

QUANTUM CORE INSTITUTE

QCI-QS1-S5

Insurance Carrier Supplement

Quantum Readiness Guidance for Regional and Specialty Insurance Carriers

Document ID	QCI-QS1-S5
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	Regional property and casualty carriers, life and annuity carriers, specialty lines carriers, managing general agents, and their technology service providers handling policyholder data and transaction records subject to NAIC Model Law requirements and state department of insurance examination
Effective date	September 23, 2026
Review cycle	Annual, or upon material NAIC model law developments, state DOI examination guidance changes, IAIS technology risk guidance updates, or a new edition of QCI-QS1

This supplement extends QCI-QS1 for the specific regulatory, actuarial, and data longevity context of regional and specialty insurance carriers. It maps quantum readiness requirements to the NAIC Insurance Data Security Model Law, state department of insurance examination frameworks, and the policy administration vendor dependencies that define most carriers' cryptographic posture. It addresses the data longevity characteristics of insurance that create the longest confidentiality horizons of any sector in the QCI supplement series.

Foreword

Insurance is the sector where long-horizon risk thinking is a professional discipline, not an abstract concern. Actuaries calculate mortality tables over 50-year periods. Life carriers price annuities assuming decades of future payments. Specialty lines underwriters model scenarios that have never occurred. The analytical culture of insurance is uniquely equipped to understand quantum risk — which makes the near-universal absence of quantum readiness programs in this sector one of the more striking gaps QCI has encountered across any industry.

The data longevity argument is more powerful for insurance than for any other sector in this supplement series. A whole life insurance policy issued to a 30-year-old in 2026 creates a confidentiality obligation extending to 2080 or beyond. Actuarial databases built over decades contain mortality, morbidity, and claims data whose value and sensitivity persist indefinitely. Annuity payment records carry financial and identity information that must remain protected for the life of the contract plus applicable statute of limitations periods. The policyholder data encrypted today and transmitted to reinsurers, third-party administrators, and state regulators will remain sensitive long after current encryption standards have been broken.

The regulatory environment is aligned for early movers. The NAIC Insurance Data Security Model Law has been adopted by 24 states and provides a direct framework for quantum readiness requirements in insurance. The IAIS technology risk guidance is moving toward explicit cryptographic resilience requirements. State department of insurance examinations are beginning to probe cybersecurity programs with increasing depth. Carriers that build documented quantum readiness programs now will be ahead of the examination questions rather than responding to examination findings.

The reinsurance dimension adds a consideration unique to this sector. A carrier's quantum exposure is not limited to systems they control directly. Policyholder data transmitted to reinsurers, ceded under treaty agreements, and processed by third-party administrators creates a cryptographic exposure chain that extends well beyond the carrier's own perimeter. Quantum readiness in insurance requires both a carrier-level program and a counterparty assessment discipline that this supplement addresses specifically.

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 confidentiality horizon replaces the data longevity field and is recorded as a date. Reinsurers and third-party administrators that hold ceded policyholder data on a critical flow are treated as critical suppliers for gate G70 purposes, which means a carrier cannot score above 70 until they have attested (new section 5.4). The Defensible readiness band now begins at 81, coverage under gate G60 is fixed at 95 percent of validated critical systems and critical flows, and the reinsurance transmission interfaces are the flows. Section 2.5 turns the NAIC mapping into the obligations register QCI-2.2-01 requires, and the 90-day quick start carries the 60-day supplier deadline and the annual refresh.

1. Scope and applicability

This supplement applies to:

- Regional property and casualty carriers licensed in one or more states and subject to NAIC model law cybersecurity requirements or equivalent state insurance cybersecurity laws
- Life and annuity carriers whose policy obligations extend over multi-decade periods, creating the longest confidentiality horizons of any entity in the QCI supplement series

- Specialty lines carriers including excess and surplus lines insurers, surety, title insurance, mortgage guaranty, and other specialty lines where policy data retention and transaction integrity obligations are material
- Managing general agents (MGAs) and managing general underwriters (MGUs) with delegated underwriting authority and access to policyholder data on behalf of carrier principals
- Third-party administrators (TPAs) processing claims or policy data under service agreements with carriers subject to this supplement

Why insurance data longevity is categorically different

The NAIC Model Law definition of nonpublic information includes personal financial information, health information, and information whose compromise would cause material harm to a consumer. Insurance carriers hold all three categories for policyholder populations that span decades. A life carrier may hold nonpublic information about a policyholder for 60 or more years — from policy issuance to claim settlement to statute of limitations expiry. No other commercial sector in the QCI supplement series holds sensitive personal data for periods this long with this breadth of sensitive data types. This creates a harvest-now, decrypt-later exposure window that extends further into the future than quantum computing timeline uncertainty itself.

Note on the AI-cryptographic provisions

QCI-QS1 carries conditional AI-cryptographic provisions. Where AI systems fall within the assessment scope — for a carrier, most often underwriting, pricing, fraud or claims-triage models — 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. Regulatory context

2.1 NAIC Insurance Data Security Model Law

The NAIC Insurance Data Security Model Law (MDL-668), adopted in 24 states as of early 2026, is the primary regulatory framework for insurance carrier cybersecurity in the United States. The Model Law requires carriers to implement an information security program that includes risk assessment, third-party service provider management, and incident response. Post-quantum cryptography maps directly to all three:

NAIC Model Law element	Requirement summary	Quantum readiness mapping
Section 4: Information Security Program	Carriers must implement a comprehensive written information security program based on risk assessment.	The quantum risk assessment, QASI inventory, and Q-Risk Score together constitute the quantum readiness component of the information security program. Document QCI-QS1 conformance, with its assessment type, as a sub-section of the information security program narrative.

NAIC Model Law element	Requirement summary	Quantum readiness mapping
Section 4(D): Risk Assessment	Annual risk assessment identifying reasonably foreseeable internal and external threats to nonpublic information.	Quantum computing is a reasonably foreseeable external threat to nonpublic information confidentiality. An annual risk assessment that omits quantum computing as an identified threat is increasingly difficult to defend as comprehensive. Add the QCI-QS1 risk analysis as the quantum component of the annual risk assessment.
Section 4(F): Third-Party Service Provider Management	Carriers must oversee service providers with access to nonpublic information, including contractual protections and periodic assessment.	Policy administration vendors, TPAs, and data processors with access to policyholder data are third-party service providers subject to this requirement. The Annex C attestation is a cryptographic safeguard assessment that satisfies the periodic assessment obligation for cryptographic controls specifically.
Section 5: Exemptions	Smaller carriers meeting asset and premium thresholds may qualify for reduced program requirements.	Exempt carriers should still complete a QASI and document quantum risk awareness. The exemption reduces program formality requirements, not the underlying exposure. A carrier that holds whole life policies remains exposed to harvest-now, decrypt-later risk regardless of its size.
Section 6: Investigation and Notification	Breach notification requirements apply to unauthorized acquisition of nonpublic information.	A future quantum decryption event affecting previously encrypted data in transit or at rest may trigger breach notification obligations. Carriers should consult counsel on whether a delayed-decryption scenario constitutes a notifiable event under their state's adoption of the Model Law, and record the conclusion as an incident-readiness decision under QCI-4.4-01.

2.2 State adoption variations

The 24 states that have adopted the NAIC Model Law have done so with varying modifications. Practitioners and carriers should review their specific state adoptions, but the following variations are most commonly material to quantum readiness:

- New York Cybersecurity Regulation (23 NYCRR 500): New York's regulation is more prescriptive than the NAIC Model Law and applies to all entities licensed under the New York Banking Law, Insurance Law, and Financial Services Law. The regulation requires encryption of nonpublic information in transit and at rest. PQC migration is a direct requirement when current encryption standards are no longer adequate — carriers licensed in New York should treat quantum readiness as a regulatory obligation with an enforcement mechanism, not merely a best practice.
- Ohio, Mississippi, South Carolina, Michigan, and Indiana adoptions follow the NAIC Model Law closely with minimal modifications. Carriers in these states can apply this supplement's guidance to Model Law compliance with minimal state-specific adaptation.
- States without Model Law adoption: approximately 26 states have not yet adopted the Model Law as of early 2026. Carriers operating only in these states face less immediate examination pressure but are not exempt from the underlying exposure. The harvest-now, decrypt-later risk to policyholder data does not vary by state of domicile.

2.3 IAIS technology risk guidance

The International Association of Insurance Supervisors (IAIS) publishes guidance on technology risk in insurance that influences domestic regulatory development. The IAIS Issues Paper on Cyber Risk Supervision and the Application Paper on the Supervision of Insurer Cybersecurity both reference cryptographic resilience as a supervisory concern. The IAIS is actively developing guidance on quantum computing as a systemic technology risk to the insurance sector — carriers with international operations or reinsurance relationships subject to foreign supervisor oversight should monitor IAIS guidance developments as an indicator of where domestic regulation is heading.

2.4 State department of insurance examination context

State DOI examinations are the enforcement mechanism for insurance cybersecurity requirements. The examination cycle for most regional carriers is every three to five years. Examiners are increasing the depth and technical sophistication of cybersecurity examination procedures, following the NAIC's Financial Examination Handbook updates that incorporate cybersecurity as a standard examination area.

The quantum readiness documentation package described in this supplement — risk assessment with quantum component, supplier attestation file, Q-Risk Score history with assessment type, information security program narrative — is designed to produce the artifacts that DOI examiners will look for when cybersecurity examination procedures incorporate quantum readiness questions. Carriers that have this documentation when the examination question arrives are commended. Those that do not have it create findings that stay in examination history.

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 for a carrier; each adds its own state adoptions, and verifies every entry against the source before the register is used.

Obligation	Issuer and document	Status	Affected systems and suppliers	Action and deadline
Information security program; annual risk assessment; third-party oversight; notification	NAIC MDL-668 as adopted by each licensing state	Law in adopting states; cite each state's version	PAS, claims, actuarial, agent portal; PAS vendor, TPAs, reinsurers, brokers	Quantum component in the annual risk assessment; Annex C attestation in third-party oversight; counsel view on delayed-decryption notification
Cybersecurity regulation, encryption in transit and at rest	NYDFS 23 NYCRR 500, current amendment	Regulation, for New York licensees	All systems holding nonpublic information	Treat PQC migration as a regulatory obligation; record the dated annual certification

Obligation	Issuer and document	Status	Affected systems and suppliers	Action and deadline
Insurer cybersecurity supervision	IAIS Application Paper on the Supervision of Insurer Cybersecurity	Guidance; indicator of regulatory direction	Group and cross-border operations	Monitor; record IAIS quantum guidance when issued
Financial examination	NAIC Financial Examination Handbook, cybersecurity procedures	Examination standard	All in-scope systems	Maintain the examination package in section 2.4; refresh with each quarterly score

3. Insurance data longevity and delayed-decryption exposure

3.1 The 50-year problem

Insurance is the only commercial sector in the QCI supplement series where the confidentiality horizon extends to 50 years and beyond. This creates a harvest-now, decrypt-later exposure window that outlasts the uncertainty in quantum computing timeline projections. Whatever the actual date when quantum computers capable of breaking current encryption become available — whether 2035, 2040, or later — the policyholder data a life carrier is encrypting today will still be sensitive and will still need to be protected on that date. Under QCI-QS1 the horizon is recorded as a date on each QASI record, and the long-horizon exposure flag (QCI-5.3-01) is raised wherever that date falls beyond the migration window.

Insurance data type	Typical retention	Exposure	Rationale
Whole life and universal life policy records	Duration of policy plus 7 to 10 years minimum; often permanent	Critical	A policy issued to a 25-year-old creates a 65-plus year data obligation. This exceeds any quantum timeline projection. Treat as permanent high exposure.
Annuity contract records	Duration of contract plus applicable statute of limitations; 30 to 60-plus years	Critical	Annuity records contain financial identity, beneficiary data, and payment history. Forgery or disclosure of annuity records enables financial fraud with multi-decade impact.
Actuarial mortality and morbidity data	Indefinite — historical experience data is retained permanently	High	Actuarial experience data aggregates individual health and mortality information. State-actor adversaries would find multi-decade mortality databases valuable for population-level intelligence.
Medical underwriting records	10 to 25 years depending on state law and policy type	High	Medical underwriting files contain health information used in coverage decisions. Disclosure affects employment, insurance eligibility, and personal privacy.
Claims files — long-tail liability lines	Open until final resolution plus statute of limitations; can extend 20 to 30-plus years	High	Long-tail liability claims (asbestos, environmental, professional liability) remain open for decades. Claims files contain sensitive health, legal, and financial information.

Insurance data type	Typical retention	Exposure	Rationale
Treaty reinsurance cession records	Duration of treaty plus 10 years minimum	High	Reinsurance cession records contain policyholder data shared with counterparties. Exposure extends to data in transit between carrier and reinsurer — both endpoints matter, and the transmission is a critical flow.
Property and casualty — standard lines	7 to 10 years typically	Medium to High	Shorter than life lines but policy and claims records still contain nonpublic financial and identity information. Long-tail lines (GL, workers comp) extend the retention window significantly.
Title insurance and mortgage guaranty records	Duration of property ownership plus applicable statutory period; can be 30 to 50-plus years	High	Title and MG records are tied to real property and maintain their value as long as the property exists. Compromise enables chain-of-title fraud with long-horizon impact.

3.2 The reinsurance exposure amplifier

Policyholder data does not stay within the carrier's perimeter. Reinsurance treaty cessions, facultative placements, and data sharing with third-party administrators mean that sensitive policyholder information travels across multiple cryptographic boundaries. Each transit is a potential harvest point, and each is a critical flow the QASI must carry with protection and authentication recorded at every hop (QCI-5.2-01).

For carriers with significant reinsurance programs, the quantum readiness question is not just 'are our own systems protected?' It is 'are all the systems that hold our ceded data protected?' The answer to the second question is almost universally unknown, because carriers rarely assess reinsurer cybersecurity programs with the depth needed to evaluate cryptographic posture. The supplier request process in QCI-QS1 applies to reinsurance counterparties as well as technology vendors — and this supplement addresses that counterparty assessment dimension specifically.

The actuarial argument for quantum readiness

Actuaries are trained to assess long-horizon risks with quantifiable but uncertain timelines. Quantum computing threat to encryption has exactly the characteristics that actuarial modeling handles well: a non-zero probability of occurrence over a long horizon, consequences that increase in severity over time if unmitigated, and a mitigation cost that is significantly lower if action is taken early. Frame the quantum readiness investment as an actuarially sound risk mitigation decision: the expected cost of early action is a fraction of the expected cost of late action or non-action. This framing reaches actuarial leadership and appointed actuaries in a way that conventional security arguments do not.

4. Policy administration vendor landscape

4.1 Vendor concentration and quantum dependency

Most regional insurance carriers depend on one of a small number of policy administration system (PAS) vendors for their core insurance operations. The PAS is the cryptographic center of gravity for the carrier's policyholder data — it handles data storage, communication encryption, and often identity management. As with core banking vendors in the financial

institution supplement, the carrier's quantum readiness is significantly constrained by the PAS vendor's PQC roadmap. The PAS vendor is a critical supplier under QCI-7.1-01 in every case, and gate G70 turns on its attestation.

The status column records what each vendor had published as of September 23, 2026 and changes with every vendor release. Confirm the current position with the vendor and record it, with the date, in the supplier record.

Vendor	Primary platforms	PQC status (reviewed September 23, 2026)	Recommended carrier action
Majesco	CloudInsurer, Policy, Billing, Claims	No public PQC statement located. The Spring '26 release announcement (April 2026) and FY25 results address AI and cloud, not cryptography.	Issue the Annex C request through account management. Reference NAIC Model Law Section 4(F) third-party oversight obligation. Request a written roadmap referencing NIST FIPS 203, 204, 205 and the officer attestation.
Duck Creek Technologies	Policy, Billing, Claims, Distribution	Trust page lists ISO 27001, SOC 1 and SOC 2 Type II and PCI-DSS, with GDPR, DORA and APRA alignment; it gives no cryptographic algorithm detail and no PQC statement.	Engage Duck Creek's platform security team through the account manager. For SaaS clients, Duck Creek controls the crypto stack entirely — vendor engagement is the only available action, and the attestation is the only evidence QCI-4.8-03 accepts.
Guidewire	PolicyCenter, BillingCenter, ClaimCenter, InsuranceSuite	No public PQC statement located on guidewire.com or in the Guidewire trust center.	Route through Guidewire's CISO or product security team, not account management. Reference Guidewire's existing security commitments and frame PQC as a natural extension of their security standards leadership.
OneShield	Policy, Billing, Claims (specialty and E&S focus)	Registered under the Cloud Security Alliance AI Controls Matrix (2026), the first insurance software vendor to do so. No PQC statement located.	Direct engagement with OneShield technical team is feasible given smaller vendor scale. Coordinate with peer OneShield clients to submit a joint request — collective leverage is high relative to vendor scale, and one attestation can serve many.
Legacy mainframe systems (various)	IBM-based platforms, often decades old	IBM z17 generally available June 2025. CCA 8.4 for z17 and z16 adds ML-KEM and ML-DSA on Crypto Express 8S, with EP11 support on z/OS and Linux on IBM Z; IBM zCDI, ADDI and CAT provide cryptographic discovery. Infrastructure-level readiness is real; application-layer PAS cryptography remains carrier- or vendor-managed and has no roadmap of its own.	This is the most complex vendor situation. Carriers on legacy mainframe PAS need to separate the IBM infrastructure-level PQC question from the application-layer crypto question. Engage IBM for infrastructure and internal teams for application layer. Begin migration planning to modern PAS as a long-term strategic action, recorded as a long-lead decision under QCI-4.2-02.

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.

- Majesco, Spring '26 release announcement, April 7, 2026, and FY25 results, February 3, 2026: majesco.com/press

- Duck Creek Technologies, Security and Trust: duckcreek.com/trust
- OneShield, registration under the Cloud Security Alliance AI Controls Matrix, 2026: oneshield.com/knowledge_hub
- IBM, Quantum Safe on IBM Z: ibm.com/z/quantum-safe; IBM Crypto Education Community, CCA 8.4 for IBM z17 and z16: ML-KEM and ML-DSA, June 26, 2025, and Using ML-DSA and ML-KEM on IBM Z, November 6, 2025: community.ibm.com

5. Reinsurance counterparty quantum risk assessment

5.1 Why reinsurance counterparties require separate assessment

Reinsurance represents a data sharing relationship that most carrier cybersecurity programs treat as a contractual and financial risk matter, not a cryptographic exposure. In the quantum readiness context, every policyholder data transmission to a reinsurance counterparty is a potential harvest event. The data shared — policy details, claims history, medical underwriting data — is among the most sensitive in the carrier's possession, and it travels to systems the carrier does not control.

The scale of this exposure is significant. A carrier with active treaty reinsurance programs may transmit policyholder data to five to fifteen reinsurance counterparties annually. Each counterparty's cryptographic posture is a component of the carrier's effective quantum exposure. A carrier with an excellent internal quantum readiness program but no reinsurer assessment discipline has an incomplete program.

5.2 Reinsurance counterparty request framework

The QCI-QS1 supplier request process applies to reinsurance counterparties with the following adaptations. The adaptations change the framing and the routing of the request; they do not change the minimum contents of QCI-7.2-01 or the attestation form of QCI-7.2-02.

- Frame the request as a counterparty risk assessment, not a vendor security assessment. Reinsurers are not vendors — they are financial counterparties. The request should reference the carrier's information security program obligations under the NAIC Model Law and ask for the reinsurer's written confirmation that policyholder data received from the carrier is protected by cryptographic controls that include a post-quantum migration roadmap.
- Target the reinsurer's CISO or Chief Information Officer, not the treaty underwriter. Reinsurer underwriters manage the financial relationship. The technical question requires a technical contact. The attestation still needs an officer's signature.
- Distinguish between data at rest and data in transit. Some reinsurers may have strong encryption at rest but legacy TLS configurations for data transmission. Request confirmation of both, and record the transmission as a critical flow with its protection at each hop.
- For facultative placements, the counterparty is the individual reinsurer accepting the risk, not a treaty relationship. Facultative quantum risk assessment requires a lighter-weight process — a standard attestation request that can be incorporated into the facultative placement documentation.

5.3 The reinsurance broker intermediary

Many carriers place reinsurance through intermediary brokers (Aon, Marsh, Guy Carpenter, and others). These brokers handle policyholder data as part of placement submissions. They are third-party service providers under the NAIC Model Law and should receive Annex C requests

as part of the carrier's third-party oversight program. The reinsurance broker's quantum readiness is often better than the reinsurer's because brokers operate modern technology platforms with more frequent update cycles than legacy reinsurance administration systems.

5.4 What gate G70 means for a carrier

Under QCI-QS1 v2.3, a carrier cannot score above 70 until every critical supplier has provided a current, adequate response and an officer-signed attestation (gate G70, QCI-6.3-01), and an approved exception does not lift the cap. A critical supplier is one whose product or service sits on a critical trust pathway or critical flow (QCI-7.1-01). That definition reaches further in insurance than in most sectors: the PAS vendor and the claims platform, certainly, but also every TPA and every reinsurer that receives policyholder data on a treaty or facultative flow the QASI has marked critical. A reinsurer is a counterparty in the treaty and a critical supplier in the register.

The practical consequence is that a carrier's score is capped at 70 by its least responsive reinsurer until that reinsurer attests, however strong the internal program. That is the standard measuring the exposure honestly: the ceded data is exposed at the reinsurer, not at the carrier. The carrier's levers are the counterparty request of section 5.2 with its 60-day deadline (QCI-7.2-04), treaty renewal language that makes the attestation a condition, and coordination with other cedants through the broker so the reinsurer signs once. A carrier held at 70 with the register showing each request, its deadline, its escalation and the data-minimization treatment verified is in a defensible examination position. A carrier reporting 76 with an unattested reinsurer holding its life book is not.

6. QASI record guidance for insurance carriers

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). Records that have not been validated by their system owner and a technical reviewer, or that are older than 90 days, do not count toward coverage (QCI-5.1-03, QCI-5.1-04).

QASI field	Insurance-specific guidance
Business criticality	Policy administration system: always High. Claims system: High. Actuarial and pricing systems: High if they hold individual policyholder data, Medium if aggregate only. Reinsurance administration: High for systems transmitting policyholder data, Medium for aggregate reporting. Agent portal: High if it provides access to policyholder nonpublic information.
Data classification	Apply NAIC Model Law nonpublic information definition: personal financial information, health information, and information whose compromise would cause material harm. Most policyholder data qualifies as Regulated for QASI purposes. Actuarial experience data is Confidential at minimum — its aggregate nature does not reduce sensitivity.
Confidentiality horizon	Record a date, using the longer of the contractual obligation period and the applicable statute of limitations. For whole life and annuity: use permanent or 60-plus years. For long-tail liability lines: use 30 years as a conservative estimate. For standard P&C lines: use 10 years minimum. Do not use the minimum statutory retention period — use the realistic period during which a claim could be made or data could be subpoenaed. The appointed actuary confirms the basis.

QASI field	Insurance-specific guidance
Critical flows	Inventory reinsurance data transmission interfaces explicitly as flows (QCI-5.2-01). These are often API connections or secure file transfers that have different cryptographic configurations than policyholder-facing systems. Document the protocol, the key-establishment method, the authentication, and the counterparty at each hop. Add TPA feeds, agent portal sessions, and regulator submissions.
Supplier dependencies	Document the PAS vendor, the claims system vendor, and the reinsurance administration system separately. Add reinsurance counterparties and TPAs as suppliers where they hold ceded policyholder data on a critical flow — they are not vendors in the commercial sense but they are critical suppliers for Pillar 5 and gate G70.
Identity records	Under QCI-5.2-02, agent and adjuster credentials are human identities; the API keys and certificates between the PAS, the claims platform, the reinsurance gateway and the TPAs are workload identities. Both are inventoried, with the signing algorithm and the trust anchor recorded.
Exposure flags	Raise the long-horizon flag (QCI-5.3-01) for any system holding nonpublic personal information with a horizon beyond the migration window. For life and annuity systems and long-tail liability claims systems it is always raised. For reinsurance interfaces it is raised at both endpoints. For standard P&C systems with short retention, raise it only where the data includes health information. Treatment status is recorded separately (QCI-5.3-02); a plan does not clear a flag.
Treatment and compensating controls	Data minimization is the most effective insurance compensating control — carriers that transmit only the minimum data necessary to reinsurers and TPAs reduce their third-party exposure. Tokenization of policyholder identifiers in transmitted data is a strong compensating control that many carriers already implement for fraud prevention purposes. Either counts as treatment only once verified in the actual transmission (QCI-5.3-02).

7. Governance model for insurance carriers

QCI-4.1-01 requires documented responsibilities across the functions below and a cross-functional steering function. The mapping for a carrier:

QCI-QS1 role	Insurance carrier mapping	Insurance-specific consideration
Executive Sponsor	CISO, CTO, or Chief Risk Officer — whoever has cross-functional authority over information security and vendor management	At many regional carriers the CRO has broader enterprise risk authority than the CISO. Where this is the case, the CRO is the more appropriate executive sponsor because quantum risk spans both IT security and enterprise risk management.
Quantum Risk Owner	Senior information security manager or enterprise risk manager with access to technology and actuarial teams	The Quantum Risk Owner needs actuarial access to set confidentiality horizons accurately. Appoint someone who has relationships with both IT security and the actuarial function.

QCI-QS1 role	Insurance carrier mapping	Insurance-specific consideration
Steering function (risk committee)	Enterprise Risk Committee or Technology Risk Committee with representation from actuarial, IT, compliance, and legal	Appointed actuaries and chief actuaries should be represented on the quantum risk governance structure. Their analytical expertise is directly applicable to the long-horizon risk assessment that quantum readiness requires.
Governing body	Board Audit Committee or Risk Committee — wherever cybersecurity reporting currently goes	State insurance boards and mutual company boards often include fewer technology-sophisticated directors than stock company boards. Frame quantum risk for this audience using policy obligation and regulatory examination language rather than technical security language. Any accepted risk is approved explicitly (QCI-8.2-01).
Third-party oversight	Vendor management team with both IT vendor and reinsurance counterparty scope	This is the governance structure gap most unique to insurance: most vendor management programs cover technology vendors but not reinsurance counterparties. Extending third-party oversight scope to include reinsurers requires explicit governance authorization, and the register must carry both.

8. Q-Risk Score guidance for insurance carriers

8.1 Realistic band targets by carrier profile

Bands run from Exposed (0 to 19) through Defensible readiness (81 to 100); a score of 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). None approaches 70, and none could while the PAS vendor or a critical reinsurer is unattested.

Carrier profile	Typical start	12-month target	Primary constraint
Regional P&C carrier, under \$500M DWP	10 to 22	28 to 44 (Behind to Mobilizing)	P5 — PAS vendor attestation and reinsurer assessment both absent
Regional P&C carrier, \$500M to \$2B DWP	14 to 28	34 to 52 (Behind to Mobilizing)	P3 — long-tail line horizons underappreciated; P4 — PAS vendor migration dependency
Life and annuity carrier, any size	8 to 20	26 to 42 (Behind to Mobilizing)	P3 — 50-plus year horizon requires explicit governing-body acknowledgment; P5 — reinsurer assessment absent
Specialty lines / E&S carrier	10 to 22	28 to 44 (Behind to Mobilizing)	P2 — specialty data types require custom QASI field guidance; P5 — MGA and TPA ecosystem is complex
Title insurance carrier	8 to 18	24 to 40 (Behind to Mobilizing)	P3 — permanent retention obligation for real property records; P4 — legacy title plant systems

Carrier profile	Typical start	12-month target	Primary constraint
MGA or MGU	6 to 16	22 to 36 (Behind)	P1 — governance often informal given MGA structure; P5 — carrier principal oversight of MGA quantum posture is a gap on both sides

9. Insurance carrier 90-day quick start

This sequence adapts QCI-QS1 Clause 9.1 for a carrier. It is a planning aid, not a conformance grace period.

Timeframe	Phase	What to accomplish	Output
Week 1	Governance and scope	Name executive sponsor and Quantum Risk Owner. Declare the assessment boundary and criticality criteria (QCI-1.1-01). Engage actuarial leadership to confirm confidentiality horizons by line of business. This actuarial consultation is unique to insurance and should happen in week 1 — it shapes the horizon field for every subsequent record. Seed the obligations register from section 2.5.	Named governance roles. Approved boundary. Actuarial horizon confirmation by line of business. Quantum risk added to information security program scope. Register started.
Week 2	PAS vendor engagement	Issue the Annex C request to the policy administration system vendor. This is the highest-leverage near-term action because the PAS holds the largest concentration of policyholder nonpublic information. Reference NAIC Model Law Section 4(F) in the request.	PAS vendor request issued with 60-day response deadline (QCI-7.2-04). Logged in supplier record with NAIC Model Law reference.
Weeks 3 to 4	Reinsurance and TPA requests	Issue attestation requests to the top five reinsurance counterparties and top three TPAs. Use the counterparty framing from section 5.2 rather than the standard vendor framing; keep the QCI-7.2-01 minimum contents.	Reinsurance and TPA requests issued with the 60-day deadline. Counterparty request log opened, separate from the IT vendor log but in the same supplier register.
Weeks 5 to 7	QASI build	Build linked QASI records for all critical systems and critical flows using the guidance in section 6. Apply actuarially confirmed horizons. Raise the long-horizon flag on every qualifying record. Validate each record with its owner and a technical reviewer.	QASI complete for critical systems and flows; coverage computed for each per QCI-5.1-03. Horizons documented per record with actuarial basis. Top 10 remediation targets identified.
Weeks 8 to 9	Risk assessment update	Add the quantum computing section to the annual information security risk assessment. This integrates QCI-QS1 with NAIC Model Law Section 4(D) compliance in a single document. Record the cryptographic incident scenarios of QCI-4.4-01 in the incident plan.	Information security risk assessment updated with quantum component. Legal counsel briefed on the delayed-decryption notification question.
Week 10	Score	Produce the first Q-Risk Score with the Annex B worksheet, labelled self-assessment (QCI-1.2-03), with gate results. Apply the reinsurance dimension as a P5 sub-note.	Q-Risk Score snapshot with assessment type and conformance status. P5 note distinguishing IT vendor status from reinsurance counterparty status.

Timeframe	Phase	What to accomplish	Output
Weeks 11 to 12	Brief and plan	Deliver the governing-body insert (QCI-8.1-01) using actuarial framing for horizons. Brief the appointed actuary separately on long-horizon risk implications. Open the exception register (QCI-4.3-02) for unresponsive suppliers. Prepare the DOI examination documentation package. Diary the annual supplier refresh (QCI-7.2-04).	Governing-body briefing delivered. Appointed actuary briefed. Exception register open. DOI examination package prepared.

10. Summary and engagement

Insurance carriers hold the longest-lived sensitive personal data of any commercial sector. The policies written today will create confidentiality obligations that extend decades past any current quantum computing timeline estimate. The carriers that build documented quantum readiness programs now will not be caught unprepared when PQC requirements become examination standards, when reinsurers begin requiring quantum readiness attestation from cedants, or when the first delayed-decryption event affecting insurance data becomes public.

The actuarial culture that defines this sector is QCI's greatest ally here. The argument for early action is an actuarial argument: the expected cost of acting now is a fraction of the expected cost of acting under pressure, and the probability-weighted harm of inaction compounds with every year that policyholder data remains harvested but unread. No other sector in the QCI supplement series is better equipped analytically to make this calculation and act on it.

QCI engagement support for insurance carriers

QCI works with regional P&C carriers, life and annuity carriers, specialty lines carriers, and MGAs to deliver QCI-QS1 assessments calibrated to insurance confidentiality horizons, facilitate reinsurance counterparty quantum risk assessments, integrate quantum readiness into NAIC Model Law compliance programs, and prepare appointed actuary briefings that translate quantum risk into the probability and long-horizon framing that actuarial leadership responds to. Independent assessment under QCI-1.2-03 is available separately. Contact QCI to discuss how an engagement is structured for your carrier profile and line of business mix.

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; confidentiality horizon replaces data longevity and is recorded as a date; reinsurers and TPAs on critical flows treated as critical suppliers for gate G70 (new section 5.4); reinsurance interfaces inventoried as critical flows; Defensible readiness band at 81; G60 fixed at 95 percent for systems and flows; obligations register section 2.5 added; identity record and treatment guidance per QCI-5.2-02 and QCI-5.3-02; 60-day supplier deadline and annual refresh; assessment type labelling; governing-body terminology.
1.1	June 10, 2026	Aligned to QCI-QS1 v2.2; AI-cryptographic provisions note added.