From Quantum Curiosity to Commercial Value

An executive framework for determining whether quantum computing is relevant to the business, which problems deserve attention, and whether expected value justifies investment.

WHITE PAPER • 2026 EDITION

Classical first. Quantum where justified. Evidence before scale.

Business fit • problem selection • commercial benefits • ROI • governance • quantum-safe security

Jami Kiran
Trusted Global Technology Advisor
AI • Data • Cybersecurity • Cloud • Quantum

PURPOSE AND AUDIENCE

Why this white paper exists

Quantum computing is moving from laboratory discussion into board-level strategy. Yet interest alone is not a business case.

Executives face two different questions. The first is whether quantum computing could improve a commercially important problem. The second is whether quantum-era security requires action before useful large-scale quantum computing is available. These questions must be assessed separately, with different timelines, owners and investment criteria.

Opportunity question

Can a quantum, hybrid or quantum-inspired approach create measurable advantage over the best classical method?

Value · Feasibility · Timing

Security question

Which long-lived data, systems and cryptographic dependencies require migration to quantum-resistant protection?

Inventory · PQC · Crypto agility

Intended readers

Boards and CEOs

Strategic relevance, investment discipline and risk oversight.

CIOs, CTOs and CISOs

Architecture, security, data and technology readiness.

Business and innovation leaders

Problem selection, value measurement and adoption.

Central principle: the objective is not to prove that the company needs quantum computing. The objective is to determine where quantum is relevant, where it is not, and what evidence is required before the next investment.

Readiness is a business discipline

> **Fifteen years ago, organisations assessed cloud readiness before modernising at scale. Today, they need the same discipline for quantum.**

Quantum readiness is not the purchase of a quantum computer. It is the ability to identify suitable problems, compare quantum approaches with strong classical baselines, prepare data and talent, quantify commercial value, manage security exposure and make evidence-based funding decisions.

A company may be ready to explore when:

- A high-value problem is limited by computational complexity.
- Even a small improvement would create material value.
- Data and business ownership are available.
- A credible classical benchmark can be established.

A company should pause when:

- The real constraint is poor data or an immature process.
- Classical methods already meet the business need.
- The improvement cannot be valued or adopted.
- The use case has no accountable business owner.

Seven executive decisions

1. **Business relevance:** Is the problem strategically and financially important?
2. **Quantum fit:** Does the problem structure suit optimisation, simulation, sampling or related methods?
3. **Classical baseline:** What is the best current solution?
4. **Readiness:** Are data, talent, architecture and governance sufficient?
5. **Commercial value:** Do risk-adjusted benefits justify total investment?
6. **Security:** What must be done about post-quantum cryptography now?
7. **Stage gate:** What evidence is required to continue, revise, pause or stop?

What quantum computing is—and is not

Classical computers represent information using bits. Quantum computers use qubits and exploit quantum phenomena including superposition, entanglement and interference. These properties enable different algorithmic approaches; they do not make every calculation faster.

Gate-based quantum

Quantum circuits apply gates to qubits. Long-term potential depends on improving scale, fidelity and error correction.

Quantum annealing

A specialised approach primarily associated with optimisation problems.

Hybrid computing

Classical systems orchestrate workflows while quantum processing is applied to selected sub-problems.

Terminology executives should use carefully

Term	Practical meaning	Decision implication
Quantum utility	A useful result in a constrained real-world context.	Useful does not automatically mean commercially superior.
Quantum advantage	A material improvement over the best known classical approach.	The comparator and metric must be explicit.
NISQ	Noisy intermediate-scale quantum hardware.	Experiments require realistic noise, cost and scale assumptions.
Logical qubit	An error-corrected qubit built from multiple physical qubits.	Physical-qubit counts alone can mislead business planning.
Quantum-inspired	Classical algorithms influenced by quantum ideas.	May create near-term value without quantum hardware.
PQC	Post-quantum cryptography designed to resist quantum attacks.	Security migration can begin independently of use-case investment.

Executive rule: fund validated business value and quantum-safe resilience—not qubit headlines.

DECISION PRINCIPLE

Classical first, quantum where justified

A credible quantum business case begins by proving the limitation of the best available non-quantum solution.

Compare four solution paths

1. **Current process**
   Manual, heuristic or existing production method.
2. **Best classical method**
   Optimisation, simulation, AI, HPC, GPUs or specialist software.
3. **Quantum-inspired or hybrid**
   Near-term improvements using classical and emerging techniques.
4. **Quantum method**
   Gate-based, annealing or future fault-tolerant approach.

Measure the same outcomes

- Accuracy or solution quality
- Processing time and throughput
- Infrastructure and energy cost
- Reliability and repeatability
- Integration and operating effort
- Security, privacy and compliance

Example comparison scorecard

Criterion	Weight	Classical	Hybrid	Quantum
Business outcome improvement	30%	Baseline	Evidence required	Evidence required
Time to value	20%	Known	Near term	Uncertain by use case
Total cost	20%	Known	Moderate	Experiment dependent
Operational fit	15%	High	Medium	Low to medium
Strategic option value	15%	Low	Medium	Potentially high

A quantum experiment is successful when it improves evidence and decisions—even if the final decision is to continue with a classical solution.

Start with the business problem

Do not begin with hardware. Begin with a costly, slow, risky or strategically important decision.

Business questions

- What decision or process are we trying to improve?
- Who owns the outcome and budget?
- What is the present cost, loss, delay or risk?
- What improvement would be material?
- Would the business adopt the result?

Computational questions

- What makes the problem difficult?
- How does complexity grow with scale?
- Is the problem optimisation, simulation, sampling or learning?
- Can it be encoded efficiently?
- What is the best classical benchmark?

Quantum-fit indicators

Optimisation

Many interacting choices, constraints and combinatorial possibilities.

Simulation

Molecules, materials, physical systems or complex dynamics.

Sampling

Probability distributions that are difficult to reproduce classically.

High repetition

The problem is solved frequently enough for small gains to compound.

Material value

Even modest improvement produces meaningful cash, risk or resilience value.

Evidence access

Data, experts and baselines exist to validate the result.

Automatic warning signs

Red: no business owner, no KPI, no data and no classical baseline.

Amber: attractive problem, but adoption, encoding or evidence is uncertain.

Green: material value, suitable structure, measurable baseline and accountable owner.

INDUSTRY OPPORTUNITY MAP

Make the business case sector-specific

Industry	Customer problem	Potential approach	Measures
Financial services	Portfolio, risk, fraud and liquidity decisions	Optimisation, sampling	Risk-adjusted return, loss avoided, latency
Pharmaceuticals	Drug and molecular discovery	Simulation, optimisation	Time to candidate, hit rate, research cost
Manufacturing	Scheduling, materials and maintenance	Optimisation, simulation	Throughput, downtime, yield, scrap
Automotive and aerospace	Batteries, engineering and routing	Simulation, optimisation	Range, weight, design time, utilisation
Energy and utilities	Grid balancing, trading and asset planning	Optimisation, simulation	Losses, congestion, uptime, margin
Telecom and logistics	Network design, fleets and capacity	Graph and route optimisation	Service level, miles, latency, utilisation
Public sector and defence	Mission logistics, planning and sensing	Optimisation, sensing	Readiness, response time, resilience
Retail and consumer	Pricing, assortment and supply chain	Optimisation, learning	Margin, availability, waste, conversion

Security is universal.

Long-lived financial, health, intellectual-property, infrastructure and sovereign data may require quantum-safe migration even if no quantum-computing use case is approved.

Value is local.

A use case becomes investable only when sector economics, regulation, data sensitivity and operating reality are included.

Translate technical possibility into business value

Revenue

New products, improved pricing, faster discovery, better customer decisions.

Cost

Better routing, scheduling, allocation, simulation and resource utilisation.

Risk

Fraud, resilience, quantum-safe security, compliance and operational exposure.

Speed

Shorter planning, research, design, optimisation and decision cycles.

Quality

Better solutions, more accurate simulation and improved service outcomes.

Option value

Talent, partnerships, IP and readiness for future technical progress.

Benefit statement template

If [solution] improves [business measure] by [range], across [volume], the gross annual benefit is [value].

Risk-adjust the claim

Expected benefit = gross benefit × technical-success probability × adoption probability

Benefits should be separated into cashable savings, revenue, risk reduction and strategic option value. This prevents optimistic, non-cash benefits from being treated as guaranteed financial returns.

> **Cost of delay:** also model the value lost if the organisation waits—such as avoidable security exposure, missed capability development or delayed product learning.

Calculate the full cost of readiness

Quantum platform access is only one component of the investment.

Cost category	Typical contents
Problem and research	Discovery, formulation, algorithms and domain expertise
Data and classical compute	Preparation, HPC, cloud, GPUs and benchmark development
Quantum access	QPU usage, simulators, tooling and vendor services
People and partners	Talent, universities, consultants and ecosystem relationships
Integration	APIs, orchestration, observability and fallback routes
Trust and compliance	Security, privacy, assurance, audit and legal review
Adoption	Process change, training, productisation and operations

Total investment

One-time build cost

+ recurring operating cost

+ adoption and change cost

+ risk contingency

= complete business case

Avoid false precision.

Use ranges and scenario bands. Technical progress, adoption and vendor pricing remain uncertain.

Minimum financial outputs

ROI

Net benefit divided by investment.

B/C

Benefit-to-cost ratio.

NPV

Time-adjusted value.

Payback

Time to recover investment.

Make assumptions visible and challengeable

The example below illustrates an 18-month readiness programme. It is not a forecast or guarantee. Every number must be replaced with customer data.

CONSERVATIVE

US$3.0M

Risk-adjusted benefit

2.0× benefit/cost
100% net ROI

12–18 month payback

BASE CASE

US$6.0M

Risk-adjusted benefit

4.0× benefit/cost
300% net ROI

9–12 month payback

UPSIDE

US$9.0M

Risk-adjusted benefit

6.0× benefit/cost
500% net ROI

6–9 month payback

Illustrative base-case benefits

Value lever	Benefit	Evidence required
Avoid low-value pilots	US$2.2M	Current project and vendor spend; duplication rate
Accelerate priority opportunities	US$1.6M	Cycle-time baseline; adoption probability
Reduce quantum-security exposure	US$1.4M	Crypto inventory; data lifetime; migration risk
Build reusable capability	US$0.8M	Talent, data, API and governance reuse

Net ROI = (risk-adjusted benefit − US$1.5M investment) ÷ US$1.5M

Ask: "Which assumption feels least credible?" Lower it, recalculate the case and agree the evidence required before the next investment.

Convert evidence into governed decisions

1. **Strategic thesis** — Define market relevance, disruption and ambition.
2. **Problem formulation** — Translate the business problem into a computational form.
3. **Data and encoding** — Assess quality, access, sovereignty and representation.
4. **Algorithm and hardware** — Compare classical, inspired, hybrid and QPU approaches.
5. **Advantage validation** — Test quality, speed, cost, energy and confidence.
6. **Hybrid integration** — Design APIs, orchestration, fallback and observability.
7. **Trust and security** — Address PQC, privacy, safety, compliance and audit.
8. **Operating model** — Establish talent, partners, ownership and funding gates.
9. **Commercialisation** — Define product, pricing, adoption and ecosystem roles.
10. **Scale and learn** — Track KPIs and renew the opportunity portfolio.

Cross-cutting decision lenses

Customer value · Revenue and cost · Risk and resilience · Talent and change · Data sovereignty · Responsible innovation

Evidence gate: every stage must produce a decision—continue, revise, pause or stop.

READINESS SCORING

A transparent assessment model

Score each dimension from 0 to 5. Weighting should reflect the organisation's strategy and risk profile.

Dimension	Weight	Key question
Strategic relevance	15%	Does the opportunity support a material business priority?
Problem fit	20%	Is the problem structure plausibly suitable for quantum methods?
Commercial value	20%	Can value be measured and risk-adjusted?
Data readiness	10%	Is suitable, governed data available?
Technology readiness	10%	Are tools, baselines and access sufficient?
Talent and ecosystem	10%	Can the organisation assemble the required capability?
Integration and operations	5%	Can the result fit into real workflows?
Governance and security	10%	Are risk, compliance, PQC and ownership addressed?

Readiness score = Σ (dimension score ÷ 5 × dimension weight)

0–39: Foundation first

Resolve business, data, ownership or security constraints.

40–69: Validate selectively

Run tightly scoped discovery or proof activity.

70–100: Proceed with gates

Advance the best use cases with explicit evidence criteria.

Score quality matters more than score precision

Every score should include evidence, confidence and an accountable owner. Unsupported high scores create false readiness.

STAGE-GATE GOVERNANCE

Fund evidence, not open-ended experimentation

Gate	Decision question	Required evidence
1. Business value	Is the problem worth solving?	Owner, KPI, baseline, materiality
2. Computational need	Is computation the real constraint?	Process and bottleneck analysis
3. Quantum fit	Does the structure suit quantum methods?	Problem formulation and expert review
4. Data readiness	Can the problem be tested responsibly?	Data access, quality and sovereignty
5. Comparative evidence	Does it improve on the classical baseline?	Repeatable benchmark results
6. Commercial case	Do benefits justify full cost and risk?	Scenario model and confidence factors
7. Scale readiness	Can it be integrated, governed and adopted?	Architecture, controls, owners and KPIs

Continue

Evidence meets the agreed threshold.

Revise

Change the problem, method or scope.

Pause

Wait for technology, data or ownership.

Stop

The use case is not commercially justified.

Stopping can be a valuable outcome. It protects capital, strengthens the portfolio and releases scarce talent for higher-value opportunities.

Do not wait for a quantum use case to begin PQC readiness

NIST approved FIPS 203, FIPS 204 and FIPS 205 in August 2024. These standards address quantum-resistant key establishment and digital signatures. Migration still requires inventory, integration, testing and operational change.

Why action starts now

Long-lived sensitive data may be collected today and targeted for decryption later.

Cryptography is embedded across applications, devices, certificates, protocols and suppliers.

Migration across a large estate can take years.

Five-step security workstream

1. Identify long-lived sensitive information.
2. Inventory cryptographic assets and dependencies.
3. Prioritise systems by exposure and migration difficulty.
4. Test approved PQC and hybrid approaches.
5. Build crypto agility into architecture and procurement.

Governance ownership

Owner	Responsibility
Board / risk committee	Risk appetite, material exposure and oversight
CISO	Inventory, policy, architecture and migration programme
CIO / CTO	Platform, application and supplier integration
Legal / privacy	Data lifetime, contractual and regulatory obligations
Procurement	Crypto-agility and PQC requirements for suppliers

Build capability without creating a science project

Minimum core team

Executive sponsor — strategic priority and funding

Business owner — KPI and adoption

Domain expert — problem and evidence

Quantum specialist — formulation and methods

Classical specialist — baseline and benchmarking

Data / platform lead — data and integration

Security / risk lead — PQC, privacy and assurance

Portfolio governance

One opportunity register

Common scoring and stage gates

Separate security and use-case workstreams

Vendor-neutral benchmarks

Quarterly continue / revise / stop reviews

Reusable data, APIs and evidence

Partner without becoming dependent

Use universities, vendors, cloud providers and consultants for specialist capability, but retain ownership of the business problem, data, benchmark, commercial model and decision criteria.

> **Procurement principle:** buy learning and evidence in stages. Avoid long commitments before problem fit and comparative value are established.

Move from interest to an evidence-based portfolio

DAYS 1–30

Align

- Name sponsor and owners.
- Define strategic themes.
- Launch PQC inventory.
- Collect 10–20 candidate problems.

DAYS 31–60

Assess

- Score quantum fit and value.
- Establish classical baselines.
- Identify data and security gaps.
- Select 3–5 opportunities.

DAYS 61–90

Decide

- Build scenario business cases.
- Approve evidence gates.
- Start one or two proofs.
- Publish the readiness roadmap.

Board-ready outputs by day 90

Quantum opportunity portfolio

Ranked use cases with owners, KPIs, fit, timing and evidence gaps.

Readiness score

Transparent assessment across business, data, technology, talent and governance.

Quantum-safe risk view

Critical data, cryptographic dependencies and migration priorities.

Investment roadmap

Stage-gated funding, partner strategy and 12–24 month actions.

> **The first goal is not to run a quantum algorithm. It is to improve the quality of the organisation’s next decision.**

Twelve questions every organisation should answer

1. Which business problems are becoming too complex, slow, costly or risky?
2. What is the measurable cost of the current limitation?
3. Who owns the outcome and would adopt a better answer?
4. What is the best classical method available today?
5. Does the problem structure plausibly fit optimisation, simulation, sampling or learning?
6. Is the required data available, governed and suitable for encoding?
7. What improvement would be commercially material?
8. What is the full investment, including people, data, integration and change?
9. Which assumptions have the weakest evidence?
10. What evidence is required before the next funding decision?
11. Which long-lived data and systems require PQC migration?
12. What would make us continue, revise, pause or stop?

Use QuantumReadyCheck

Convert these questions into a structured readiness score, industry opportunity map and practical roadmap.

https://quantumreadycheck.com/

CONCLUSION

Prepare for value, not for fashion

The most quantum-ready organisations will not necessarily spend the most. They will make the best decisions under uncertainty.

They will identify commercially important problems, maintain strong classical baselines, quantify benefits honestly, separate use-case investment from security migration, build reusable capability and stop weak ideas early. They will understand that readiness is a portfolio discipline—not a single proof of concept.

> **What evidence would justify our next quantum investment?**

Created and authorised by

Jami Kiran

Trusted Global Technology Advisor

AI • Data • Cybersecurity • Cloud • Quantum
Global transformation leadership across 30+ countries
7 AI patents • Board and executive advisory

QuantumReadyCheck

A privacy-conscious executive readiness experience for assessing business fit, industry opportunity, commercial value, governance and roadmap priorities.

quantumreadycheck.com

Important: this paper provides a decision framework, not financial, legal, cybersecurity or investment advice. Quantum capabilities, standards, pricing and performance continue to evolve. Validate decisions with qualified specialists and current evidence.

GLOSSARY

Selected terminology

Term	Definition
Qubit	The basic unit of quantum information.
Superposition	A quantum state represented as a combination of basis states.
Entanglement	Quantum correlation in which a system must be described jointly.
Interference	The reinforcement or cancellation of quantum probability amplitudes.
QPU	Quantum processing unit.
NISQ	Noisy intermediate-scale quantum computing.
Error correction	Methods for protecting logical quantum information from physical errors.
Hybrid workflow	A workflow combining classical and quantum computation.
Quantum-inspired	A classical method influenced by concepts or mathematics associated with quantum approaches.
Quantum utility	A useful quantum result in a defined context.
Quantum advantage	A material improvement over an explicitly defined classical comparator.
PQC	Cryptographic methods designed to resist attacks by quantum computers.
Crypto agility	The ability to identify and change cryptographic algorithms and dependencies efficiently.
Harvest now, decrypt later	The risk that encrypted data is collected today for attempted decryption in the future.

REFERENCES

Selected authoritative sources

1. National Institute of Standards and Technology (NIST), "Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography," 13 August 2024. https://www.nist.gov/news-events/news/2024/08/announcing-approval-three-federal-information-processing-standards-fips
2. NIST Computer Security Resource Center, "Post-Quantum Cryptography Project." https://csrc.nist.gov/Projects/post-quantum-cryptography
3. NIST National Cybersecurity Center of Excellence, "Migration to Post-Quantum Cryptography — Frequently Asked Questions." https://pages.nist.gov/nccoe-migration-post-quantum-cryptography/FAQ/
4. NIST, FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard; FIPS 204, Module-Lattice-Based Digital Signature Standard; FIPS 205, Stateless Hash-Based Digital Signature Standard.
5. European Union Agency for Cybersecurity (ENISA), "Post-Quantum Cryptography — Integration Study," 18 October 2022. https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study
6. IBM Quantum Learning, "Quantum Computing Fundamentals." https://quantum.cloud.ibm.com/learning/en/courses/quantum-business-foundations/quantum-computing-fundamentals
7. IBM Quantum Learning, "Quantum Bits, Gates, and Circuits." https://quantum.cloud.ibm.com/learning/en/courses/utility-scale-quantum-computing/bits-gates-and-circuits
8. United States National Quantum Initiative, official programme information and advisory materials. https://www.quantum.gov/

Method note

The commercial models and scenarios in this paper are illustrative. They are designed to support structured analysis and should not be interpreted as evidence of guaranteed quantum advantage or financial return. Current vendor claims, technical performance and standards should be revalidated at the time of each decision.

Suggested citation

Kiran, J. (2026). *From Quantum Curiosity to Commercial Value: An Executive Framework for Quantum Readiness, Business Fit, Investment and ROI.* QuantumReadyCheck.com.