into the cryptographic incident playbook required by QCI-4.4-01.

5. NIS2-specific vendor engagement

5.1 How NIS2 changes the vendor conversation

Under NIS2, vendor engagement on cryptographic controls is a mandatory supervisory obligation, not a risk management preference. Article 21(2)(d) requires entities to address supply chain security including the relationships with direct suppliers and service providers. The implementing regulation requires documented assessment of ICT service provider security practices.

This creates a clear leverage position when issuing an Annex C request. The entity is fulfilling a statutory obligation. A vendor’s response — or non-response after the 60-day deadline — becomes a dated regulatory artifact. Entities should issue requests on formal letterhead referencing NIS2 Article 21(2)(d) and retain all correspondence with dates.

5.2 Tiering vendor engagement under NIS2

NIS2 does not create a CTPP-equivalent designation list, but it does require entities to assess suppliers of ICT services that are critical to their essential functions. Entities should tier their vendor engagement using the QASI supplier records to identify which suppliers warrant Priority 1 engagement (vendor provides or materially touches cryptography for essential function systems, and is therefore a critical supplier under QCI-7.1-01) versus Priority 2 (vendor dependency is significant but not for essential function systems).

Vendor tier	NIS2 definition	QCI-QS1 engagement requirement
Priority 1: Essential function suppliers	ICT service providers whose services are critical to the entity's essential functions under NIS2 Annex I or II	Full Annex C request pack; officer-level attestation required (QCI-7.2-02); exception register entry under QCI-4.3-02 if no adequate response within 60 days; governing-body insert visibility. These are the suppliers gate G70 counts.
Priority 2: Important function suppliers	ICT service providers whose services support important but non-essential functions	Abbreviated questionnaire drawn from Annex C; roadmap documentation required; exception register entry if inadequate response; management-level visibility
Priority 3: General suppliers	All other ICT service providers	Standard security assessment with PQC readiness question added; no attestation required; flag for Priority 1 review if function classification changes

6. Sector-specific considerations

NIS2 covers eighteen sectors with different regulatory maturity, existing compliance frameworks, and quantum exposure profiles. The following sector notes provide calibration guidance for the most common QCI engagement contexts.

6.1 Energy

Energy entities — electricity, oil and gas, district heating — operate critical infrastructure with long asset lifecycles and embedded cryptographic dependencies in industrial control systems (ICS) and SCADA environments. Quantum exposure is high because ICS cryptography is typically rigid: firmware updates are infrequent, vendor roadmaps are long, and hardware replacement cycles are measured in decades, not years. The control communications themselves are the critical flows.

- OT/ICS: Priority QASI focus: OT/ICS cryptographic dependencies, including proprietary protocols with embedded key management and firmware signing chains (QCI-4.6-02). Consider a separate OT assessment boundary (QCI-1.1-01), as the critical infrastructure supplement QCI-QS1-S4 recommends.
- Vendor gap: Priority vendor engagement: ICS vendors and SCADA platform providers often have the least mature PQC roadmaps of any sector, and under gate G70 an unattested SCADA vendor caps the score at 70.
- Regulatory layering: The EU's Network Code on Cybersecurity (Implementing Regulation 2024/1366) adds sector-specific obligations for electricity entities that layer on top of NIS2 Art 21; record it in the obligations register.

6.2 Health

Health entities face dual quantum exposure: long-lived patient data (often retained for 25 to 75 years depending on jurisdiction) creates long confidentiality horizons, while medical device and clinical system cryptography is often rigid and vendor-controlled. The combination of long horizons and low crypto agility makes health one of the most exposed NIS2 sectors.

- Confidentiality horizons: Priority QASI focus: patient record systems, clinical data repositories, diagnostic imaging storage with long retention requirements; raise the long-horizon flag (QCI-5.3-01) by default.
- MDR/IVDR intersection: The EU Medical Device Regulation (MDR) and In Vitro Diagnostic Regulation (IVDR) create additional cryptographic lifecycle obligations for medical device manufacturers that are separate from NIS2.

6.3 Digital infrastructure and ICT service management

DNS providers, IXPs, cloud providers, data centres, CDNs, and managed security service providers under NIS2 Annex I have dual exposure: their own cryptographic infrastructure and the cryptographic posture of the services they provide to other NIS2 entities. These entities are simultaneously in scope for NIS2 and in scope for their customers' NIS2 vendor engagement obligations.

- Request recipients: Entities in this sector should expect to receive multiple Annex C requests from NIS2-obligated customers, each with a 60-day deadline. A single product-specific, officer-attested response prepared in advance answers all of them.
- Competitive advantage: A proactive PQC roadmap and attestation capability reduces friction across all customer relationships and positions the entity ahead of the mandatory supervisory requirements. A customer cannot score above 70 without it.

7. The NIS2 90-day quick start

Essential and important entities that have not yet established a quantum readiness program may be operating with gaps in their NIS2 Article 21 cryptographic controls compliance. The sequence below prioritizes producing the evidence artifacts that a competent authority supervision will request, while simultaneously building the program foundation. It adapts QCI-QS1 Clause 9.1, is calibrated for an essential entity, and is a planning aid rather than a conformance grace period; important entities can extend timelines by approximately 30 percent.

Weeks	Phase	Priority actions	NIS2 artifact produced
1 to 2	Establish	Assign named Quantum Risk Owner with NIS2 Art 21 mandate. Declare the assessment boundary and map NIS2 'essential 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 NIS2 Art 21 obligations. Named accountability documented. Management body briefing scheduled. Obligations register started.
3 to 6	Inventory	Build linked QASI records for all systems supporting essential functions and the critical flows between them. Document the certificate lifecycle for essential function systems (Implementing Reg Art 8) as the key and trust records of QCI-4.6. Flag all ICT service provider dependencies and tier them.	Validated QASI satisfying Art 7 cryptographic controls requirements. Certificate inventory satisfying Art 8. Prioritized supplier engagement list. Coverage figures for systems and flows.

Weeks	Phase	Priority actions	NIS2 artifact produced
7 to 9	Analyze	Map data classification to horizon and profile fields (Implementing Reg Art 7.2). Raise exposure flags for long-retention data. Issue Annex C requests to Priority 1 suppliers with the 60-day deadline.	Data classification-to-crypto linkage documented per Art 7. Supplier request records with dates and deadlines. Exposure flags active.
10	Score	Produce the first Q-Risk Score, labelled self-assessment (QCI-1.2-03), with gate results. Be honest. A score of 35 with evidence is a defensible NIS2 posture. A score of 65 without evidence is a supervisory liability.	Q-Risk Score snapshot with evidence links, assessment type and conformance status. Scoreable against NIS2 pillar mapping.
11 to 12	Report	Deliver the first management body briefing insert with NIS2 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.	Governing-body insert satisfying NIS2 Art 20 management body reporting obligation. Exception register. Migration roadmap.

8. NIS2 supervision preparation checklist

The items below reflect what a NIS2 competent authority supervision team, applying the Commission Implementing Regulation 2024/2690, is likely to request during an on-site or documentary inspection of cryptographic controls. Produce these artifacts before supervision, not in response to a request.

Governance artifacts

- Written quantum risk policy statement referencing NIS2 Art 21 cryptographic controls obligations
- Named Quantum Risk Owner with documented mandate, including NIS2 cybersecurity risk management function alignment
- Management body meeting 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 essential functions and their critical flows, each with a named system owner and a validation date within 90 days
- Certificate inventory satisfying Implementing Reg Art 8 — all certificates for essential function systems, with owner, expiry date, renewal status and migration path
- ICT service provider list with NIS2 supply chain security assessment status for each Priority 1 vendor

Cryptographic controls artifacts

- Documented encryption and cryptographic controls policy per Implementing Reg Art 7, incorporating the approved cryptographic profile of QCI-4.5-01
- Data classification outputs linked to cryptographic control selections for each QASI record
- Documented compensating controls for any system where cryptographic technology cannot be updated, with rationale, held in the exception register
- Test and acceptance records under QCI-4.7 for at least one essential function pathway, including the representative end-to-end test gate G80 requires

Vendor artifacts

- Dated request records for all Priority 1 ICT service providers, 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

Reporting artifacts

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

9. Summary and engagement

NIS2 has converted quantum readiness from a risk management best practice into a supervised compliance obligation for essential and important entities across eighteen EU sectors. The evidence QCI-QS1 requires — named ownership, validated QASI coverage, supplier attestations, tested crypto agility, quarterly management body reporting — is precisely the evidence a NIS2 competent authority supervision will request.

Entities that complete a QCI-QS1 assessment using this supplement will have a defensible, evidence-backed quantum readiness posture that satisfies NIS2's Article 21 cryptographic controls requirements and is aligned to the EU PQC Roadmap milestones through 2030.

Engagement

This supplement provides the framework for NIS2 entities to understand and map their quantum readiness obligations. QCI engagements for NIS2 entities provide assessment support, sector-specific benchmark data, supply chain vendor engagement guidance, and supervision 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); supply chain mapping pointed to QCI-7.1, 7.2, 7.3-01 and 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; COM(2026) 13 noted as proposed; flows and OT boundary guidance added; 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).