QTONIC QUANTUM
POST QUANTUM READY

POST-QUANTUM READINESS BENCHMARK

Benchmark Methodology Note

Best-and-final public supporting note for media, analyst, customer, and procurement inquiries related to Qtonic Quantum's synthesized post-quantum readiness benchmark.

Version	Prepared by	Use	Contact
1.0 - May 2026	Qtonic Quantum Corp	Public supporting note	contact@qtonicquantum.com

Executive Summary

Qtonic Quantum presents this benchmark as a synthesized readiness estimate, not a direct census of every Fortune 1000 company, federal system, or military/NSS environment. The benchmark estimates practical post-quantum readiness by weighting actual migration capability, deployed post-quantum cryptography, inventory completeness, vendor visibility, and procurement-ready evidence more heavily than awareness, policy existence, or planning activity.

18 / 100	24 / 100	30 / 100	24 / 100
Fortune 1000 enterprises	U.S. civilian federal	U.S. military / NSS / DoD	Equal-weighted average

Core principle: the benchmark intentionally discounts general awareness and policy discussion unless supported by cryptographic inventory, tested deployment, vendor evidence, or procurement-ready proof.

Recommended Public Formulation

Qtonic Quantum's synthesized benchmark estimates Fortune 1000 post-quantum readiness at 18 / 100, U.S. civilian federal readiness at 24 / 100, and U.S. military/NSS/DoD readiness at 30 / 100. The benchmark synthesizes public deployment telemetry, federal accountability findings, national-security policy guidance, and Qtonic Quantum field observations.

Public use note: when citing the benchmark, identify it as a Qtonic Quantum synthesized readiness benchmark and include the applicable range or limitation when space permits.

Methodology at a Glance

The benchmark is designed to answer one practical question: can an organization produce evidence of post-quantum readiness when a buyer, auditor, acquiring agency, insurer, or board asks for proof?

Readiness Scoring Pipeline

1. Source collection	2. Evidence classification	3. Readiness scoring	4. Segment calibration	5. Range review

The methodology combines public sources and Qtonic Quantum field observations, then applies conservative interpretation to avoid treating awareness, policy, or future intent as deployed readiness.

Directional Weighting

Evidence category	Directional weight	Reason
Deployed quantum-safe or hybrid controls	Highest	Direct evidence that migration is operating in a real environment.
Cryptographic inventory completeness	High	Readiness is not credible without knowing where vulnerable cryptography exists.
Vendor and dependency visibility	High	Enterprise exposure is often inherited through suppliers, products, managed services, and cloud platforms.
Migration execution maturity	Medium-high	Shows resourcing, prioritization, timelines, and operational remediation.
Procurement-ready evidence	Medium-high	Shows whether claims can survive buyer, auditor, agency, insurer, or board scrutiny.
Awareness, policy, or strategic planning	Lowest	Important context, but not evidence of deployed readiness without inventory or implementation proof.

Formal weighting rule: direct deployment telemetry, validated implementation evidence, and field observations are weighted more heavily than surveys, policy statements, public strategy language, or general awareness indicators.

Evidence Hierarchy and Confidence Model

The benchmark uses an evidence hierarchy so that observable deployment and technical signals are treated as stronger than opinion, awareness, or mandate language. This prevents the score from overstating readiness when organizations have plans but limited implementation.

Confidence tier	Evidence type	How it influences scoring
Tier 1 - Highest	Validated deployment evidence and tested PQC/hybrid implementations	Strong positive readiness signal.
Tier 2	Cryptographic inventory findings and vulnerability assessments	Strong signal for operational visibility and exposure.
Tier 3	Vendor, dependency, and procurement documentation	Strong signal when tied to actual systems and reviewable evidence.
Tier 4	Public deployment telemetry and sector-level adoption data	Useful calibration signal, especially for observable external services.
Tier 5	Surveys and executive self-reporting	Useful directional signal, discounted when unsupported by deployment evidence.
Tier 6 - Lowest	Policy mandates, roadmaps, awareness, or planning statements	Context only unless paired with inventory, execution, or deployment proof.

Observed vs. Inferred Signals

Signal class	Examples	Treatment
Observed signals	Validated deployment, inventory outputs, test evidence, vendor documentation, confirmed findings.	Weighted more heavily.
Inferred signals	Survey responses, strategy documents, policy milestones, mandate exposure, public-sector guidance.	Used to calibrate but discounted if not tied to deployment.

Confidence level is strongest when multiple evidence classes point in the same direction. For the current benchmark, DigiCert implementation data, IBM/CSA readiness scoring, F5 deployment telemetry, GAO federal findings, NIST/NSA timelines, and Qtonic Quantum field observations all support a low-readiness conclusion.

Scoring Architecture

The benchmark evaluates practical post-quantum readiness across six dimensions. Each dimension is interpreted through an implementation-weighted lens: evidence of deployed controls, inventory, and remediation matters more than general awareness.

Readiness dimension	What is assessed	Procurement-ready signal
Inventory completeness	Visibility into RSA, ECC, key exchange, certificates, libraries, protocols, embedded dependencies, and supply-chain exposure.	Current, repeatable, evidence-backed cryptographic inventory.
Quantum-vulnerable exposure	Concentration of CRQC-vulnerable primitives and long-lived sensitive data pathways.	Exposure reduction, compensating controls, or documented migration path.
Deployment maturity	Actual use of quantum-safe or hybrid post-quantum mechanisms in relevant environments.	Tested deployment rather than policy intent.
Vendor dependency visibility	Cryptographic dependencies inherited through suppliers, products, managed services, and cloud platforms.	Written vendor evidence and mapped dependencies.
Migration execution	Prioritization, ownership, budget, timelines, and remediation programs for cryptographic transition.	Funded execution with measurable milestones.
Readiness evidence	Documentation that can satisfy buyers, auditors, acquiring agencies, insurers, and boards.	Evidence package that can survive review.

Score Interpretation Bands

Score band	Interpretation
0-20	Minimal practical readiness. Awareness may exist, but inventory evidence, deployed controls, and procurement proof are limited.
21-40	Planning-stage readiness. Governance or inventory activity may exist, but migration remains incomplete and evidence is immature.
41-60	Partial readiness. Some PQC/hybrid deployment, vendor evidence, or migration programs exist, but coverage is inconsistent.
61-80	Advanced readiness. Material inventory, deployment, and procurement evidence exist across important systems.
81-100	Mature readiness. Broad, tested, evidence-backed post-quantum posture with ongoing governance and auditability. As of May 2026, Qtonic Quantum believes few if any large organizations demonstrate sustained enterprise-wide maturity in this upper band.

Segment Benchmark and Dual-Axis Interpretation

The benchmark distinguishes strategic readiness from operational readiness. Awareness and governance have improved, but deployment maturity, inventory completeness, and procurement-ready evidence remain materially lower.

Segment	Point estimate	Defensible range	Strategic readiness	Operational readiness	Primary rationale
Fortune 1000 enterprises	18 / 100	12-25	Moderate awareness	Low deployment	Awareness exists, but real PQC deployment and complete inventory evidence remain rare.
U.S. civilian federal	24 / 100	18-32	Higher governance	Planning-stage execution	Mandates and inventories exist, but GAO findings show strategy, coordination, and milestone gaps.
U.S. military / NSS / DoD	30 / 100	23-40	High policy pressure	Hard migration ahead	Clearer deadlines, but weapons systems, OT, embedded platforms, classified systems, and refresh cycles slow implementation.
Equal-weighted average	24 / 100	18-32	Directional only	Directional only	Simple average across the three segments, not a census or market-size-weighted estimate.

Equal-weighted average caveat: the equal-weighted average is presented only as a directional simplification and should not be interpreted as proportional market exposure, aggregate national readiness, or a statistically weighted estimate of all affected systems.

Why the Fortune 1000 Estimate is 18 / 100

The Fortune 1000 score is an extrapolated readiness estimate, not a direct audit of every Fortune 1000 company. It reflects low public implementation signals, low broad-market quantum-safe deployment, and Qtonic Quantum field observations frequently identifying incomplete cryptographic inventory coverage and limited procurement-ready migration evidence in large enterprise environments.

Public Evidence Base

The benchmark uses public evidence to calibrate Qtonic Quantum field observations and to avoid relying on internal experience alone. The source mix supports a consistent conclusion: awareness is ahead of deployment, and deployed post-quantum readiness remains early-stage.

Source class	Key public signal	Benchmark implication
NIST standards baseline	NIST finalized the first three PQC standards in August 2024.	The standardized baseline is still new for large-scale production migration.
DigiCert 2025 Quantum Readiness Study	69% recognized quantum risk; only 5% had implemented quantum-safe encryption.	Awareness materially exceeds implementation.
IBM Institute for Business Value / Cloud Security Alliance	Average quantum-safe readiness score: 25 / 100. Top decile scored 35 or above; highest score reached 50.	Even leaders remain short of mature readiness.
F5 Labs web telemetry	8.6% of the top one million websites supported hybrid PQC key exchange; 23.1% among top 1,000; about 2.9% among identified banking websites.	Public deployment signals remain low, including in security-sensitive sectors.
GAO 2025 federal findings	Federal strategy documents lacked full strategy definition, performance measures, interim agency migration milestones, and comprehensive coordination.	Government posture is more inventory/planning than completed migration.
OMB / NSA / CNSA 2.0 guidance	Agencies and NSS owners face inventory, acquisition, phase-out, mandatory-use, and 2035 readiness milestones.	Policy pressure is clear, but full deployed transition remains multi-year.

How external evidence is used

Public evidence is not treated as a substitute for system-level audits. Instead, it is used to bound plausible readiness estimates, identify directional adoption patterns, and prevent the benchmark from assigning high readiness based on mandates or awareness alone.

Qtonic Quantum Field Data: Definitions and Boundaries

Qtonic Quantum field observations are used as corroborating evidence. They inform segment estimates, but they do not make the benchmark a statistical census or independently audited dataset.

Field Data Scope

Field observations are derived from multiple enterprise cryptographic risk and vulnerability assessments across large-enterprise and regulated environments conducted during 2025-2026. Where cited publicly, field evidence should be described as Qtonic Quantum field observations unless an independent review or formal dataset publication is completed.

Term	Definition
Field engagement	A Qtonic Quantum enterprise assessment, review, or readiness engagement involving cryptographic risk, post-quantum exposure, or migration evidence.
Cryptographic finding	A vulnerable algorithm, weak or non-compliant primitive, exposed certificate, library dependency, protocol issue, key-exchange issue, or other cryptographic control requiring review or remediation.
Harvest-now-decrypt-later exposure	A pathway in which long-lived sensitive data may be collected today and later decrypted if relevant public-key protections are broken by a cryptographically relevant quantum computer.
Procurement-ready evidence	Documentation, inventory, technical validation, implementation review, vendor evidence, and remediation status that can support a buyer, auditor, acquiring agency, insurer, or board review.

Preferred field-data language

Use: "Qtonic Quantum field observations frequently identify incomplete cryptographic inventory coverage and limited procurement-ready migration evidence in large enterprise environments." Avoid: broad claims that imply a census, full-market audit, or independently validated statistical sample unless those artifacts are separately published.

Limitations and Proper Use

This methodology is designed to support clear public communication while avoiding overclaiming. The benchmark should be used as a conservative, evidence-based readiness estimate, not as a substitute for a customer-specific cryptographic assessment.

Limitations

Limitation	Meaning
Not a census	The benchmark does not directly audit every Fortune 1000 enterprise, federal system, or military/NSS environment.
Not independently audited	The methodology has not been independently validated by a third-party standards body unless separately stated.
Synthesized evidence model	Scores combine public telemetry, surveys, government findings, policy guidance, field observations, and expert interpretation.
Field-data boundaries	Qtonic Quantum field observations may overrepresent organizations already concerned about cryptographic risk.
Segment estimates	Segment scores are conservative estimates intended to communicate readiness direction and relative maturity.

Appropriate and Inappropriate Uses

Appropriate use	Inappropriate use
Citing the benchmark as Qtonic Quantum's synthesized readiness estimate.	Claiming the benchmark is a direct Fortune 1000 census.
Using the ranges to show uncertainty and defensibility.	Presenting point estimates as exact measurements without noting synthesized methodology.
Using the benchmark to frame market readiness, procurement pressure, and evidence gaps.	Claiming independent third-party validation unless a review has been completed.
Using the note to support media, analyst, customer, and procurement discussions.	Using the benchmark as legal, compliance, investment, audit, or procurement advice.

Public Source List

The sources below are the public evidence base supporting the benchmark. Qtonic Quantum field data is used as corroborating internal evidence and should be described as field observations unless independently audited.

Source	Reference
NIST: First finalized post-quantum encryption standards, August 2024	https:/ / www.nist.gov/ news-events/ news/ 2024/ 08/ nist-releases-first-3-finalized-post-quantum-encryption-standards
DigiCert: 2025 Quantum Readiness Study	https:/ / www.digicert.com/ news/ quantum-readiness-gap-a-digicert-study-on-quantum-safe-encryption
IBM Institute for Business Value / Cloud Security Alliance: Secure the Post-Quantum Future, 2025 Quantum-Safe Readiness Index	https:/ / www.ibm.com/ thought-leadership/ institute-business-value/ en-us/ report/ 2025-quantum-safe-readiness
F5 Labs: The State of Post-Quantum Cryptography on the Web, 2025	https:/ / www.f5.com/ labs/ articles/ the-state-of-pqc-on-the-web
U.S. Government Accountability Office: Quantum Computing - Leadership Needed to Coordinate Cyber Threat Mitigation Strategy, GAO-25-108590, 2025	https:/ / www.gao.gov/ products/ gao-25-108590
NIST: Cryptographic Module Validation Program / FIPS 140-3 Transition Effort	https:/ / csrc.nist.gov/ projects/ cryptographic-module-validation-program
OMB M-23-02: Migrating to Post-Quantum Cryptography	https:/ / www.whitehouse.gov/ wp-content/ uploads/ 2022/ 11/ M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf
NSA / CNSSP 15 / CNSA 2.0 guidance and transition timelines	https:/ / media.defense.gov/ 2022/ Sep/ 07/ 2003071834/ -1/ -1/ 0/ CSA_CNSA_2.0_ALGORITHMS_.PDF
NIST IR 8547: Transition to Post-Quantum Cryptography Standards, Initial Public Draft	https:/ / csrc.nist.gov/ pubs/ ir/ 8547/ ipd
Craig Gidney: How to factor 2048 bit RSA integers with less than a million noisy qubits, arXiv, May 2025	https:/ / arxiv.org/ abs/ 2505.15917

Note: Links are provided as reference pointers. Readers should verify current versions of source materials before relying on any quoted timelines or requirements.

Legal Notice, Non-Reliance, and Copyright

Non-reliance. This document is provided for general informational and public communication purposes only. It is not intended to be, and should not be relied upon as, legal, regulatory, compliance, procurement, investment, insurance, audit, engineering, security certification, or professional advice. Readers should consult qualified advisors and conduct independent technical and legal review before making decisions based on post-quantum readiness, cybersecurity compliance, procurement requirements, or cryptographic migration.

No warranty. Qtonic Quantum Corp provides this document on an "as is" basis without warranties of any kind, express or implied, including but not limited to warranties of accuracy, completeness, merchantability, fitness for a particular purpose, non-infringement, or suitability for any particular procurement, regulatory, technical, or business purpose.

Synthesized estimate. The benchmark described in this document is a synthesized readiness estimate derived from public deployment telemetry, surveys, federal accountability findings, national-security guidance, Qtonic Quantum field observations, and expert interpretation. It is not a direct census, statistical audit, independent third-party validation, or complete assessment of every organization, system, or segment referenced.

Third-party sources and no endorsement. References to NIST, GAO, OMB, NSA, Cloud Security Alliance, IBM, DigiCert, F5 Labs, arXiv, the U.S. Department of Justice, or any other third party are for attribution and evidentiary context only. Such references do not imply endorsement of Qtonic Quantum Corp, this document, the benchmark, or any Qtonic Quantum product or service by those organizations.

Trademarks. Qtonic Quantum, QScout, QStrike, QSolve, Qtonic Quantum Lab, and related marks are trademarks, service marks, or trade names of Qtonic Quantum Corp. Other names, brands, and marks are the property of their respective owners.

Forward-looking and change-sensitive information. Regulatory, procurement, standards, and threat timelines may change. Quantum computing research, post-quantum cryptography implementation practice, federal acquisition requirements, and industry adoption rates are evolving. Readers should verify current requirements, standards, and source materials before acting on any dates, estimates, or readiness conclusions.

Permitted attribution. When citing this document, use: Qtonic Quantum Corp, *Post-Quantum Readiness Benchmark Methodology Note*, Version 1.0, May 2026. Public summaries should describe the benchmark as a Qtonic Quantum synthesized readiness estimate unless and until a separately published independent validation is completed.

Contact: contact@qtonicquantum.com
Website: qtonicquantum.com