

QUANTUM CORE INSTITUTE

QCI-QS1-S4

Critical Infrastructure Supplement

Quantum Readiness Guidance for Water Utilities and Regional Energy Operators

Document ID	QCI-QS1-S4
Version	1.2
Status	Public — Free to download and cite
Publisher	Quantum Core Institute (QCI)
Normative ref	QCI-QS1 Version 2.3 (September 23, 2026). Clause references are QCI requirement identifiers.
Applies to	Water and wastewater utilities, rural electric cooperatives, municipal utilities, and regional transmission organizations operating critical infrastructure subject to CISA, NERC CIP, EPA, or TSA security requirements
Effective date	September 23, 2026
Review cycle	Annual, or upon material CISA, NERC CIP, EPA, or TSA regulatory developments, or a new edition of QCI-QS1

This supplement extends QCI-QS1 for the specific operational technology, regulatory, and consequence context of water utilities and regional energy operators. It maps quantum readiness requirements to NERC CIP standards, CISA cross-sector guidance, EPA cybersecurity requirements, and TSA security directives. It addresses the operational technology dependency problem that makes this sector's quantum exposure fundamentally different from any other sector QCI covers.

Foreword

Every other sector in the QCI supplement series faces a quantum readiness problem measured in data breaches, regulatory findings, and financial exposure. Critical infrastructure faces a quantum readiness problem measured in public safety consequences.

A cryptographic failure in water treatment authentication does not produce a regulatory finding. It produces an operational condition where an adversary controls chemical dosing in a public water supply. A compromised grid authentication system does not trigger a compliance event. It creates the conditions for a coordinated power outage affecting hospitals, emergency services, and the populations they serve. The consequence category is different and that difference must shape how operators approach quantum readiness — with urgency calibrated not to audit schedules but to public welfare.

The operational technology systems controlling water treatment, power generation, and grid management were designed for reliability and availability, not cryptographic agility. Most SCADA and industrial control systems in service today were not designed to be updated at the pace that cryptographic threats demand. Vendors are slow, change management is conservative, and the tolerance for system downtime during upgrades is near zero. These constraints are real and this supplement respects them. But they do not eliminate the obligation to plan — they make planning more urgent, not less.

The operators who begin now — inventorying their OT cryptographic dependencies, engaging their SCADA vendors, building their regulatory documentation, and establishing governance — will have the time and the options that operators who wait will not. When NERC CIP is updated to include explicit PQC requirements, when CISA issues binding operational directives for water systems, when EPA security rules for water utilities gain enforcement teeth — the operators with documented programs will be the ones in compliance. The others will be the case studies.

What changed in version 1.2

Version 1.2 aligns this supplement to QCI-QS1 version 2.3. The largest change is structural: the separate IT and OT scores this supplement has always recommended are now produced as two declared assessment boundaries under QCI-1.1-01, each with its own conformance record, coverage figures and score, because the standard no longer permits two Core scores for one boundary (section 7.1). Three scoring changes follow: the Defensible readiness band begins at 81; gate G70 is no longer satisfied by a documented exception, so an OT boundary cannot score above 70 until every SCADA and ICS vendor has attested (section 5.4); and gate G60 is fixed at 95 percent validated coverage of both critical systems and critical flows, which for OT means the control communications themselves. Section 2.5 turns the regulatory mapping into the obligations register QCI-2.2-01 requires, and section 4 gains the firmware-signing and key-lifecycle rules of QCI-4.6.

1. Scope and applicability

This supplement applies to:

- Community water systems and wastewater utilities subject to America's Water Infrastructure Act (AWIA) cybersecurity requirements and EPA security assessments
- Rural electric cooperatives, municipal electric utilities, and regional transmission organizations subject to NERC CIP reliability standards
- Natural gas distribution companies and pipeline operators subject to TSA security directives

- Combined utility operators providing water, gas, and electric service under integrated OT infrastructure
- SCADA and industrial control system vendors whose products materially affect the cryptographic posture of critical infrastructure operators in scope

IT versus OT: the fundamental distinction

This supplement addresses two distinct environments that most critical infrastructure operators manage separately: information technology (IT) systems handling business operations, billing, customer data, and corporate communications; and operational technology (OT) systems including SCADA, distributed control systems (DCS), programmable logic controllers (PLCs), and remote terminal units (RTUs) that directly control physical infrastructure. Quantum readiness applies to both environments but the constraints, risks, and remediation approaches differ significantly. Under QCI-QS1 v2.3 the two are declared as separate assessment boundaries (QCI-1.1-01), and this supplement addresses both, with explicit callouts where the guidance differs.

Note on the AI-cryptographic provisions

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

2. Regulatory context

2.1 Energy sector: NERC CIP alignment

The NERC Critical Infrastructure Protection (CIP) standards are the primary regulatory framework for bulk electric system cybersecurity in North America. The following CIP standards are most directly relevant to quantum readiness:

NERC CIP standard	Subject	Quantum readiness relevance
CIP-005	Electronic Security Perimeters	Encrypted communications protecting ESP boundaries rely on key establishment vulnerable to quantum attack. PQC migration of perimeter encryption is a direct CIP-005 concern.
CIP-006	Physical Security of BES Cyber Systems	Authentication systems protecting physical access to critical cyber systems use public-key cryptography. Quantum compromise of authentication undermines physical security controls.
CIP-007	Systems Security Management	Patch management and security configuration requirements. Cryptographic algorithm updates fall within the scope of security configuration management under CIP-007.

NERC CIP standard	Subject	Quantum readiness relevance
CIP-010	Configuration Change Management and Vulnerability Management	Vulnerability assessments must identify emerging threats to BES cyber systems. Quantum computing represents an emerging threat to cryptographic controls that CIP-010 assessments must address.
CIP-013	Supply Chain Risk Management	Vendors of hardware, software, and services for BES cyber systems must be assessed for security risk. Quantum readiness attestation from OT vendors is a direct extension of CIP-013 supply chain risk requirements, and the Annex C request is the instrument.

NERC has not yet issued explicit PQC requirements within the CIP standards. However, the trajectory is clear: NERC's long-term reliability standards development process has identified post-quantum cryptography as an area requiring standards action, and FERC has directed NERC to address emerging cybersecurity threats including quantum computing in future CIP revisions. Operators that have documented quantum readiness programs aligned with existing CIP standards will be better positioned for the transition when explicit PQC requirements arrive.

2.2 Water sector: EPA and AWIA requirements

America's Water Infrastructure Act of 2018 (AWIA) requires community water systems serving more than 3,300 people to conduct risk and resilience assessments and develop emergency response plans. CISA and EPA have both identified cybersecurity — including cryptographic controls — as a required element of these assessments.

- Risk and resilience assessments under AWIA Section 2013 must address cybersecurity vulnerabilities of process control systems. Quantum computing threats to SCADA authentication and communications encryption are cybersecurity vulnerabilities within the scope of this requirement.
- EPA's Water Sector Cybersecurity Brief (2023) explicitly references post-quantum cryptography as an emerging risk that water utilities should monitor and begin planning for. This guidance is advisory but provides the regulatory basis for including quantum readiness in AWIA assessment updates.
- The Water Information Sharing and Analysis Center (WaterISAC) has issued alerts on quantum computing threats to water sector OT systems. Membership in WaterISAC and engagement with their quantum readiness guidance satisfies the information sharing component of AWIA resilience requirements.

2.3 Pipeline and gas: TSA security directives

TSA's cybersecurity security directives for pipeline operators (SD Pipeline-2021-01 and subsequent revisions) require operators to implement specific cybersecurity measures for critical OT systems, including authentication controls and network segmentation. The directives do not yet address post-quantum cryptography explicitly, but the authentication and network security requirements they mandate rely on cryptographic controls that quantum computing will eventually compromise.

Pipeline operators should treat TSA security directive compliance as the floor, not the ceiling, for quantum readiness. The cryptographic controls required by TSA directives need PQC migration planning that anticipates future directive updates.

2.4 Federal policy and CISA cross-sector guidance

CISA's post-quantum cryptography guidance applies to all critical infrastructure sectors and provides the most comprehensive federal framework for OT quantum readiness planning. Since June 2026 the federal benchmark also carries dates: Executive Order 14412 (June 22, 2026) directs federal key-establishment transition by December 31, 2030 and authentication transition by December 31, 2031, and OMB M-26-15 (June 24, 2026) sets the federal migration method. Neither binds a non-federal operator directly, but federally owned or funded utilities, and operators that exchange data with federal agencies, inherit them through contract and interoperation; QCI-QS1 Annex E records them as S12 and S13. Key CISA guidance elements:

- CISA's Cybersecurity Advisory on Post-Quantum Cryptography identifies operational technology systems as among the highest-priority migration targets due to their long deployment lifetimes and the difficulty of applying patches and updates.
- CISA's Infrastructure Security Division has published sector-specific guidance for water and energy that references PQC migration as a required element of long-term resilience planning.
- Operators participating in CISA's Cyber Hygiene program can request assessments that include evaluation of cryptographic controls — a direct entry point for quantum readiness assessment.

2.5 Obligations register entries for this sector

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 mappings above are the seed. The entries below are the minimum; each operator adds its state public utility commission requirements and any federal funding conditions, and verifies every entry against the source. A general migration target never overrides an earlier applicable deadline.

Obligation	Issuer and document	Status	Affected systems and suppliers	Action and deadline
NERC CIP-005, 006, 007, 010, 013	NERC; current enforceable versions	Regulation, mandatory for BES cyber systems	ESP perimeters, physical access, patching, change management, OT vendors	Add the quantum threat to the CIP-010 assessment; Annex C attestation in the CIP-013 plan
AWIA Section 2013 risk and resilience assessment; emergency response plan	EPA; AWIA 2018	Law, for systems serving over 3,300	SCADA authentication and communications; treatment control	Quantum threat section at the next RRA cycle; cryptographic incident scenario in the ERP
TSA pipeline security directives	TSA; SD Pipeline-2021-01 series, current revision	Directive, mandatory for covered operators	Pipeline OT authentication and segmentation	Treat as the floor; record the directive revision and its cryptographic requirements

Obligation	Issuer and document	Status	Affected systems and suppliers	Action and deadline
Federal PQC transition	EO 14412; OMB M-26-15	Federal policy; applies by ownership, funding or interoperation	Federally funded or federally connected systems	Confirm applicability; where applicable, key establishment by December 31, 2030, authentication by December 31, 2031
Sector information sharing	E-ISAC, WaterISAC membership and alerts	Voluntary; satisfies AWIA information-sharing element	All OT	Maintain membership; use sector channels for coordinated vendor engagement

3. The operational technology cryptographic problem

3.1 Why OT crypto exposure is different

Information technology systems can typically be updated, patched, and reconfigured on timelines measured in weeks to months. Operational technology systems controlling physical infrastructure operate under constraints that make the same updates take years — when they are possible at all. Four constraints define the OT crypto problem:

OT constraint	How it affects crypto migration	QCI-QS1 implication
Availability requirement	OT systems cannot tolerate the downtime that cryptographic upgrades typically require. A water treatment SCADA system serving 500,000 people cannot be taken offline for a crypto migration window.	Crypto agility in OT requires vendor-delivered updates that can be applied without system downtime. Most current OT platforms cannot meet this requirement. Score crypto agility as None for most OT systems. QCI-4.7-01 still requires a representative test before acceptance; for OT that means a test bench or redundant train, with the relationship to production documented.
Long deployment lifetime	OT systems are designed to operate for 15 to 30 years. A SCADA system deployed in 2010 may still be in production in 2035 — well within the quantum threat timeline. Its cryptographic configuration was established at deployment and has rarely changed.	Exposure compounds over remaining service life. Apply the compounding lens from the government supplement to every OT system with more than five years remaining. QCI-4.2-02 requires long-lead hardware and trust-anchor decisions to start when the lead-time analysis requires, not after IT work is finished.
Vendor control of crypto stack	Most OT crypto is implemented in firmware and embedded software that operators cannot modify. Algorithm changes require vendor firmware updates, which require vendor development, testing, certification, and deployment support.	OT vendor engagement is not optional. An operator who has not engaged their SCADA and ICS vendors on PQC roadmaps is carrying unmanaged third-party quantum risk regardless of their internal security program maturity, and under gate G70 the OT boundary is capped at 70 until they attest.

OT constraint	How it affects crypto migration	QCI-QS1 implication
Safety and reliability certification	OT systems in critical infrastructure often carry safety or reliability certifications that require re-certification after any significant change, including firmware updates. This adds 6 to 24 months to any migration timeline.	Migration timelines for certified OT systems must account for re-certification. This is not a delay to plan around — it is a constraint to plan with. Begin vendor engagement now to understand certification implications before they become critical path items. A certification is a supplier assertion under QCI-4.8-03, not system acceptance.

3.2 The IT-OT convergence risk amplifier

The trend toward IT-OT convergence — connecting operational technology networks to enterprise IT networks and increasingly to cloud services — creates a quantum risk amplifier unique to this sector. As OT systems gain network connectivity, the cryptographic boundary between the physical infrastructure and the internet expands. Each new connection is a potential harvest target.

Operators who have implemented IT-OT convergence for remote monitoring, predictive maintenance, or operational efficiency should treat every IT-OT interface as a high-priority QASI entry and, under QCI-5.2-01, as a critical flow with protection and authentication recorded at each hop. The cryptographic controls protecting these interfaces — the TLS sessions, the VPN tunnels, the API authentication — are IT crypto operating in an OT risk context. They are both more likely to be updated than embedded OT firmware and more immediately exposed to network-based harvesting.

The consequence distinction

Every other QCI supplement addresses quantum risk as a data confidentiality and regulatory compliance problem. This supplement addresses quantum risk as a public safety problem. An adversary who compromises the authentication controlling a water treatment SCADA system does not need to decrypt historical data. They need only forge authentication credentials to issue control commands. Quantum computing enables both the long-term data compromise and the near-term authentication forgery — and for operational technology systems, both attack vectors lead to physical consequences. In the standard's terms the OT exposure is a verification horizon, not a confidentiality horizon: authentication must remain unforgeable for the operational life of the system. This consequence distinction must be communicated to every executive sponsor and governing body in this sector.

4. QASI record guidance for critical infrastructure operators

The standard QASI record groups (QCI-5.2-01) apply to both IT and OT boundaries. The following guidance addresses OT-specific interpretation of key fields. A field may hold a known value, an explicit unknown with an investigation action, owner and due date, or a justified not-applicable value (QCI-5.1-02); for OT firmware whose cryptographic contents the vendor has not disclosed, “unknown — vendor asked [date]” is the honest entry, and the record stays outside validated coverage until it is resolved.

QASI field	Critical infrastructure guidance
System ID and boundary	Create separate QASI records for IT systems and OT systems, in their separate assessment boundaries. Do not aggregate. An enterprise IT system and a SCADA control system have fundamentally different risk profiles, migration constraints, and vendor dependencies even when operated by the same organization.
Business criticality	All SCADA, DCS, PLC, and RTU systems: always High. All IT-OT interface systems: High. Enterprise IT systems supporting operations (ERP, historian, asset management): High to Medium depending on OT integration depth. Corporate IT with no OT connectivity: Medium or Low. Criticality follows QCI-1.1-02, which counts safety consequences explicitly.
Data classification	OT systems: classify as Operational Critical regardless of whether they process traditional data. The cryptographic controls protecting OT command and authentication are protecting physical infrastructure, not data. This distinction matters for how risk is communicated to leadership.
Confidentiality and verification horizons	For IT systems: apply standard retention analysis to the confidentiality horizon. For OT systems: the verification horizon is the one that matters — how long authentication credentials and communication integrity must remain unforgeable. Answer: for the remaining operational life of the system, which may be 15 to 25 years. Record it as a date.
Critical data flows	New in v2.3: flows are a separate coverage denominator (QCI-5.1-03), and in OT the flows are the point. Inventory at minimum: SCADA master to RTU and PLC communications, DCS to safety system links, historian and IT-OT interfaces, remote access paths, and firmware update channels, with protection and authentication at each hop.
Crypto functions used	Document OT crypto with the same specificity as IT crypto. SCADA communications protocols (DNP3 Secure Authentication, IEC 62351, Modbus with TLS) use specific cryptographic implementations. Document the protocol version and its cryptographic component, and the firmware signing scheme for update chains. 'SCADA communications' is not sufficient.
Key and trust lifecycle	QCI-4.6-01 and 4.6-02 apply to OT with particular force: device certificates that cannot be rotated without a site visit, firmware signing keys held by the vendor, and secure-boot roots baked at manufacture. Record who holds each key, how it is rotated, and what the recovery path is. Where CNSA 2.0 applies to firmware signing, stateful hash-based signatures (LMS, XMSS) carry the signing-state safeguards of QCI-4.6-01.
Crypto agility status	Default to None for all OT systems unless the vendor has explicitly demonstrated the ability to change cryptographic algorithms via a tested, non-disruptive firmware update. Partial is acceptable only if the operator has documented at least one algorithm change completed without operational disruption.
Exposure flags	For OT authentication systems: raise the long-verification-horizon flag (QCI-5.3-01) by default. An adversary who harvests OT authentication traffic today may be able to forge credentials in the future. The consequence of forged OT authentication is not a data breach — it is operational control compromise. Record the operational consequence explicitly. Treatment status is recorded separately (QCI-5.3-02).

QASI field	Critical infrastructure guidance
Compensating controls	Network segmentation is the most effective OT compensating control. An OT system on a properly segmented network with no external connectivity reduces harvest exposure because traffic cannot be captured remotely. Record segmentation as treatment only if it has been verified through network architecture review, not assumed — which is what QCI-5.3-02 requires before any mitigation counts.

5. OT vendor landscape and engagement

5.1 The SCADA vendor PQC problem

The OT vendor landscape presents the most concentrated and least responsive vendor engagement challenge of any sector QCI covers. A small number of vendors — Siemens, Schneider Electric, Honeywell, ABB, Emerson, and a handful of sector-specific ICS vendors — supply the majority of critical infrastructure OT systems globally. These vendors operate on product lifecycles measured in decades, their development priorities are driven by reliability and safety certifications rather than security roadmaps, and their customer base has historically not demanded cryptographic agility.

This is changing. CISA, NERC, and international equivalents are beginning to require OT vendors to address security as a first-class product requirement. The operators who begin demanding PQC roadmaps now — formally, in writing, through procurement and contract mechanisms — are the ones who accelerate that change and protect their own systems in the process.

5.2 Vendor-specific engagement considerations

The status column below records what each vendor had published as of September 23, 2026 and changes with every release. Confirm the current position with the vendor and record it, with the date, in the QASI supplier record (QCI-5.2-01). The engagement question that now matters most is the last one: whether the vendor will sign the Annex C attestation for the platform release the operator runs, because gate G70 depends on it.

Vendor	Primary OT platforms	PQC status (reviewed September 23, 2026)	Operator engagement approach
Siemens	SIMATIC, WinCC, SINEC, SCALANCE	Corporate awareness posts (January 2023; December 8, 2025) and a May 2025 Cre8Ventures partnership with Xiphra on PQC hardware IP for automotive and industrial IoT. No published PQC roadmap or release dates for SIMATIC, WinCC, SINEC or SCALANCE; ProductCERT advisories carry no PQC content.	Engage through the Siemens Energy or Siemens Digital Industries account team. Reference the CIP-013 supply chain obligation. Request a written roadmap with NIST FIPS alignment dates by release, and the attestation.
Schneider Electric	EcoStruxure, Modicon, ClearSCADA, Triconex	No public PQC statement or product roadmap located for EcoStruxure, Modicon, ClearSCADA or Triconex. Corporate cybersecurity pages do not address quantum.	Route through the EcoStruxure security team. Reference IEC 62443 cybersecurity requirements and CISA guidance. Request the approved key-establishment profile and timeline for communication protocols, and the attestation.

Vendor	Primary OT platforms	PQC status (reviewed September 23, 2026)	Operator engagement approach
Honeywell	Experion PKS, ControlEdge, Uniformance	Quantum Origin quantum-generated keys integrated into smart utility meters (September 2023) and a Colt, Honeywell and Nokia space-based quantum-safe trial (June 2025). Neither is a PQC roadmap for Experion PKS, ControlEdge or Uniformance, and the June 2026 Experion R530 feature pack, R600 and OT Cybersecurity Suite announcements do not address PQC.	Engage the Honeywell Forge security team directly. Reference TSA directive requirements for pipeline clients. Request a scoped CBOM or SBOM with cryptographic library versions (QCI-5.4-03).
ABB	Ability System 800xA, AC500, Symphony Plus	Innovation article "Preparing for the quantum age" (June 29, 2026) states ABB's hybrid-construction position and flags secure boot, software verification and secure manufacturing on embedded devices, with a fuller ABB Review article promised. No product roadmap for 800xA, AC500 or Symphony Plus. The 2019 FOX615 quantum-safe encryption card belongs to the grid communications business that is now Hitachi Energy.	Route through ABB's cybersecurity practice. Reference IEC 62351 and NERC CIP-013 obligations. Request the attestation on the cryptographic library inventory and the dates behind the hybrid position.
Emerson	DeltaV, Ovation, PACSystems	DeltaV zero-trust white paper (May 2025) commits to digitally signed Area Control Network communications, CA-signed device firmware and an OT-dedicated PKI, all specified on classical algorithms. No PQC statement located for DeltaV, Ovation or PACSystems.	Engage through Emerson's cybersecurity services team. Reference NRC requirements for nuclear clients if applicable. Request a PQC readiness statement for current platform versions, on the attestation form, covering the firmware signing scheme.
OSIsoft / AVEVA (PI System)	PI Data Archive, PI Asset Framework	October 2024 partnership with Oxford Quantum Circuits concerns quantum computing applications, not cryptography. No PQC statement located for PI System.	Engage the AVEVA security team. PI System is an IT-OT interface — prioritize this engagement because PI connections create an external harvest surface for OT data and are a critical flow in both boundaries.

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

- Siemens Blog, Post-Quantum Cryptography: Securing the Future Before It Arrives, December 8, 2025: blog.siemens.com; Siemens Cre8Ventures, partnership with Xiphora, May 12, 2025: blogs.sw.siemens.com/cre8ventures
- Honeywell, quantum-hardened encryption keys in smart utility meters, press release, September 2023: pmt.honeywell.com; Colt, Honeywell and Nokia space-based quantum-safe cryptography trial, June 2025: aerospace.honeywell.com
- ABB, Preparing for the quantum age, June 29, 2026: abb.com/global/en/company/innovation/news/quantum-security
- Emerson, Defining the Industrial Zero Trust Vision for DeltaV, white paper, May 2025: emerson.com/documents/automation/
- AVEVA, strategic partnerships announced at AVEVA World, October 2024: aveva.com/en/about/news/press-releases/2024/

5.3 Industry association leverage

Critical infrastructure operators have access to sector-specific information sharing organizations that provide collective leverage with OT vendors that individual operators cannot achieve alone. Use these channels actively:

- E-ISAC (Electricity Information Sharing and Analysis Center): NERC-affiliated organization providing threat intelligence and coordinating sector-wide security responses. E-ISAC is actively engaged on quantum computing threats. Membership gives operators access to sector-coordinated vendor engagement.
- WaterISAC: Water sector equivalent providing threat intelligence and security guidance. WaterISAC has issued quantum computing threat alerts and can coordinate sector-wide vendor engagement for common water utility OT platforms.
- ICS-CERT (now CISA ICS): Provides vulnerability coordination for ICS vendors. An operator who reports inadequate vendor PQC response to CISA ICS creates a coordination pathway that individual vendor relationships cannot provide.
- NERC CIP compliance user groups: Most major OT vendors have NERC CIP compliance user groups where operators share implementation experience. These groups are effective forums for coordinating PQC requirement pressure across multiple operators using the same platform, and for agreeing a common attestation request so that a vendor signs once for many.

5.4 What gate G70 means for OT operators

Under QCI-QS1 v2.3, an assessment boundary cannot score above 70 until every critical supplier in it has provided a current, adequate response and an officer-signed attestation (gate G70, QCI-6.3-01). An approved exception, however well managed, does not lift the cap. For an OT boundary whose SCADA, DCS or safety-system vendor has not attested — which as of the September 23, 2026 review in section 5.2 is all six vendors listed there — the OT score stays at 70 or below regardless of the operator's own work, and the vendor's name recurs in the governing-body insert every quarter until it does.

That is the rule working as designed, and in this sector it is the standard saying out loud what section 3.1 has always said: the operator cannot fix the vendor's firmware. The pressure belongs with the vendor, and the operator's levers are the ones in this chapter: the Annex C request with a 60-day deadline (QCI-7.2-04), CIP-013 and procurement language that makes the attestation a contract deliverable (QCI-7.1-02), and sector-coordinated requests through the ISACs. An operator held at 70 by an unattested vendor, with the register showing the request, the deadline, the escalation and the compensating segmentation verified, has a defensible position with NERC, EPA and its board. An operator that reports an OT score of 74 with an unattested SCADA vendor has a finding.

6. Governance model for critical infrastructure operators

6.1 The IT-OT governance bridge

Most critical infrastructure operators manage IT and OT through separate governance structures. The CISO owns IT security. The VP of Operations or Chief Engineer owns OT reliability. Quantum readiness requires a governance bridge between these two structures because OT crypto exposure is a security risk and an operational risk simultaneously. QCI-4.1-01 requires documented responsibilities across engineering, system owners, procurement,

incident response, legal and assurance, and a cross-functional steering function; the bridge is that function.

QCI-QS1 required role	Critical infrastructure mapping	Why both IT and OT involvement is required
Executive Sponsor	CISO or VP of Operations — whoever has authority over both IT and OT security. In some utilities this is the CEO directly.	Quantum risk spans the IT-OT boundary. A sponsor who owns only one side cannot authorize action on the other, and the sponsor approves both assessment boundaries (QCI-1.1-01).
Quantum Risk Owner	Security architect or OT security lead with access to both IT and OT system documentation.	Both QASIs must be built. A Risk Owner without OT access cannot complete the OT inventory, and control systems engineers are the technical reviewers OT records need (QCI-5.1-02).
Steering function (risk committee)	Joint IT-OT security committee. If one does not exist, create it for this program — quantum risk is the right forcing function.	OT migration decisions require operations sign-off. IT migration decisions require security sign-off. Both are needed at the same table.
Governing body	Utility board, co-op board of directors, or municipal council as applicable.	Quantum risk at a water or energy utility is a board-level matter because the consequence of failure is public safety, not just financial or reputational exposure. Any accepted risk is approved explicitly (QCI-8.2-01).
Vendor risk	Procurement team with OT procurement experience. SCADA vendor contracts require different expertise than IT vendor contracts.	OT vendor contracts often have different termination rights, SLA structures, and change management provisions than IT contracts. Procurement needs OT context to negotiate the attestation, notification and evidence-access terms QCI-7.1-02 expects.

7. Q-Risk Score guidance for critical infrastructure operators

7.1 Two assessment boundaries: IT and OT

Earlier editions of this supplement recommended producing two Q-Risk Scores, one for IT and one for OT. QCI-QS1 v2.3 keeps the practice and changes its form. A Core score belongs to a declared assessment boundary (QCI-1.1-01), and organization-specific splits of one boundary may be reported only as supplemental metrics (QCI-6.3-02). The operator therefore declares two boundaries — the IT estate and the OT estate, with the IT-OT interfaces assigned to one and referenced from the other — and each boundary carries its own conformance record, its own coverage figures for systems and flows, its own gate results and its own score. The two scores will almost always differ significantly: IT environments typically score higher due to greater patch frequency and crypto agility, while OT environments score lower due to vendor dependency and long deployment lifetimes.

Present both to leadership with the explanation that the OT score reflects the operational technology environment that directly controls physical infrastructure. The OT score is the one with public safety implications. Each is reported with its assessment type (QCI-1.2-03) and its

conformance status beside it (QCI-1.2-04). Do not average them, and do not present a blended figure as the organization's score.

7.2 Realistic band targets

QCI-QS1 defines score bands from Exposed (0 to 19) through Defensible readiness (81 to 100). A score of exactly 80 is Advancing, and no score above 80 is possible unless gates G60, G70 and G80 have all passed (QCI-6.3-01, QCI-6.5-01). The targets below are planning guidance, not Core-profile thresholds (QCI-6.3-02). No OT target approaches 70, and none could while any SCADA or ICS vendor is unattested.

Operator profile	IT score start	OT score start	12-month target (IT / OT)	Primary constraint
Large water utility, 100K-plus connections	18 to 30	6 to 14	40 to 55 / 18 to 28	OT vendor roadmap absence; availability constraint limits migration testing
Small to mid water utility, under 100K	10 to 20	4 to 10	28 to 42 / 14 to 22	Limited dedicated OT security staff; SCADA vendor responsiveness
Rural electric cooperative	12 to 22	5 to 12	30 to 44 / 16 to 24	SCADA vendor concentration; limited security resources
Municipal electric utility	16 to 28	8 to 16	36 to 50 / 20 to 32	IT-OT governance bridge; NERC CIP compliance overhead
Pipeline or gas distribution operator	14 to 24	6 to 14	32 to 48 / 18 to 28	TSA directive compliance priority; OT change management constraints

8. Critical infrastructure 90-day quick start

This sequence adapts the Practitioner Handbook's establishment sequence and QCI-QS1 Clause 9.1 for an operator with both estates. It is a planning aid, not a conformance grace period.

Timeframe	Phase	What to accomplish	Output
Week 1	Assign, bound and bridge	Name the executive sponsor with authority over both IT and OT. Declare the two assessment boundaries and assign the IT-OT interfaces (QCI-1.1-01). Establish the IT-OT governance bridge by adding quantum risk to the agenda of any existing joint IT-OT committee, or scheduling the first joint meeting. Seed the obligations register from section 2.5.	Named sponsor. Two approved boundaries. Joint IT-OT committee quantum risk agenda item established. Obligations register started.
Week 2	OT system and flow identification	Create a list of all OT systems and control communications in scope before beginning the QASI. This is harder than IT asset inventory because OT asset registers are often incomplete or siloed in operations. Engage the control systems engineer team — they know what exists.	OT system and flow list validated by control systems engineering. IT-OT interface systems explicitly identified.

Timeframe	Phase	What to accomplish	Output
Weeks 3 to 4	Vendor requests	Issue Annex C requests to the top three OT vendors and top two IT vendors. For OT vendors, route through the account team and explicitly reference CIP-013 supply chain obligations or AWIA cybersecurity requirements as applicable. Coordinate through the sector ISAC where other operators share the platform.	Five requests issued with a 60-day response deadline (QCI-7.2-04). OT vendor requests cite the regulatory obligation.
Weeks 5 to 7	QASI build — IT boundary	Build linked QASI records for the IT boundary first, systems and flows. IT QASI is faster to complete because crypto fields are more accessible. This builds team familiarity with the inventory process before tackling the harder OT inventory.	IT QASI complete for critical systems and flows; coverage computed per QCI-5.1-03. IT score producible.
Weeks 8 to 9	QASI build — OT boundary	Build the OT QASI with the control systems engineering team as technical reviewers. Apply the OT-specific field guidance from section 4. Record unknowns explicitly. Flag all IT-OT interface flows as separate high-priority records.	OT QASI complete for critical systems and control flows. IT-OT interfaces explicitly flagged. Vendor dependency and key custody documented per system.
Week 10	Score — both boundaries	Produce separate IT and OT Q-Risk Scores using the Annex B worksheet, each with its own gate results and assessment type. Note that OT scores will almost always be lower. Frame the OT gap as a vendor-dependency finding, not an operations team failure.	IT Q-Risk Score and OT Q-Risk Score, each self-assessed and labelled. Gap analysis between IT and OT postures documented.
Weeks 11 to 12	Brief and plan	Deliver the governing-body insert using the dual-boundary format (QCI-8.1-01). Frame the OT gap in consequence terms. Open the exception register under QCI-4.3-02 for OT vendors without roadmaps. Issue E-ISAC or WaterISAC notification if applicable. Start the roadmap with milestone types per QCI-4.2-02, including long-lead device and trust-anchor decisions.	Governing-body briefing delivered. Exception register open for OT vendors without roadmaps. Sector ISAC notified if applicable. Roadmap draft begun.

9. Regulatory compliance integration

9.1 NERC CIP compliance integration for energy operators

Energy operators can integrate QCI-QS1 quantum readiness requirements with existing NERC CIP compliance programs to reduce duplication and align evidence production; QCI-4.2-01 permits the standard's records to live in existing management systems. The following integration points are most efficient:

- CIP-010 vulnerability assessments: Add a quantum computing threat section to the annual vulnerability assessment. Document the threat, current cryptographic controls, vendor PQC status, and planned response. This satisfies both QCI-QS1's exposure analysis requirements and CIP-010's vulnerability assessment obligation with a single artifact.
- CIP-013 supply chain risk management plan: Add quantum readiness attestation as a required element of the supply chain risk management plan for all OT vendors. The Annex C

request and attestation satisfy the CIP-013 vendor assessment requirement for cryptographic risk specifically, and they are what gate G70 counts.

- CIP-007 security patch management: PQC firmware updates are security patches within the scope of CIP-007. Establishing the process for evaluating and applying PQC firmware updates now — before they are available — ensures the CIP-007 compliance process is ready when vendors deliver updates, and that the QCI-4.7 test and acceptance steps are built into it.

9.2 AWIA compliance integration for water operators

Water utilities subject to AWIA can integrate QCI-QS1 with their risk and resilience assessment (RRA) and emergency response plan (ERP) update cycles:

- RRA update: The next AWIA RRA update cycle is the natural point to add a quantum computing threat assessment section. Include SCADA authentication and communications encryption in the cybersecurity vulnerability section with quantum threat documentation and the verification horizons from section 4.
- ERP integration: The emergency response plan should address the cryptographic incident scenarios of QCI-4.4-01, including authentication compromise, trust-anchor failure and unauthorized downgrade. A scenario where OT authentication credentials are forged requires a response plan distinct from conventional intrusion response, and QCI-4.4-02 requires it to be exercised at least annually.
- EPA Cybersecurity Guidance alignment: EPA's sector cybersecurity guidance references PQC as an emerging area. Documenting QCI-QS1 alignment in the RRA demonstrates proactive engagement with EPA priorities.

10. Summary and engagement

Critical infrastructure operators carry a quantum readiness obligation that is different in kind from every other sector. The consequence of failure is not a regulatory finding or a data breach. It is compromised control of systems that deliver water to communities and power to hospitals. That consequence demands a response calibrated to its severity — which means planning now, before the technology timeline compresses further.

The operators who build governance, complete inventory, engage vendors, and establish regulatory documentation now are the ones who will have options when PQC requirements become mandatory. They will be able to demonstrate an active, documented program. They will have the vendor relationships to accelerate migration when roadmaps mature. They will not be starting from zero when NERC CIP, EPA, or CISA issue explicit requirements. And they will be able to say, with the exception register as evidence, exactly which vendor is holding the OT score at 70.

QCI engagement support for critical infrastructure operators

QCI works with water utilities, electric cooperatives, municipal utilities, and pipeline operators to deliver dual-boundary IT and OT assessments against QCI-QS1, facilitate OT vendor engagement through sector ISAC channels, integrate quantum readiness into NERC CIP and AWIA compliance programs, and prepare board-level consequence briefings. Independent assessment under QCI-1.2-03 is available separately. Engagements are structured to respect OT operational constraints — QCI does not require access to live control systems to conduct a quantum readiness assessment. Contact QCI to discuss how an engagement is scoped for your operational profile.

Revision history

Version	Date	Changes
1.2	September 23, 2026	Aligned to QCI-QS1 v2.3; vendor status table refreshed against supplier publications as of September 23, 2026, with sources listed: references by requirement identifier; IT and OT scores recast as two declared assessment boundaries (7.1); band targets restated for the 81-point Defensible readiness threshold; gate G70 no longer satisfied by exceptions (new section 5.4); G60 fixed at 95 percent for systems and flows, with control-flow guidance; obligations register section 2.5 added; federal policy context updated for EO 14412 and OMB M-26-15; verification horizon replaces data longevity for OT; key and trust lifecycle field added per QCI-4.6; vendor table reframed around the attestation; incident scenarios and annual exercises per QCI-4.4; governing-body terminology.
1.1	June 10, 2026	Aligned to QCI-QS1 v2.2; AI-cryptographic provisions note added.