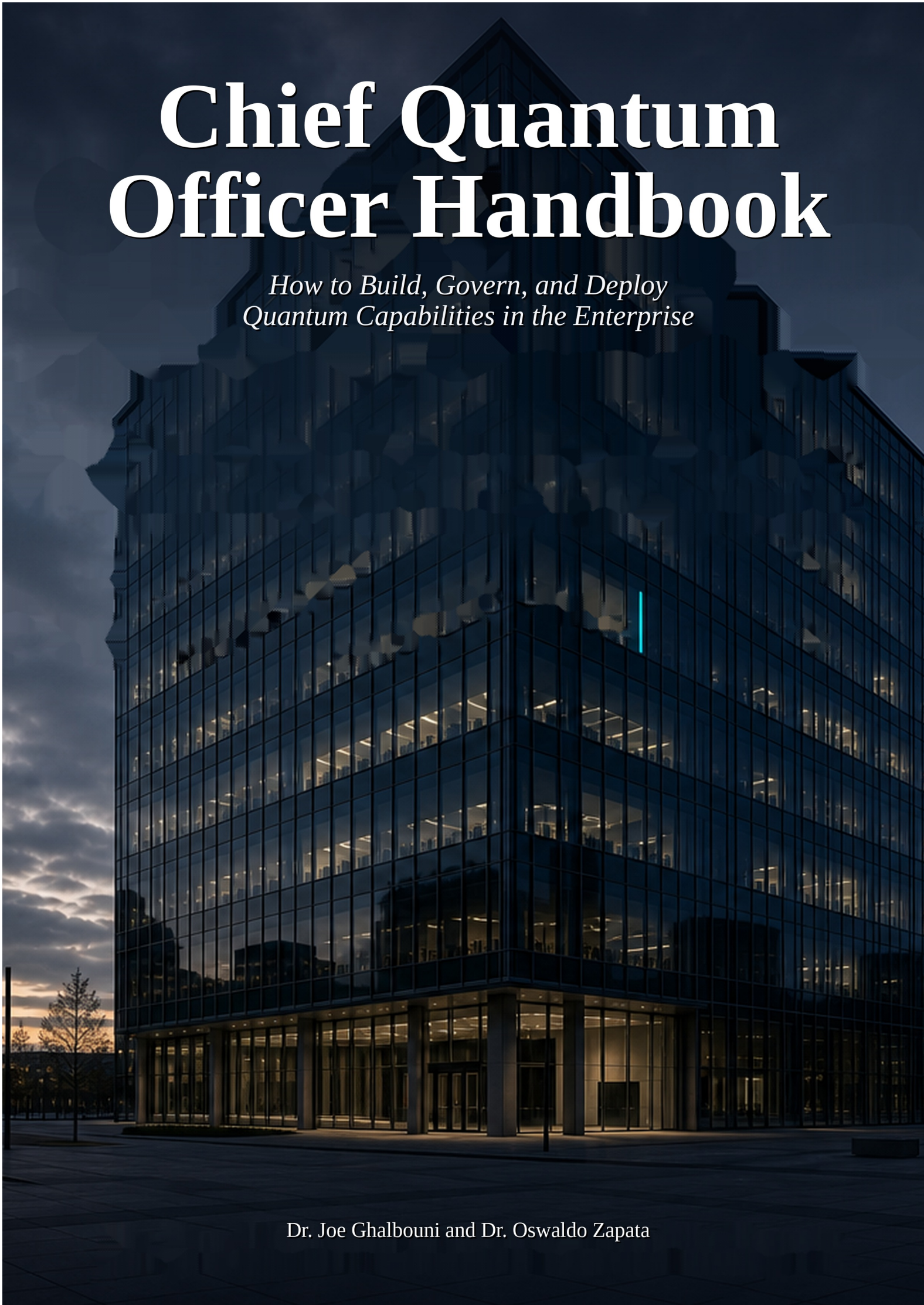
Chief Quantum Officer Handbook

How to Build, Govern, and Deploy Quantum Capabilities in the Enterprise



Dr. Joe Ghalbouni and Dr. Oswaldo Zapata

Chief Quantum Officer Handbook

How to Build, Govern, and Deploy Quantum Capabilities in the Enterprise

Dr. Joe Ghalbouni and Dr. Oswaldo Zapata

August 2026

Contents

Preface

This handbook is for people taking or seeking the Chief Quantum Officer (CQO) role — the executive accountable for making the firm's quantum transition happen.

It is a working book, not a textbook. It does not teach the algorithms, and it does not sell a vendor. The through-line is what this reality requires the CQO to understand, decide, communicate, monitor, or do: a cryptographic replacement that has already started; a compute class the firm must be ready to absorb only when it beats the best classical alternative on a problem the business owns; a filter that decides what the board is allowed to hear.

The instruments — inventories, questionnaires, decision cards, calendars, scorecards — are how the office runs. Use them. Change the weights in writing. Do not wait for a classroom.

What this book is not: a physics course, a market map, a catalogue of devices, or a promise that quantum computing is about to replace the classical stack. Compute advantage remains an evidence question. Cryptographic replacement is already a program. Hold both.

This book was written by Dr. Joe Ghalbouni and Dr. Oswaldo Zapata.

Introduction

The CQO is not a quantum evangelist. The CQO is an enterprise transformation officer responsible for turning quantum computing, post-quantum cryptography (PQC), quantum-safe infrastructure, and selected quantum communication technologies into a disciplined business and security roadmap.

The role exists because three pressures sit on the same desk: a compute class the firm must be ready to absorb, a cryptographic clock that has already started, and a vendor circuit that will fill any vacuum. Chapter 1 is the diagnostic. What follows is what success looks like on the calendar.

Success is operational, not theatrical.

Twelve months. The office can point at a signed mandate, a quantum council that records fund / explore / kill / archive, a scored use-case portfolio, a cryptographic inventory in motion with the Chief Information Security Officer (CISO), a PQC program charter, a vendor panel with exit terms, a working envelope of honest proofs of concept sized to real owners, and a board pack built from the decision log. PQC is current program work. Compute novelty does not outrun it.

Twenty-four months. The same instruments are still in use. Waves that were chartered have coverage the council can read. Compute rows that earned Scale have a receiving team, a fallback, and a cost model — or they are not called production. Contracts carry algorithm, certificate, and protocol agility. Residual risk is dated. A speaking calendar that outruns the inventory is still a failure.

Thirty-six months. Cryptographic replacement is still a multi-year program — that is the point of starting it in year one. The lasting target is the ability to change cryptography again without another decade-long invention, and an absorption layer (data, workflow, skills, egress rule) so that if a quantum processor beats

the classical stack on a problem the business owns, the firm can run the comparison without a scramble. The board hears residual risk, not a belief story.

Twelve months here is a picture of the office working, not a substitute for the hundred-day calendar and the twelve-month instruments in Chapters 22–23.

Hold both clocks. Evaluate before you adopt. Secure before you scale. Let the log — not the tour — speak.

Part I — The Role of the Chief Quantum Officer

You already have the chair. The office exists, or it is about to — either way, the work on the desk is the same. The firm's quantum transition runs on two clocks: a multi-year cryptographic replacement that has already started, and a compute capability the firm must be ready to absorb when — and only when — it beats the best classical alternative on a problem the business owns. Between those clocks sits a third piece of work that never appears on a vendor slide: the hype filter that decides what gets funded, what gets killed, and what the board is allowed to hear.

Strategy, gates, security coordination with the CISO, and the decision log are yours. Implementation stays with the teams that already run systems. Part I sets the office and the mandate so the first sixty days can turn them into a portfolio and a filter.

---

1. Why the CQO's desk looks like this

Three pressures create the job, and none of them is a purchase order. Name someone who will absorb a compute class when it is real, keep the cryptographic clock funded, and kill work that cannot pass a written filter. You are that someone. The chapter is a diagnostic of what is already on the desk — not a memo that invents the role.

Force 1 — A future compute capability the firm must be ready to absorb

Some problem classes remain hard after the firm has spent seriously on classical high-performance computing and graphics processing units (GPUs). Exact combinatorial search hits a wall on size and constraint density. High-accuracy simulation of molecules, materials, and certain energy systems remains expensive in time and energy. Those constraints are real. Classical HPC remains the production estate.

Quantum processors are a candidate for a few of those hard classes — where classical methods are already showing diminishing returns on quality, time, or energy cost. For everything else, the firm will keep using central processing units (CPUs), GPUs, and well-tuned solvers. The CQO's job is not a capital request for a dilution refrigerator. It is readiness.

Ready to absorb means four things you can point at: the data can move or a faithful proxy exists; a hybrid job can run without a vendor portal; someone on payroll can run the firm's own solver as the baseline; and the security architect has already said what may leave the building.

Write the short list this month: problem classes where the current HPC or GPU spend is already flattening. Define "ready to absorb" as data, workflow, skills, and the egress rule — not as a refrigerator. Tell the board you are buying the right to compare, not a machine.

Force 2 — Immediate cybersecurity and post-quantum migration pressure

A sufficiently capable fault-tolerant quantum computer would break the public-key cryptography that still protects most enterprise traffic, identity, software updates, and stored archives. That is the premise. Do not wait for a classroom explanation of the algorithms. Plan as if those algorithms can run.

Cryptographic replacement takes years. Certificates, public-key infrastructure (PKI), Transport Layer Security (TLS), virtual private network (VPN), Secure Shell (SSH), code signing, hardware security modules, embedded devices, and third-party products do not move on a quarterly cycle. Harvest-now-decrypt-later is the planning problem: an adversary can record ciphertext today and decrypt it when the capability arrives. Any record whose confidentiality must outlast that horizon is already in scope — patient data, trade secrets, long-dated contracts, state secrets, industrial control configurations, insurance archives.

Standards and dated national guidance now exist. The National Institute of Standards and Technology (NIST) has published Federal Information Processing Standards (FIPS) 203 (ML-KEM) for key encapsulation and FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA) for digital signatures. France's national cybersecurity authority (ANSSI) states that it aims to impose post-quantum cryptography obligations for products entering its qualification process from 2027, and that it will not be reasonable to purchase products that do not integrate PQC after 2030. In June 2025 the Network and Information Security (NIS) Cooperation Group, with Commission support, published a coordinated PQC implementation roadmap. The U.S. National Security Agency has published Commercial National Security Algorithm suite (CNSA) 2.0 transition guidance for national security systems.

The CQO does not take operational security away from the CISO. The CQO makes this a dated, funded, board-visible program instead of a ticket in a security backlog.

Walk into the CISO's inventory meeting with a confidentiality-lifetime sort.

Force 3 — Separate useful experimentation from vendor hype

Vendors, labs, and internal enthusiasts will solicit capital, attention, and scarce engineering time. Some of that solicitation is serious. A large share is modality lock-in, toy-graph slides, and "quantum machine learning" with no classical baseline. The CQO is the person who kills that work early and funds the rest under a written filter.

The filter comes before the workshop. If the firm starts with a vendor tour and writes the criteria afterwards, the criteria will fit the tour.

No vendor workshop until Chapter 7 is on paper.

Weight the buckets for this firm

Finance has portfolio construction, execution, risk, and a loud vendor circuit. The same four questions — can we formulate it, is there a classical baseline, is quantum relevant, who owns the outcome — travel across sectors. Placement of candidates into the four use-case buckets belongs in Chapter 6. Weight the four buckets for this firm this month; do not import a finance template.

A short note for the CEO

If the mandate letter is not yet signed, that is the CEO's first move, not yours as a creation myth for this chapter. Name the CQO, put the mandate on one or two pages, and give the office a reporting line, a council, and a budget envelope before the firm signs a lab lease, a multi-year cloud commit, or a "quantum center"

announcement. Until that signature exists, vendor conversations land wherever they are convenient, PQC work competes with the rest of the security backlog, and no one is accountable for the kill decisions. Chapter 2 carries the letter's contents.

CQO actions

- Assess which of the three forces is already costing the firm time, risk, or money, and write that split in the firm's own language.
- Deliver the short list of diminishing-return problem classes and the four-point "ready to absorb" definition to the first council.
- Walk into the CISO's inventory meeting with a confidentiality-lifetime sort and a first-wave candidate list.
- Put the Chapter 7 filter on paper before any vendor workshop.
- Brief the board that the firm is buying the right to compare, and that PQC is a multi-year replacement program with a compliance clock.

---

2. The CQO mandate

The CQO owns the enterprise quantum strategy. The CQO does not need to own every implementation team. Security engineering, data science, HPC operations, procurement, and vendor engineers stay where they sit. The CQO sets the portfolio, the gates, the vendor bar, and the story the board hears.

If you cannot read a paper's limitation section, vendors will own you. If you can only read papers, you will fund science the firm cannot run. Hire for both, or staff the missing side in the core office in month one. The CQO is accountable for making the transition happen — not for being the organization's resident quantum expert.

Portfolio: what the CQO owns, what the CQO coordinates

The mandate is easy to collapse into a job the firm already understands. Hold the owns / coordinates split in writing before the first vendor conversation.

Domain	CQO owns	CQO coordinates	Others execute
Technology scouting	Watchlist, kill/keep criteria, briefing cadence	Research partners, standards bodies, selected labs	Applied scientists read the papers and run the tests
Use-case portfolio	Taxonomy, scoring, fund / explore / kill decisions	Business-unit discovery	Domain teams formulate problems and supply data
Security / PQC	Quantum-threat strategy, inventory sponsorship, board translation, migration roadmap with CISO	Cryptographic discovery, vendor crypto questionnaires	CISO and security engineering run operations and the migration build
Vendor evaluation and risk	Evaluation framework, panel, exit terms, evidence standard	Procurement, legal, information security	Procurement contracts; legal owns paper; security owns control design
Internal education	Three-track plan (executive, technical, business-unit)	Human Resources (HR) / Learning and Development (L&D), communications	Practitioners teach the workshops
Budget design	Envelope, gates, line-item discipline		Finance runs the ledger

Domain	CQO owns	CQO coordinates	Others execute
		Chief Financial Officer (CFO), BU controllers	
Executive reporting	Decision log, readiness map, risk register	Corporate secretary, risk committee	—

How the role sits next to neighboring jobs

Neighboring job	What the CQO does	What the other role owns
Researcher / chief scientist	Validates claims, sets the scientific bar, reads limitations, refuses unexplained advantage	Applied scientists and academic partners invent, implement, and publish
Innovation / emerging-tech manager	Scores deliverability, compliance, and commercial utility; applies a kill rule	Innovation office may scout broadly; it does not hold the PQC clock or the production gate
CISO	Sponsors quantum-threat strategy, PQC inventory, and board-level translation	CISO keeps operational cybersecurity, incident response, and the security build
Communications / “quantum marketing”	Speaks when asked, and only with evidence already in the decision log	Communications owns positioning; visibility is secondary to the mandate

A CQO who cannot validate a technical claim will be captured by vendors. A CQO who only validates technical claims will fund science the firm cannot use. Hold both.

RACI — owns, decides, advises, is informed

Use this table in the mandate letter. Adjust names; do not adjust the idea that one person decides.

Decision	CQO	Chief Technology Officer (CTO) / Chief Information Officer (CIO)	CISO	CFO	Business-unit head	Legal / risk	Board / CEO
Quantum strategy and annual roadmap	A / R	C	C	C	C	I	I (approves envelope)
Use-case fund / explore / kill	A / R	C	I	C	C (owner signs)	I	I
PQC inventory scope and wave plan	A (strategy)	C	A / R (operations)	I	I	C	I
Vendor panel and major contract	A / R (technical bar)	C	C	C	I	C	I above threshold
Proof of Concept (PoC) start and end-decision	A / R	C	C if data leaves	I	A (outcome)	I	I
Production go / no-go	A (gate)	C	C (security review)	C (cost)	A / R (owner)	C	I

Decision	CQO	Chief Technology Officer (CTO) / Chief Information Officer (CIO)	CISO	CFO	Business-unit head	Legal / risk	Board / CEO
External claims and press	A (facts)	I	C	I	I	C	A (if public)
Education plan	A / R	C	C	I	C	I	I

R = does the work. A = accountable for the decision. C = consulted. I = informed.

Mandate letter — minimum contents

Require a one- to two-page mandate letter signed by the CEO or equivalent. Do not start on a verbal understanding.

- Purpose: absorb useful quantum compute; complete a dated PQC transition with the CISO; kill theater.
- Authority: single door for quantum vendor intake; authority to halt a PoC that fails the filter; a seat on the relevant risk or technology committee.
- Boundaries: CISO keeps security operations; business units own outcomes; the CQO does not run the data-science department.
- First-year envelope: a number the CFO will recognize, with gates (Chapter 8), not a blank research fund.
- Reporting: monthly council, quarterly executive, annual board.

CQO actions

- Get the mandate letter signed and file the owns / coordinates split with the CISO, CTO or CIO, and CFO.
- Put the RACI table into the first council pack and refuse decisions that have no A.
- Open a single vendor-intake door and route the first conversation through legal.
- Set the first-year portfolio as PQC coordination plus a short compute list.
- Report decisions made, not experiments counted; remeasure after six months what landed in the wrong office.

---

3. Where the CQO sits

Reporting line is a design choice with failure modes. Put the CQO only under the CISO and quantum becomes a cryptography program with a science hobby. Put the CQO only under innovation and PQC loses the compliance clock. Put the CQO inside a standard IT lifecycle and the roadmap is forced into refresh cycles that do not match either cryptographic replacement or hardware uncertainty.

Candidate homes

Home	What works	Reporting risk	What the CQO insists on
CTO office		Compute experiments crowd out PQC	Formal dotted line to the CISO; PQC on every quarterly agenda

Home	What works	Reporting risk	What the CQO insists on
	Technical authority; architecture access; honest hardware skepticism		
CIO office	Integration, identity, data estate, vendor management	Quantum treated as another platform refresh	Independent roadmap; not a line item in the enterprise resource planning (ERP) upgrade
CISO office	PQC gets funded and staffed	Compute, simulation, and optimization disappear; board hears only threat	Dual mandate in writing; a compute portfolio with business owners
Chief Strategy Officer / corporate strategy	Peer seat; multi-year capital; mergers and acquisitions (M&A) and sovereignty questions	Weak grip on architecture and security operations	Dotted lines to CTO/CIO and CISO; an architect in the core office
Innovation / emerging tech	Permission to explore	No kill discipline, no production path, no CISO	Value filter as a standing rule; security architect in the room
Transformation office	Cross-functional delivery muscle	Program-office theater; slides instead of gates	Named business owners and a decision log

Recommendation — seat and dotted line first

Report close to the CTO, the CIO, or the Chief Strategy Officer. Install a formal dotted line to the CISO. The CQO needs a peer seat: present when technology, risk, and capital are decided, not summoned after the vendor has already been chosen. That seat is earned by decisions, not by title inflation.

Keep the quantum compute roadmap off the standard IT lifecycle so it is not forced into a three-year hardware refresh.

PQC visibility — second

Make PQC visible to the board as part of the CQO's strategic umbrella, executed with the CISO's organization. Keep quantum-safety under that umbrella so it is not reduced to a control family in last year's security plan.

Quantum Key Distribution (QKD) and other quantum-communication work sit in scope only if Chapter 6 Bucket D says so. Do not fight QKD inside the org-chart conversation.

Alliances the CQO must build

Technical peers are necessary and insufficient.

- CFO: envelope, gates, cost-to-serve of any later production path, and the habit of killing work that cannot state an ask.
- Business-unit heads: they own outcomes. A use case without a named owner is research, and should be labeled that way.
- Legal and compliance: export controls, data jurisdiction, publication rights, intellectual property (IP) in joint work, regulated-sector constraints (finance, pharma, defense, telecom, public sector).

- Procurement: a quantum contract is a deep-tech contract. Exit, reproducibility, data egress, and modality portability belong in the paper, not in a slide appendix.
- Risk: harvest-now-decrypt-later and vendor concentration belong on the enterprise risk register, not in a lab notebook.

If the first pain is X

The table below is the instrument for choosing a home when the firm's first pain is already named. Read it before you negotiate the chart.

If the firm's first pain is…	The reporting risk is…	The CQO insists on…
Regulator or customer asking about PQC dates	Quantum is parked entirely under security and never builds compute readiness	Dotted line to CISO *and* a compute portfolio with two named business owners
A CEO who wants a "quantum lab" after a site visit	Innovation theater and a premature hardware buy	Reporting to CTO/CIO or strategy; year-one policy of no on-prem quantum processing unit (QPU) unless the council records an exception
HPC / simulation teams asking for quantum access	A science project with no security or vendor governance	Architecture access plus CISO on data egress and keys
A business unit with a painful optimization stack	A single-use-case office that ignores PQC	The use case can lead; the mandate still includes the security clock
Board anxiety after a competitor announcement	Communications-led program	Peer seat on the technology or risk committee; no press without a decision log
Sovereign or defense procurement pressure	CQO buried in compliance with no path to experimentation	Strategy or CTO home; legal and export in the council from day one

If the chart does not show a dated PQC program, a capped research option, and a production gate that can say no, the firm will treat quantum as a hobby. Fix the chart before you fix the slides.

CQO actions

- Decide the reporting line against the candidate-homes table and write the CISO dotted line into the mandate.
- Take a peer seat on the technology or risk committee, or escalate the absence of one.
- Engage the CFO, one BU head, and legal in the first thirty days.
- Document the first-pain / reporting-risk pair the firm actually has, and the year-one no-on-prem policy unless the council records an exception.
- Escalate if the CQO is being used as a spokesperson without budget or gates.

---

4. The CQO operating model

No Chief Quantum Officer operates alone. The technical surface, the regulatory surface, and the vendor surface are too wide. Build three tiers and write down what each tier decides, how often it meets, and what it produces. The mandate without a cadence is a title.

Tier 1 — Core CQO Office

A small permanent staff. Hire for judgment and delivery, not for a publication list.

Seat	Primary job	The CQO uses this seat to…
Senior quantum lead	Technical bar on algorithms, modalities, and papers	Validate claims; design honest tests; refuse unexplained advantage
Technical program manager	Cadence, dependencies, decision log, budget hygiene	Keep explore / PoC / kill dates real
Security architect	Cryptographic inventory design, data-egress rules, vendor security model	Bind every experiment to a security constraint
Applied scientist or engineer	Hands-on hybrid workflows, simulators, benchmark harness	Produce evidence the council can use
Enterprise architecture (access, not always a full-time seat)	Identity, data platforms, HPC, integration paths	Stop the lab from becoming an island

In a smaller firm, two people may cover these seats. Do not drop the security architect or the program manager in the first year. A lone scientist with a cloud account is not an office.

The core office decides: what enters the scoring pipeline, what is ready for the council, which vendor conversations are opened, which internal tests start. It produces: the readiness map, the portfolio table, the decision log, draft business cases, vendor evaluations, and the board pack.

Cadence: weekly working session; daily contact during a live PoC or a migration wave.

Tier 2 — Extended Quantum Council

The council is where the firm decides. The CQO chairs. Members:

- CQO
- CTO or CIO
- CISO
- Head of data science or quantitative research
- Legal
- Procurement
- Risk
- Compliance
- Business-unit leads for active use cases
- Selected external advisers (time-boxed, under non-disclosure agreement (NDA), no vendor with a live bid)

The council decides: fund / explore / kill / archive; PQC wave scope; vendor panel membership; production go / no-go recommendations; what the board is told. It produces: signed gates, an updated portfolio, a risk register, and a quarterly narrative.

Cadence: monthly, with a short extraordinary session when a PoC hits its end-decision or a regulator dates a requirement. The meeting is a decision slot, not a seminar, if the core office has done the work. A half-day workshop once a quarter is not a substitute for a monthly decision meeting.

Advisers advise. They do not vote. Vendors present by invitation and leave before the decision.

Tier 3 — Execution squads

Temporary. One squad per funded use case or per security-migration stream. A squad has a business owner, a technical lead from the core office or the BU, a security counterpart when data or cryptography is in play, and named vendor or internal engineers. When the gate is kill or archive, the squad dissolves. When the gate is scale, the work moves into a production owner — often not the people who ran the PoC.

Squads decide day-to-day experiment design inside the key performance indicators (KPIs) the CQO set before start. They produce: the benchmark card (Chapter 12), the PoC write-up, and a recommended end-decision. They do not invent a new success metric after seeing the result.

Cadence and artifacts

Before the first council, the CQO needs a single page that says who meets, what they decide, and what they must leave on the table. That is this instrument.

Body	Meets	Decides	Must produce
Core CQO Office	Weekly	Intake, test design, what goes to council	Readiness map, portfolio, decision log, draft cases, vendor scores
Quantum Council	Monthly	Fund / explore / kill / archive; PQC waves; panel; go / no-go	Signed gates, risk register, quarterly narrative
Execution squad (compute)	Stand-up during the PoC	Tactical experiment choices inside pre-set KPIs	Benchmark card, write-up, recommended decision
Execution squad (PQC / crypto)	Stand-up during a wave	Sequencing inside the wave plan	Inventory coverage, vendor questionnaire results, cutover plan
Board / risk committee	Quarterly or at the firm’s risk cycle	Envelope, appetite, public claims	— (receives the CQO pack)

Working rules

- Single intake: a use case, a vendor, or a research collaboration enters through the core office. Side-door pilots are a governance failure.
- Pre-committed KPIs: the CQO establishes goals and metrics before a PoC starts (Chapter 11).
- Security in the room: if data may leave, if a new software development kit (SDK) is installed, or if a protocol changes, the security architect sees it before procurement.
- Dissolution: squads end. Permanent “quantum teams” without a portfolio are how demos become furniture.

The office and the mandate now exist on paper. The first sixty days turn them into a portfolio and a filter — that is Part II.

CQO actions

- Name the three tiers and the people, including part-time seats, and file who covers the CQO for two weeks.
- Publish the monthly council agenda as decisions, not updates, and open a single intake path.
- Sponsor one PQC squad and at most two compute squads in year one unless the filter says otherwise.

- Put the decision log on a weekly review and escalate the first side-door pilot to the council.
- Ensure every squad has a business owner before it is staffed.

Part II — Building the Quantum Strategy

Strategy here is a sequence of diagnostics, a portfolio, a kill filter, and a one-page business case. The CQO does not open with a vision speech. The CQO opens with evidence the council can score. Part I gave you the office and the mandate; the next chapters turn that authority into a ranked list of what to fund and what to refuse.

---

5. Enterprise quantum readiness and the first 60 days

The first 60 days are a diagnostic. Resist the urge to announce a roadmap, pick a hardware partner, or stand up a branded lab. Walk into the first full council with a Readiness Map, a cryptographic-exposure sketch, a draft use-case list, a vendor inventory, and a short list of decisions the council actually has to take.

Eight workstreams run in parallel. The CQO chairs all eight; specialists collect the facts.

The eight workstreams

1. Business-unit interviews. Sit with the people who own profit and loss (P&L), operations, research and development (R&D), and risk. Ask where classical methods are already expensive, slow, or unstable; where data already exists; and who would own a better answer. Do not lead with quantum. Lead with pain. Record owner, problem class, data location, current method, and political heat.

2. Data availability. For each candidate problem, establish whether the data exists, whether it can be used, and whether it can leave its current security zone. Note volume, cleanliness, refresh rate, rights, and jurisdiction. A beautiful formulation with unreachable data is research.

3. Compute, HPC, and GPU review. Inventory what the firm already runs: solvers, simulation codes, GPU clusters, schedulers, and the teams who operate them. The classical baseline for later chapters lives here. If the firm cannot describe its current stack, it cannot claim a quantum improvement.

4. Cryptographic exposure. Begin the inventory with the CISO: protocols, PKI, certificates, code signing, VPNs, HSMs, long-lived archives, and third-party products that terminate cryptography. Classify data by confidentiality lifetime. Harvest-now-decrypt-later is the sorting key.

5. Vendor dependency. List every quantum, “quantum-inspired,” and PQC conversation already in flight. Note who invited them, what data they have seen, and whether a contract exists. Side-door pilots discovered in week six are a finding, not an inconvenience.

6. Skills. Before opening a hiring campaign, assess adjacent talent: scientific computing, optimization, quantitative research, cryptography engineering, enterprise architecture. Appetite matters as much as credentials. Name who can sit on a squad in 90 days and where the firm must hire or contract.

7. Regulatory exposure. Identify which clocks apply: NIST standards for any U.S. federal or contractor surface; ANSSI qualification and procurement guidance for French government and critical operators; CNSA

2.0 where national-security systems are in scope; sectoral rules in finance, health, telecom, energy, and defense; customer questionnaires already arriving. Date what you can date. Mark what you cannot.

8. Executive appetite. Separate curiosity, fear, and willingness to fund a kill. A CEO who wants a press cycle and a CFO who will only fund gated work are different starting conditions. Write the difference down. It changes the first-year split between PQC and compute.

Algorithmic and data-pipeline viability — checklist

The CQO assigns a named reviewer (applied scientist or quantitative lead) to complete this for every candidate that survives the first interview pass. Without it, Chapter 6 has nothing honest to classify.

- Problem statement fits on one page, with decision variables, constraints, and what "better" means.
- Current classical method is named, including software and, where relevant, hardware.
- Instance size class is known (order of variables, constraints, time horizon).
- Constraint structure is known (linear, integer, nonlinear, stochastic, physics-based).
- Data exists and has an owner; rights and jurisdiction are written down.
- A faithful synthetic proxy can be built if production data cannot move (Chapter 11).
- Pipeline from source system to a solver or simulator is described; hand-built spreadsheets are flagged.
- Pre- and post-processing cost is estimated in people-time and compute-time.
- Privacy, residency, and export constraints are listed before any cloud quantum account is opened.
- A business owner has agreed to look at the result, including a negative result.

If three or more items are unknown after two weeks, the candidate stays at "awareness" and does not consume PoC budget.

Cybersecurity audit — checklist

Jointly owned with the CISO. The CQO sponsors and translates; security engineering collects.

- Inventory started: TLS, VPN, SSH, PKI, certificates, code signing, identity providers, application programming interfaces (APIs), HSMs, email, backup encryption, field devices.
- Long-life data identified: records that must remain confidential past 2030, and systems that cannot be updated easily (embedded, industrial, sovereign).
- Public-key dependencies mapped: where the firm still relies on RSA or elliptic-curve schemes for key establishment or signatures.
- Third-party products listed, with a vendor crypto questionnaire in draft (algorithms supported, hybrid mode, agility, roadmap — dates as the vendor states them, not as a slide implies).
- Crypto-agility assessed: can the firm change algorithms and certificates without a decade-long project?
- Harvest-now-decrypt-later exposure ranked by data shelf life × ease of interception × value to an adversary.
- New quantum-stack components (SDKs, cloud accounts, notebooks) added to the security review queue *before* use.
- Privileged access to any quantum cloud or simulator placed under existing identity and logging standards.
- PQC standards in use as a reference set: NIST FIPS 203 / 204 / 205, and any national guidance that applies.
- Board-visible dates collected (regulator, customer, internal policy) and parked for the council.

Do not declare systems certified for post-quantum cryptography. Require inventory coverage, algorithm agility, and a completed vendor questionnaire. Named national qualification schemes, where they exist, are the CISO's language; the CQO's language is coverage, dates, and residual risk.

Quantum Readiness Map — four ranks

Assign one rank to the enterprise as a whole and, if useful, one rank per domain (compute experimentation, cryptographic migration, skills, governance). Production-ready is rare. Say so.

Rank	Criteria the CQO can actually assign	What the CQO does next
Awareness only	Scattered articles and vendor meetings; no inventory; no named owners; no classical baselines written down; no mandate.	Write the mandate; start interviews and the crypto inventory; block hardware purchases.
Experimenting	One or more tests have run; data and owners are partial; classical baselines are uneven; vendor intake is informal; PQC work may have started in a corner.	Install the council, the filter, and single intake; force a baseline onto every live test; open the inventory if it is not open.
Pilot-ready	Mandate and council exist; portfolio scored; at least one candidate has owner, data path, and classical baseline; security rules for the stack are written; PQC waves sketched.	Fund one or two PoCs under Chapter 11 rules; staff a PQC squad; refuse a third PoC until the first end-decision is real.
Production-ready	A quantum or hybrid method is in an operational path with API stability, security review, fallback, cost monitoring, and a business-owner sign-off — *or* a PQC control is in production on a scoped surface.	Treat as exceptional. Govern it as production (Chapter 13). Do not generalize from one surface to the enterprise.

Most firms that take the role seriously in year one will move from awareness only to experimenting, or from experimenting to pilot-ready. A jump to production-ready on compute is a finding to challenge, not a slide to celebrate.

What the CQO walks into the first council with (day 60)

- Readiness Map with ranks and the evidence behind each rank.
- Draft use-case list in the four-bucket taxonomy (Chapter 6), each with a provisional owner.
- Cryptographic-exposure sketch: where inventory stands, first-wave candidates, open vendor questions.
- Vendor inventory: who is already in the building, what they have seen, recommended freeze until the panel exists.
- Skills note: internal names, hire-or-contract gaps.
- Regulatory note: clocks that apply, clocks that are still [unconfirmed].
- Appetite note: what leadership will actually fund, including kills.
- Proposed council charter, cadence, and the first three decisions on the table.
- Education sketch: one executive briefing, one technical workshop, one BU discovery series.
- A one-page list of things the CQO recommends *not* doing in the next quarter.

CQO actions

- Run the eight workstreams in parallel and open the CISO inventory in week one.
- File the two checklists as standing instruments and assign a named reviewer to every surviving candidate.

- Defend a Readiness Map rank at the first council with the evidence behind it.
- Document every side-door vendor already in flight and freeze intake until the panel exists.
- Bring the day-60 pack as decisions required, and refuse any roadmap announcement during the diagnostic.

---

6. Use-case portfolio — four buckets

Before spending, classify. Every candidate the firm will fund, watch, or kill sits in one of four buckets. It exists so the CQO can compare unlike things without pretending they share a clock.

A candidate that cannot be placed is not yet a candidate. “Quantum transformation” is not a bucket.

How to use the taxonomy

For each bucket, the CQO looks for a specific kind of evidence, names the typical failure mode, and decides whether the work stays in research or earns a proof of concept. A PoC is expensive in attention. Research can be a paper, a simulator study, or a partnership. Do not fund a PoC because the bucket is fashionable.

Bucket A — Optimization

What the CQO looks for. A constrained decision the firm already makes, with a named objective and a named current solver — portfolio construction with real risk limits, routing with time windows, production scheduling with changeovers, unit commitment with ramping and reserves, allocation under hard constraints. If the problem is “make this graph smaller on a toy instance,” it is not yet in this bucket.

Typical failure mode. “Optimization theater”: a variational or annealing run on a random or tiny graph, compared with a weak classical method, then presented as a path to production. The second failure is a real problem whose constraint structure was stripped out so a quantum device could swallow it.

R&D vs PoC. Keep in R&D while the formulation is unstable, the classical solver has not been given a fair run, or the instance size that matters is far beyond any honest hybrid test. Fund a PoC when a business owner exists, the classical baseline is the firm’s actual stack (or the best available equivalent), and a hybrid or quantum-inspired method can be tested on a faithful instance without gutting the constraints.

Bucket B — Simulation

What the CQO looks for. A physics or chemistry question the firm already pays to answer, where classical methods (density-functional theory, molecular dynamics, finite elements, continuum models) are the current spend. The CQO looks for a simulation group that can state the observable, the accuracy target, and the cost of the current method — catalyst energetics, battery electrolytes, small-molecule binding, defect properties, selected energy-system simulations.

Typical failure mode. A molecule small enough to be a textbook example, run on a device or a noisy simulator, with no comparison to the production DFT or MD pipeline, then used to justify a multi-year platform deal. The other failure is promising “drug discovery” as if a quantum processor were a pipeline.

R&D vs PoC. This is the bucket where a physics or chemistry team can already name the observable and the cost of the current code. It is still almost never production. Fund a PoC only when those three are written down. Keep most work in R&D or in a partnership with a national lab or university, under a written accuracy

target, and only move to PoC when the instance is in the size class the science team actually cares about — or a staged proxy they will defend.

Bucket C — Machine learning

What the CQO looks for. Skepticism first. Quantum kernels, quantum neural networks, quantum generative models, and hybrid feature maps are still mostly research. There is no near-term production path implied here.

Quantum kernel methods can, under standard complexity assumptions, give a rigorous classification advantage on certain constructed learning problems that efficient classical learners cannot beat better than chance (Liu, Arunachalam, Temme, arXiv:2010.02174). Feature-map / kernel QML is a theoretically motivated candidate route when the kernel is hard to estimate classically (Schuld & Killoran, PRL 2019; Havlíček et al., Nature 2019)—not a demonstrated enterprise result.

Huang et al. (arXiv:2011.01938) is the useful counterweight: with data, classical ML can rival quantum models even when the generating circuit is classically hard. That is one more reason the CQO insists on a strong classical baseline.

The CQO still demands a named learning task, a classical ML baseline (including the firm's current model), and a reason the quantum feature space would survive data-loading, trainability, and classical reconstruction.

Typical failure mode. A slide titled "quantum ML" that shows a circuit, a toy dataset, and an accuracy number without the classical model, without a statement of how data enters the device, and without a limitation map. Treat that as theater. Challenge it in the room.

R&D vs PoC. Default to R&D or to archive. A PoC in this bucket should be rare, small, and pre-committed to a kill if the classical baseline wins on quality and cost — which the CQO should expect. Do not imply a path to production quantum ML in the board pack.

Bucket D — Security

What the CQO looks for. A compliance clock, a data-lifetime problem, or a high-assurance communications need. Post-quantum cryptography. Crypto-agility. Quantum-safe PKI. Hybrid key establishment. Quantum random number generator (QRNG) as an entropy component. QKD only where a physics-based point-to-point link is a serious requirement — not as a general internet replacement. This bucket is often the only one with a date that is not chosen by the firm.

Typical failure mode. Treating PQC as future work while funding QKD theater, or the reverse: a full QKD proposal where a standards-based PQC migration would close the risk. Second failure: a QRNG purchase presented as a security architecture.

R&D vs PoC. PQC inventory and hybrid migration are delivery, not research. Fund them as a program with the CISO. QKD and novel quantum-communication designs stay in assessment until the link, the distance, the operational model, and the alternative (PQC on the same link) are written down. QRNG is a component evaluation.

Portfolio table the CQO can copy

Maintain this as a living sheet. One row per candidate. Status is one of: watch / research / score / PoC / deliver / kill / archive. The CQO needs this instrument now so the council sees the whole board, not a highlight reel.

Bucket	Candidate	Owner	Data	Classical baseline	Horizon	Status
Optimization	(name the decision)	(BU + named person)	(source, rights, zone)	(solver + hardware)	(this year / 2–5 / watch)	
Simulation	(name the observable)			(code + accuracy target)		
Machine learning	(name the learning task)			(current model)	research unless proven otherwise	
Security	(name the surface)	(CISO + CQO)	(inventory coverage)	(current algorithms)	dated where a clock exists	

Horizon is not a vendor roadmap date. Horizon is the firm's own: this year (can test or must migrate), two to five years (prepare data and skills), watch (reassess).

A healthy first-year portfolio for most enterprises is: security in delivery, one optimization or simulation candidate in score or PoC, machine learning in research or empty.

CQO actions

- Adopt the four-bucket taxonomy as the only intake language and refuse a row without an owner.
- Put security in delivery when a clock exists; do not let compute novelty outrun it.
- Challenge every "quantum ML" proposal against task, baseline, loading, trainability, and classical reconstruction.
- Mark R&D vs PoC on every row before money moves.
- Show the full portfolio table to the council, not a highlight reel, and reassess when a regulator dates a requirement or a classical solver improves.

---

7. The "no bullshit" value filter and scoring matrix

This chapter is an investment screen. It is shaped by buy-side and investment-office discipline: formulate the bet, name the base case, demand a reason the new method could matter, require a test that can be run, and name the person who owns the outcome. Apply it before budget, not after a workshop. The portfolio in Chapter 6 told you what kind of work each candidate is; this filter decides whether any of it gets money.

Six questions. Three of them are hard gates. Fail a hard gate and the work is not funded. The others are scored. The CQO may change the weights. The CQO may not drop a hard gate to save a relationship.

The six questions

1. Can the problem be clearly formulated?
Decision variables, constraints, objective, and what "better" means — on one page. If two informed people write different formulations, stop. This is a hard gate.

2. Is there a strong classical baseline?
The best realistic method the firm can already run, or a recognized equivalent (Chapter 12). A textbook greedy algorithm is not a baseline. This is a hard gate.

3. Is quantum actually relevant, or is this optimization theater?
Relevance means a documented reason — structure of the problem, scaling of the classical method, a simulation observable that is classically painful — not a vendor architecture diagram. Quantum-inspired classical methods may be useful; they must be labeled classical.

4. Can we test on today's hardware or simulators?
A test that requires an unbuilt machine is research. Simulators, cloud access, and hybrid solvers count. If the only honest test is "wait for fault tolerance," archive it with a reopen condition.

5. Is there a credible path from proof of concept to production?
Data path, integration surface, security zone, cost model, and an owner who would take the result. Credibility can be low in year one; it cannot be imaginary.

6. Who owns the business outcome?
A named person with authority over the process the PoC would change. A steering group is not an owner. This is a hard gate.

One-page scoring matrix

Score 0–5. Weights below are a default. Change them in writing; do not change them after seeing a vendor demo. The CQO needs this matrix on the table before the first workshop so the kill rule is not negotiated under pressure.

#	Question	Weight (default)	Hard fail?	0	3	5	Score
1	Formulation	—	Yes	Vague or contested	Draft exists, constraints incomplete	One-page formulation signed by owner and technical lead	
2	Classical baseline	—	Yes	None, or a strawman	A solver exists, not the best the firm can run	Best realistic method named, with hardware and recent results	
3	Quantum relevance	25	No	No reason beyond "combinatorial"	Plausible structure; classical pain documented	Written relevance note the senior quantum lead will defend	
4	Testability now	25	No	Requires unbuilt hardware	Simulator or limited device; instance is a stretch	Honest test on current sim / cloud / hybrid, faithful instance	
5	Path to production	30	No	No data path, no integration story	Path described; security or cost unresolved	Path, zone, cost sketch, and a receiving team named	
6	Outcome owner	—	Yes	No name, or "the innovation team"	Interested sponsor without authority	Named owner who will sign the end-decision	

Kill rule. Any hard fail on formulation (1), classical baseline (2), or owner (6) = do not fund. Do not average a zero into a passing score. Questions 3–5 may be weak if the work is explicitly labeled research and paid from a research line; they may not be weak if the ask is a PoC or a platform commitment.

Indicative bands (after hard gates pass). Use as conversation, not as a false precision:

- 0–1.5 weighted average on 3–5: archive or research memo only.
- 1.5–3.0: explore under a small cap, or kill if attention is scarce.
- 3.0–4.0: PoC candidate; still requires the Chapter 8 form.
- 4.0–5.0: rare. Recheck whether the classical baseline was truly the best.

How the CQO communicates a kill

Kills fail when they are theatrical or when they are silent. Use a short note to the owner and the council. One page.

- The candidate, the bucket, and the ask that was refused.
- The test that failed (formulation / baseline / owner / relevance / testability / path).
- What was learned that the portfolio should keep.
- What is archived, where, and what evidence would reopen it.
- What the firm will *not* say externally.

Do not offer a consolation workshop, a smaller toy instance, or a joint press line. If the owner wants to appeal, the council hears it once, with new evidence, not with a rewritten slide.

Aesthetics of the kill matter less than repeatability. After the third kill, the intake quality rises. That is the point.

CQO actions

- Freeze the six questions, the hard gates, and the kill rule in writing before the first vendor meeting.
- Refuse any request to waive a hard gate; freeze weights for the quarter.
- Engage the owner before scoring so the kill is not a surprise.
- File each kill as a one-page note with reopen conditions in the archive.
- Measure intake by clean kills and clean funds, not by workshops; reassess the filter annually, not mid-demo.

---

8. From research theme to business case

Vague themes (“quantum for supply chain,” “quantum for discovery”) are cheap to propose and expensive to staff. The CQO runs two narrowing steps, then refuses budget until a one-page form is complete. The form is the instrument. The narrative around it is optional. Chapters 6 and 7 decided what kind of work survives; this chapter turns a survivor into an ask the CFO can read.

Step 1 — Map the pain, not the technology

List the operational and scientific bottlenecks that already consume money, time, or risk. Use the interview notes from Chapter 5 and the four buckets from Chapter 6. For each item, record two judgments:

- Technical viability of a quantum or hybrid approach *versus* a better classical one (a hypothesis, not a hope).
- Business value if the hypothesis were true (who would use the answer, what decision would change, what the current method costs in time or quality).

Step 1 should produce a long list. Do not fund from it. Do not show it to vendors.

Step 2 — Downselect to a concentrated set

Apply the Chapter 7 filter. Deepen the technical and cost-benefit analysis only on rows that pass the hard gates. The output is a short set: typically a PQC delivery program plus one or two compute candidates, and a watch list. Everything else is archive or research-memo.

Downselection is a council decision. The CQO recommends. The owner of a killed row is informed before the meeting.

One-page business-case form

The CQO requires this form before budget. If a section is empty, send the form back. Budget waits on a complete form.

Field	What the CQO expects to read
Problem statement	One paragraph. Decision, constraints, observable. No market poetry.
Business owner	Named person, title, and what they will do with a result, including a negative result.
Current classical method	Software, hardware, team, typical instance size, current quality and time.
Pain point	What is failing: quality, time, energy cost, robustness, regulatory exposure. A number the owner already believes, not a number invented for the form.
Quantum hypothesis	What, specifically, might improve, and why quantum or hybrid methods are relevant. If the honest method is quantum-inspired *classical*, say so.
Data required	Source, volume class, rights, zone, and whether a faithful synthetic proxy will be used.
Benchmarking method	Metrics agreed in advance (quality, wall-clock, cost, stability). The classical comparison set (Chapter 12). Who will run the classical side.
Vendor vs internal build	Options, including “internal on simulators only.” Exit and reproducibility terms if a vendor is involved.
Success metric	The number or condition that triggers continue / scale. Matching the baseline is not success unless the form said it was.
Budget	Line items and the ask. People-time, cloud access, vendor fees, legal. State the ask the firm is actually making. Do not paste a vendor catalogue price to fill the box.
Timeline	Start, mid-gate, end-decision date. Calendar dates, not “Q3.”
Decision gate	Explore / PoC / kill / archive — and who signs.

Attach the scored Chapter 7 matrix. The form without the matrix is a story.

Gates and who signs

Gate	Meaning	Typical evidence	Who signs
Explore	Small, time-boxed study: formulation, baseline, literature, simulator probe	Completed form, passed hard gates, capped ask	CQO + owner
PoC			

Gate	Meaning	Typical evidence	Who signs
	Honest test against the classical stack on a faithful instance	Form + KPI sheet (Chapter 11) + security review if data moves	CQO + owner; CISO if data leaves or a new control appears; CFO if above a threshold the firm already uses
Kill	Stop. Archive the evidence.	Failed gate, failed KPI, or lost owner	CQO; owner informed; council recorded
Archive	Stop for now; reopen if a dated condition arrives (hardware class, regulation, data rights)	Written reopen condition	CQO + owner
Scale (rare)	Move toward a production path	Chapter 13 checklist started; metrics defined; receiving team named	CQO + owner + CTO/CIO + CISO + CFO as the firm's production-change rules require

Matching a classical baseline is not advantage and is not, by itself, a scale decision. Scale only after quality, time, cost, and stability were defined in the form and then met.

Research themes that cannot complete the form stay in the senior quantum lead's watch list. They do not appear as budget lines named after a vendor.

The portfolio and the filter now select what to fund. Part III is how funded items are built, compared, and refused when they are only demos.

CQO actions

- Run Step 1 and Step 2 as the only path from theme to money; keep the long list off vendor desks.
- Refuse incomplete one-page forms; attach the scored matrix every time.
- Agree the sign-off map with the CFO before the first ask, and set an explore-cap so small studies do not become unofficial PoCs.
- Validate that "success" was defined before the test, not after, and log every gate.
- Bring legal and procurement in once a vendor option is on the form; keep killed and archived cases searchable.

Part III — Quantum Computing Implementation

Almost no firm should own a QPU. Rent access, simulate here, and compare against the stack you already pay for. Your job is the access path, the data rule, the vendor bar, and the no. Hardware modality is a buyer's question, not a research seminar. What Part II selected, this part builds, measures, and — when the evidence is only a demo — refuses.

---

9. The hybrid enterprise stack — most firms will not buy a QPU

The year-one default for most enterprises is not to buy a quantum computer. Rent cloud access, simulate locally, and compare results against the classical stack the firm already owns. Some vendors sell an on-premises system as a special on-prem offer; treat a purchase as a council exception, not as the market's only path. The QPU, when it appears at all, is one component. Software, classical pre- and post-processing, security, and data governance are the rest.

Decide the environment before anyone tours hardware. What you buy, what may leave, and who can open an account are the first three decisions. The rest of this chapter is those decisions, not a tour of the stack. Lead with four procurement decisions in year one: access, simulator, harness, and egress rule.

Year-one refuse list — lead with the no

Minimum viable quantum lab (year one)	Refuse in year one unless the council records an exceptional reason
Cloud access to at least one multi-vendor path or two single-vendor paths	On-premises dilution refrigerator or exclusive hardware purchase
On-prem or HPC simulator the science team controls	Exclusive modality lock-in in software or in the contract
Classical benchmark harness on the firm's own solvers and GPUs	Unrestricted data egress to a vendor cloud
Access control: single sign-on (SSO), least privilege, audit logs, named account owner	Multi-year prepaid exclusive capacity without an exit clause
Data rules: classification, residency, keys, instance-metadata policy	A branded "quantum center" whose first output is a press release
Security review of SDKs and notebooks before production data is touched	Shadow accounts opened by a business unit after a conference
Spend alerts and a monthly cost line the CFO can read	A stack that cannot export circuits, results, and scripts

The minimum lab is enough to run Chapters 11 and 12. Anything on the refuse list is a capital or lock-in decision disguised as infrastructure. That refusal is policy. Dedicated on-premises machines are sold; they are not the default for a first lab. An on-prem special offer is a council exception.

What the CQO procures and constrains

Cloud quantum access. The major cloud offerings — IBM Quantum, Amazon Braket, Azure Quantum, and the hardware vendors they front — are how almost every firm will touch a device. Procure at least one path that can reach more than one modality, or two paths that together do. Constrain: identity (SSO, least privilege), logging, region, and what may be sent. Govern: a named owner for the account, a spend alert, and a rule that a notebook is not a production system.

On-premises simulation. Local or HPC-hosted simulators (statevector, tensor-network, and whatever the science team already trusts) are where most honest iteration happens. Procure licenses or open-source support as the architecture team recommends. Constrain: these simulators sit inside the same access and data rules as the rest of scientific computing. Govern: results from a simulator are labeled simulated.

HPC, GPUs, and tensor networks. The classical side of the hybrid loop — pre-processing, variational outer loops, tensor-network contraction, GPU statevector — usually matters more to year-one evidence than the QPU. Procure time on the firm's existing HPC or GPU estate before asking for a new cluster. Constrain: quantum projects do not jump the queue without a council decision. Govern: the same job scheduler and cost codes as any other scientific workload.

SDKs and workflow orchestration. Teams will want Qiskit, Cirq, PennyLane, TKET, CUDA-Q, vendor-native kits, and a workflow layer that can call a solver, a simulator, or a cloud QPU. Procure with portability

in mind (Chapter 10). Constrain: one or two supported kits in year one, not seven. Govern: version pins, dependency review, and a ban on shadow IT notebooks with production data.

Secure access and data governance. Decide, in writing, what data may leave, to which region, under which contract, and who holds the keys. Decide what must stay on-premises or in a sovereign cloud. Decide whether even metadata of a problem instance is sensitive (it often is: a routing instance can reveal network structure; a molecule can reveal a research direction). The security architect in the core office owns the rule; the CQO enforces it on every squad.

PQC posture of anything new. Every new account, SDK, VPN path, and vendor API is a cryptographic surface. Inventory it. Ask the vendor questionnaire (algorithms, hybrid mode, agility). Do not declare the new stack certified for post-quantum cryptography. Require inventory coverage, algorithm agility, and a vendor questionnaire, and require that the stack does not weaken the migration the CISO is running.

The QPU is one component

Treat the device as a back-end behind an orchestration layer. Classical code prepares instances, calls a solver or a circuit, and scores the result. If that loop only works in a vendor portal, the firm does not have a stack. It has a demo environment.

CQO actions

- Procure cloud access, a controlled simulator, and the benchmark harness before any hardware conversation matures.
- Put data egress, region, and keys in the first security paper; add every new component to the cryptographic inventory.
- Govern SDKs down to a short supported list and coordinate with enterprise architecture so the lab is not an island.
- Refuse the year-one list in writing; take on-prem or exclusive exceptions only to the council.
- Monitor spend and shadow accounts monthly.

---

10. Modalities and the vendor-evaluation framework

The CQO does not pick a hardware religion. The CQO needs enough fluency to hear a sales claim, ask for the metric, and keep software and contracts able to pivot. Chapter 9 decided the environment; this chapter decides who may sell into it.

What each modality means for a buyer

One line each. Numbers (error rates, qubit counts, roadmap dates) belong in the vendor’s evidence pack. Ask for the number; do not reprint a press figure.

- **Superconducting.** Fast gates, cloud-mature, connectivity and noise are the buyer questions; the major cloud offerings all expose this class.
- **Trapped ions.** High-fidelity gates and all-to-all or rich connectivity in current systems; slower gate times and scaling of the trap architecture are the buyer questions.
- **Neutral atoms.** Large analog or digital arrays in the cloud; calibration, connectivity pattern, and digital-gate maturity are the buyer questions.

- **Photonics.** Different engineering path (often networking-adjacent); distinguish discrete-variable from continuous-variable, and ask what is actually available to a paying customer versus a lab.
- **Annealing.** A specialized Ising / Quadratic Unconstrained Binary Optimization (QUBO) machine, not a universal gate device. Useful only if the firm's problem maps honestly. Compare against classical annealers and mixed-integer programming (MIP), not against a random search.
- **Silicon spin.** Attractive long-term integration story with semiconductor manufacturing; access and maturity for enterprise work are still the buyer questions.
- **Quantum-inspired.** Classical algorithms and hardware (tensor networks, simulated bifurcation, specialized digital annealers, GPU heuristics) *marketed* with quantum language. Label them classical. They may still win the benchmark. Winning does not make them a QPU.

Do not score a vendor until you have separated these classes. If a slide mixes two, split the slide before the meeting.

Hardware-agnostic as a contract and software rule

Applications, orchestration, and legal paper must allow a pivot. That means:

- Circuits, Hamiltonians, or QUBO instances stored in a form the firm can replay elsewhere.
- Results exportable with enough metadata to reproduce.
- SDKs that can target more than one back-end, or a thin internal layer that can.
- Contracts that do not punish a change of modality or of cloud front-end.
- No "reference architecture" that hard-wires a single vendor's queue, compiler, and portal.

Agnostic does not mean using every device. It means the firm can leave.

Vendor-evaluation framework

Use this table with procurement. Score evidence, not adjectives. Ask for the metric; file the vendor's number in the evaluation pack with the date you opened the source. The CQO needs this score sheet before the second meeting so adjectives never become the panel's record.

Criterion	What the CQO asks	Evidence that counts	Failure signal
Qubit quality	What metric, on what device, measured how, dated when?	Technical document the team has opened	A keynote number with no method
Connectivity	What is the native graph? What does compilation do to depth?	Device map + a compiled example of *our* circuit class	"Fully connected" without a compilation cost
Error rates	One- and two-qubit (or analog equivalent), state preparation and measurement (SPAM), and how often recalibrated	Device card or paper on the specific machine we would use	A single "fidelity" for a product family
Logical-qubit roadmap	What error-correction assumption, what physical overhead, what the vendor will *not* promise	Technical roadmap the lead will defend; no date unless the primary source is dated	A calendar year in a press release
Software stack	Which SDKs, compilers, hybrid loop, job control? Can we export?	A dry-run from our account	Portal-only workflow
Cloud access	Queue, region, identity integration, uptime practice	Contract + a test job under our SSO	

Criterion	What the CQO asks	Evidence that counts	Failure signal
			Personal-email onboarding for an enterprise
Support	Who answers, in what timezone, during a PoC?	Named support path in the paper	A researcher's inbox
Pricing transparency	Units (shot, time, subscription), what changes the bill, what is quote-only	Written rate card or a quote the CFO can read	"We'll find a way"
Security model	Data residency, encryption in transit and at rest, key holder, admin access, subprocessors	Security paper + questionnaire	"We're a research cloud"
Enterprise delivery	Has this vendor completed a test *like ours* (problem class, not logo slide)?	Reference the team can call, or a refusal we record	A logo wall
Exit	Export of results and scripts; replay elsewhere; what happens if the vendor disappears or is acquired	Contract clauses	Silence, or a setup fee that only pays off in year three

Run the table for PQC-product vendors as well, with the obvious swaps (algorithms, hybrid mode, agility, certification *claims* versus a completed questionnaire). Part IV of this handbook treats security products in depth. In Parts I–III, keep them on the same panel discipline.

Name vendors in the evaluation pack when you have opened their technical documents. In board language, "the major superconducting, ion, and atom cloud offerings" is safer than a ranked religion.

CQO actions

- Adopt the evaluation table as the only vendor score sheet and open every numeric claim or discard the number.
- Split mixed-modality slides before scoring; label quantum-inspired products classical.
- Require software and contracts that let the firm leave; treat the exit clause as a first-class criterion.
- Bring procurement and legal in before a second meeting.
- File a two-page council note per shortlisted vendor and review the panel quarterly.

---

11. Proofs of concept that actually matter

A PoC is the instrument that turns education into a decision. The CQO establishes goals and KPIs before it starts. A PoC that proves "not yet," with data, is a good PoC. A PoC that produces an unmeasurable slide is a wasted quarter. The stack and the vendor panel are settled enough; now the funded item has to earn an end-decision.

Five non-negotiable criteria

1. A real business problem.
The work starts from an operational or scientific bottleneck the firm already has. If the instance had to be invented so a device could run, criterion 1 has failed.

2. A real dataset or a faithful synthetic proxy.
"Faithful" means the proxy preserves the constraint structure, the size class that matters (or a staged size the owner will defend), and the noise or uncertainty the production problem carries. Random graphs, random maximum-cut (MaxCut), and shuffled tables are not faithful. A reduced instance is allowed when the reduction rule is written down and the owner agrees it still tests the decision.

3. A strict classical benchmark.
The best realistic classical alternative, on named hardware, run by people who know that stack (Chapter 12). The classical side is staffed and timed as a real workstream.

4. A measurable quantum or quantum-inspired approach.
Named method, named back-end (device, simulator, or classical quantum-inspired solver), named metrics. If the method is quantum-inspired, it is labeled classical in every sentence of the write-up.

5. An end decision.
One of four, defined below. "We learned a lot" is not an end decision.

End decisions

Decision	Meaning	The CQO does next
Kill	KPIs missed, or a hard gate discovered during the work	Stop spend; one-page note (Chapter 7); dissolve the squad
Continue	Evidence is incomplete but the remaining uncertainty is specific	Time-box the next increment; do not widen the problem
Scale	Pre-defined quality, time, cost, and stability metrics were met; a receiving team exists	Open the Chapter 13 checklist; do not hold a press meeting
Archive	Hardware, data rights, or regulation blocked an otherwise well-posed test	Write the reopen condition; keep the harness

Matching the classical baseline is not, by itself, Scale. Scale requires the metrics in the form, a receiving team, and a reason production would change.

When the CQO is shown a toy Quantum Approximate Optimization Algorithm (QAOA) slide

A common exhibit: a variational run on a small or random graph, a colorful landscape, and a claim that the firm is "on the path." Apply the five criteria in the room.

- Criterion 1 fails if the graph is not the firm's problem.
- Criterion 2 fails if the instance does not preserve constraints or size class.
- Criterion 3 fails if the comparison is a weak classical method, or none.
- Criterion 4 fails if the only metric is "the circuit ran."
- Criterion 5 fails if the recommended next step is another workshop.

In the room: thank the presenter, refuse to take the slide to the council, and ask for a Chapter 8 form. If the work already spent money, write a kill or archive note so it cannot be recycled as momentum.

What a good write-up must contain

Do not accept a write-up that cannot put the firm's current solver and the new method on the same instance, with quality, wall-clock, cost, and what would have to change in production. If that page is missing, the PoC has not ended. The write-up, which the squad cannot skip, contains:

- Problem, owner, and the pre-committed KPI sheet.
- Data lineage or the synthetic-proxy rule.
- Classical method, hardware, who ran it, wall-clock, quality, cost.
- Quantum or hybrid method, hardware or simulator, who ran it, the same metrics.
- Stability across seeds, calibrations, or days, as relevant.
- Integration notes: what would have to change in the production path.
- Security notes: what data moved, what the review said.
- The recommended end-decision and the dissenting view if there is one.
- Reproduction: scripts, versions, seeds, and where they live.

The CQO reads this document, not the slide. If the document does not exist, the PoC has not ended.

CQO actions

- Gate every PoC start on the five criteria, a KPI sheet, and a named owner.
- Define the end-decision vocabulary before kickoff and staff the classical side as a real workstream.
- Test the "faithful proxy" claim with the owner, not only with the scientists.
- Challenge toy variational slides in the room; thank the presenter and refuse the slide to the council.
- Require the write-up as the ending artifact; escalate any PoC that began without owner or KPIs.

---

12. Benchmarking against the best classical alternative

Fake advantage is an operational failure. The CQO compares any quantum or hybrid claim against the best realistic classical alternative the firm can run — or a recognized equivalent the science lead will defend — not against a weak or outdated strawman. Chapter 11 required the comparison; this chapter is the card that makes it real.

What "best realistic" includes

Staff the classical side as if it were the project.

- Exact solvers where the instance still permits them (branch-and-cut, exact diagonalization, exhaustive search on the true small case).
- Production heuristics the firm already uses.
- GPU-accelerated codes and batched solvers — including GPU optimization and quantum-circuit simulation libraries the HPC team already trusts (cuOpt, cuQuantum).
- Tensor-network methods, where they are the state of the classical art for the structure at hand (Orús's review is the map; name the contraction the science lead will defend).
- Simulated annealing and other metaheuristics, tuned, not default-parameter (Kirkpatrick 1983 is the reference class, not a performance claim).
- Mixed-integer programming with the solver and time limits operations already trust (CPLEX, Gurobi, or the equivalent the firm already licenses).

- Domain-specific classical methods: electronic-structure codes the chemistry team already runs (PySCF or the in-house stack); DFT functionals and basis sets the materials team uses; routing engines the logistics team uses; risk engines the desk uses.

Name the method. Do not transplant published speedups onto the firm's instance. The no-strawman standard is the one Hoefler, Häner, and Troyer (2023) and Babbush et al. (2021) set: compare against the best realistic classical alternative, not a convenient one.

If the quantum team cannot name the classical counterpart, the test has not started.

Production initiatives vs exploratory R&D

Write the distinction on the first page of the benchmark.

Track	Purpose	What "good" looks like	What the CQO forbids
Production-bound	Change an operational decision or a control	Pre-defined metrics met against the best realistic classical method; Chapter 13 opened	Claiming advantage from a weaker baseline
Exploratory R&D	Build skill, test code on early hardware, map limitations	A limitation map, a reproduction pack, and a reopen condition	A press release; a production promise; a silent promotion into the portfolio

Exploratory work is legitimate. It still gets a limitation map: what instance size failed, what noise did, what the compiler did to depth, what the classical method achieved on the same instance. Exploratory work does not get a keynote.

The benchmark card

The CQO requires one card per comparison. Put the card on the table in the working session. If it is not filled, the comparison has not started.

Field	Entry
Instance	Name, source, rights, and whether it is production, reduced, or synthetic-faithful
Size	Variables / qubits or equivalent; constraints; time horizon
Classical method + hardware	Solver or code, version, CPU/GPU/HPC class, time limit, who ran it
Quantum / hybrid method + hardware	Method, back-end (device / simulator / inspired-classical), version, who ran it
Wall-clock	End-to-end, including pre- and post-processing, not just device time
Quality	The metric from the form (objective, residual, chemical accuracy, constraint violation)
Cost	Units the CFO accepts (people-time, cloud units, HPC allocation). State the ask and the actual; do not invent catalogue prices.
Stability	Repeat runs, seeds, calibration windows
Integration	What would have to change to use this in the current path
Who ran it	Names, independence (classical side not run solely by the vendor)
Reproduce-how	Path to scripts, data (or proxy rule), seeds, and environment lock

A card signed only by the vendor is a vendor document. The firm’s applied scientist or quantitative lead countersigns.

Treat a claim of practical quantum advantage on a production workload as unproven unless the comparison is on the card, sourced, and countersigned by the person who ran the classical side. Matching the baseline is a data point, not a scale decision.

CQO actions

- Make the benchmark card mandatory in every working session; if it is empty, the comparison has not started.
- Challenge any comparison that used a weak classical method; require independence on the classical side.
- Label production-bound vs exploratory on page one of every test.
- Measure end-to-end wall-clock and quality, not device-only time; archive cards with the decision log.
- Reassess when the classical solver or GPU code improves — it will — and refuse a press line on exploratory work.

---

13. Production readiness and why demos die

A demo dies when it cannot survive contact with identity, data, cost, and ownership. The benchmark card in Chapter 12 told you whether the method earned a hearing; this chapter decides whether anything operational may depend on it. The CQO and the business owner sign a go / no-go list before anyone uses the word production.

Go / no-go checklist

Initial each row. A blank row is a no-go.

Criterion	Go looks like	No-go looks like	Initials (CQO / owner / other)
API stability	Versioned interface the receiving team will support; change process agreed	Portal clicks; breaking changes without notice	
Security review	Completed review; data zone respected; keys and identity under enterprise control	“We used the vendor’s demo tenant”	CISO or delegate
Data pipeline integration	Production or near-production path; refresh and quality checks	One-off extract on a laptop	
Cost monitoring	Meter, budget code, alert, and an owner who sees the bill	Unmetered cloud; surprise invoice	CFO delegate if material
Model / method governance	Method, versions, and limitations recorded; change control	An undocumented circuit in a notebook	
Reproducibility	Scripts, seeds, environment lock, independent rerun	“It worked last Thursday”	
Fallback classical path	The current method remains callable if the hybrid path fails or queues	Quantum path is the only path	
		Marketing uptime language	Legal / procurement

Criterion	Go looks like	No-go looks like	Initials (CQO / owner / other)
Vendor service-level agreement (SLA)	Written availability, support, and data-handling terms		
Regulatory acceptability	Compliance has said the method and the data path are allowable	“We’ll ask after go-live”	Legal / compliance
Business-owner sign-off	Owner accepts the metrics, the residual risk, and the operating cost	Sponsor has moved jobs	Owner

All ten are required for a production-bound compute path. PQC delivery uses a related list (inventory coverage, hybrid mode, agility, vendor questionnaire, rollback) owned with the CISO; do not wave a compute demo through because a certificate migration is going well, or the reverse.

Why demos fail to become systems

The failure is usually organizational. Describe it without a statistic.

- **No owner.** The scientist was the sponsor. When the demo ended, no operator took the page.
- **No fallback.** The design assumed the new path would always be there. Operations refused a single point of failure.
- **No cost model.** Device time, people, and integration were never expressed in the units the CFO uses.
- **No data path.** The demo used a static file. The production system needed a daily feed, rights, and quality checks.
- **Vendor demo environment is not production identity.** Different tenant, different keys, different logging, sometimes different geography. Security review starts over — or should.

Other regulars: the API changed; the method was not reproducible after a calibration; legal had not seen the data clause; a regulator would not accept an unexplained solver on a controlled decision.

What the CQO escalates vs what the CQO kills

Signal	Escalate	Kill
Owner left, successor unnamed	Once, for 30 days, to the BU head	If no successor signs
Cost model missing	To CFO delegate with a two-week ask	If the squad cannot state the ask
Security review blocked	To CISO with a scoped fix	If data rules cannot be met and no proxy is faithful
Vendor SLA absent	To procurement / legal	If the vendor will not put terms on paper
Fallback missing	To CTO/CIO and the owner	If operations will not accept a dual path and the new path is unstable
Regulatory “not yet”	Archive with a dated reopen condition	If the team wants to go live anyway
Metrics redefined after seeing results	—	Kill or force a new PoC with new pre-committed KPIs
		The go-live, until the list is signed

Signal	Escalate	Kill
Press requested before the checklist	To the CEO / communications, with a no	

Demos that die for these reasons are not an argument against quantum. They are an argument for this checklist. The CQO's reputation inside the firm will track the quality of no-go decisions at least as much as the first go.

CQO actions

- Sign the go / no-go list jointly with the owner before the word production is used.
- Kill work that redefines metrics after the result; escalate missing owners, SLAs, and security blocks on a short clock.
- Require a classical fallback before any operational dependence.
- Log every no-go in the decision log so it cannot be relitigated as a surprise.
- Coordinate CISO, legal, and the receiving team; reassess any "go" after the first operating quarter.

Part IV — Quantum Security: PQC, QKD, and Crypto-Agility

The CQO already owns two clocks. The compute clock is still uncertain. The cryptographic clock is not. A machine that could open today's public-key traffic may be years away; replacing that traffic is already a multi-year program with inventory, procurement, and a board date. Part IV is that program: PQC run jointly with the CISO, crypto-agility as the lasting target, and a disciplined assessment of QKD and QRNGs where physics adds a control the PQC program does not already cover.

---

14. The Quantum Threat Model

A Cryptographically Relevant Quantum Computer (CRQC) would put the public-key cryptography that still protects most enterprise traffic, identity, software updates, and stored archives at risk. That sentence is a planning premise. Do not wait for a classroom explanation of the algorithms, and do not wait for a vendor to date the machine. Cryptographic replacement takes years. Certificates, protocols, modules, and third-party products do not move on a quarterly cycle. The CQO's job on this chapter is to make that premise operational: inventory, a Harvest-Now Decrypt-Later (HNDL) sort, a board translation, and a procurement clock.

Compute advantage can remain a research question. The migration cannot.

Two clocks on the same desk

The firm will be asked, often in the same week, when quantum computing will beat the classical stack and when the cryptography must move. Separate the answers.

The first clock is capability. Whether a quantum processor will outperform the best classical alternative on a problem the business owns is still uncertain, and Chapter 12 is how that question is answered. The second

clock is exposure. RSA, Elliptic Curve Cryptography (ECC), the digital signatures that authenticate software and people, and the key-exchange steps that open Transport Layer Security (TLS), virtual private network (VPN), and Secure Shell (SSH) sessions are the premises. Plan as if those public-key schemes can be opened. The date of the machine is not the date of the program.

What this requires of the CQO is a sentence the council can reuse: compute readiness is gated on evidence; cryptographic replacement is gated on confidentiality lifetime and on the time it takes to change the estate. A slide that blends the two clocks — "we will migrate when the hardware is real" — is a delay dressed as prudence. Challenge it in the room.

Public-key premises, then the work

RSA, ECC, signatures, and key exchange still sit on the estate. Point at them. A threat-model workshop that draws a circuit is the wrong meeting.

A CRQC that can run the known attacks on those schemes would force a replacement of the public-key layer. Symmetric algorithms and hash functions are a different, narrower conversation; they are not a reason to leave RSA and ECC in place. The CQO does not become the resident cryptographer. The CQO ensures the CISO's engineers can point at every place those schemes still sit, and that the board hears residual risk in business language.

Walk into the CISO's inventory meeting with four columns already ruled: surface, algorithm family, confidentiality lifetime of the data it protects, and whether a third party terminates the cryptography. That is the threat model as an object.

Harvest-now-decrypt-later is the sort key

HNDL — harvest-now-decrypt-later, also named store-now-decrypt-later in the 2022 English paper from France's Agence nationale de la sécurité des systèmes d'information (ANSSI) — is the reason the program has already started. An adversary can record ciphertext today and open it when a CRQC arrives. The National Institute of Standards and Technology (NIST) names the same operation in Internal Report (IR) 8547, an Initial Public Draft of November 2024, and treats it as a reason the transition is urgent. The joint Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and NIST factsheet of 17 August 2023 frames the same problem as inventory and migration for data with a long secrecy lifetime.

The CQO does not need a new risk taxonomy for this. The CQO needs a sort.

Sort field	What the CQO asks	What "already in scope" looks like
Confidentiality lifetime	Must this record still be secret after the public-key layer is no longer safe?	Patient data, trade secrets, long-dated contracts, state secrets, industrial-control configurations, insurance archives, mergers-and-acquisitions files, long-lived keys
Interception ease	Can the ciphertext be recorded from a link, a backup, a partner, or a cloud store the firm does not control?	External TLS, partner application programming interfaces (APIs), archived mail, off-site backups, traffic that already leaves the building
Value to an adversary	What would a later decryption change — a price, a formula, a citizen, a grid configuration?	Anything the firm would still pay to keep closed in ten years
Update friction		

Sort field	What the CQO asks	What “already in scope” looks like
	Can the protecting system be changed in this refresh cycle, or is it embedded, industrial, or sovereign?	Field devices, Hardware Security Modules (HSMs) with a replacement lead time, products the vendor will not re-sign

HSMs belong on that last row from the first meeting. So do backups: a migrated front door in front of an archive still wrapped in today’s public-key layer is an HNDL gift. Prioritize by the product of lifetime, interception, and value. Ease of update tells you whether the answer is a hybrid cutover this year or a residual-risk note the board has to accept.

Establish the sort with the CISO in writing. Communicate it upward as “records we cannot afford to have opened later,” not as a physics brief. Reassess the sort when a new archive, a new partner, or a new backup path appears — the inventory will move.

Clocks the CQO translates — and clocks the CQO does not invent

Standards now exist, and they are usable. In August 2024 NIST published Federal Information Processing Standards (FIPS) 203, the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), for key encapsulation, and FIPS 204, the Module-Lattice-Based Digital Signature Algorithm (ML-DSA), and FIPS 205, the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), for digital signatures. Published 13 August 2024; Federal Register effective 14 August 2024. NIST’s PQC project page, updated 5 August 2026, states that these standards “can and should be put into use now.” Falcon (to be specified as FN-DSA in a future FIPS 206) is not a finalized FIPS. HQC (Hamming Quasi-Cyclic) — the additional KEM NIST selected for ongoing standardization — is not an issued FIPS. Do not brief either as a reason to wait.

Dated national guidance now sits next to those standards. Keep the issuers separate. Do not blend the calendars.

- **ANSSI (France).** ANSSI *aims to* impose (`vise`) PQC obligations for products *entering qualification* from 2027. ANSSI states it will *not be reasonable* to purchase products that do not integrate PQC after 2030. That 2030 line is buyer guidance, not a general statute. ANSSI’s recommendations, including hybridisation, do not today have the character of a regulatory obligation outside the classified / Diffusion Restreinte / systèmes d’importance vitale (SAIV) / visa perimeter. For a firm that sells into qualification, 2027 is a product-engineering clock. For a firm that only buys, 2030 is a reasonableness line the procurement policy can adopt without pretending it is already law.
- **Network and Information Security (NIS) Cooperation Group.** On 23 June 2025 the Group, with European Commission support, published *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*. Cite existence and date. Do not invent Member-State deadlines from a slide.
- **UK National Cyber Security Centre (NCSC).** *Timelines for migration to post-quantum cryptography* (20 March 2025) is aimed primarily at large organisations, operators of critical national infrastructure including industrial control systems, and firms with bespoke information technology. NCSC’s published milestones, quoted: by 2028 — define migration goals, carry out a full discovery exercise, build an initial plan; by 2031 — carry out early, highest-priority migration activities and refine the plan into a thorough roadmap; by 2035 — complete migration to PQC of all systems, services, and products. Apply those years only where the UK guidance applies. Do not paste them onto a French or U.S. surface.

- **CISA / NSA / NIST.** The 17 August 2023 *Quantum-Readiness: Migration to Post-Quantum Cryptography* factsheet is inventory-and-migration framing. Use it as a shared language with the CISO. Do not treat it as a market-size figure.
- **NSA Commercial National Security Algorithm suite (CNSA) 2.0.** Exists as transition guidance for national security systems. Cite that existence. Do not reprint a milestone table. If the firm has a national security system (NSS) surface, legal and the CISO read the primary suite; the CQO does not reconstruct dates from memory.

NIST IR 8547 remains an Initial Public Draft. Use it for the HNDL name and for the idea of a civilian transition plan. Do not take deprecation years from a draft into a board pack as settled NIST rules.

Prepare one regulatory note for the council: which of these clocks apply to *this* firm, which are buyer guidance, which are NSS-only, and which are still unmarked. Date what you can date. Mark what you cannot. A blended “2030 quantum deadline” that mixes ANSSI reasonableness, an NCSC completion year, and a draft NIST table is a governance failure the CQO prevents.

What the board is allowed to hear

The board pack on this threat model is four lines and a residual-risk note.

1. Public-key cryptography on the estate (RSA, ECC, signatures, key exchange) is the exposure. The machine that would open it does not have to exist this year for the recording of ciphertext to matter.
2. Replacement takes years. The program is inventory, HNDL sort, hybrid migration, and vendor pressure — to be funded and dated.
3. Standards exist and should be used: FIPS 203 / 204 / 205. National clocks that apply to this firm are listed, with issuer and strength (obligation, aim, buyer guidance, NSS-only, draft).
4. Residual risk: inventory coverage, third parties, embedded systems, and any archive still wrapped in today’s public-key layer.

Communicate that the firm is buying time-to-migrate, not a prophecy about a machine date. Refuse a board slide that dates a CRQC. Refuse a slide that treats PQC as a future research theme. If a director asks “when do we have to be done?”, answer with the clocks that actually bind this firm and with the HNDL sort, not with a vendor roadmap.

CQO actions

- Assess which national clocks apply to this firm — obligation, aim, buyer guidance, NSS-only, or draft — and write the split in the regulatory note.
- Establish, with the CISO, the four-column inventory object and the HNDL sort (lifetime × interception × value, with update friction as the sequencing constraint).
- Prioritize first-wave candidates from that sort before any algorithm debate, and walk into the inventory meeting with the sort already ruled.
- Communicate the four-line board pack; challenge any slide that dates a CRQC or that delays migration until compute advantage arrives.
- Prepare procurement language now so new purchases after the ANSSI 2030 reasonableness line, and any product entering ANSSI qualification from 2027, are not surprises; reassess the note when a new issuer dates a requirement.

---

15. Post-Quantum Cryptography Program

This is delivery. Bucket D in Chapter 6 already said so. The PQC program is a joint CQO–CISO program: the CISO owns operational cybersecurity execution, incident response, and the security build; the CQO owns quantum-specific strategy, inventory sponsorship, standards awareness, and executive translation. One roadmap. Two accountabilities. A ticket in last year's security backlog is not a program.

NIST's line on the three issued FIPS is that they can and should be put into use now. ANSSI tells organisations to start the inventory now and to put PQC into the information-system renewal cycle. The CISA / NSA / NIST factsheet frames the same work as discovery and migration. The CQO's job is to make that work dated, funded, and visible.

Joint ownership — write it once

Reuse the Chapter 2 split. Deepen it into a working responsible / accountable / consulted / informed (RACI) table the squad can run.

Workstream	CQO	CISO / security engineering	Others
Threat strategy and board translation	Accountable	Consulted	Legal / risk informed
Inventory scope and HNDL sort	Sponsors; accountable for completeness of scope	Accountable for collection and operations	Business units supply data-lifetime calls
Algorithm and hybrid profile	Sets the demand (FIPS 203 / 204 / 205; hybrid default)	Selects implementations, libraries, and cutover mechanics	Enterprise architecture consulted
Wave plan and sequencing	Jointly accountable with CISO	Accountable for the build	Chief Technology Officer (CTO) / Chief Information Officer (CIO) consulted; Chief Financial Officer (CFO) informed
Vendor crypto questionnaires	Coordinates intake and the evidence bar	Runs the questionnaire and scores answers	Procurement / legal on the paper
Testing, interoperability, rollback	Validates that a wave has an end-decision	Executes labs, pilots, and production cutover	Receiving teams sign
Residual risk and exceptions	Translates to council and board	Owns the risk register entry	Risk committee informed
New quantum-stack surfaces (software development kits (SDKs), cloud accounts)	Ensures they enter the inventory *before* use	Reviews before production data moves	—

If the chart puts the whole program under the CISO and the CQO only "advises," PQC will compete with the rest of the backlog and the board will hear it as a control family. If the chart puts the whole program under the CQO and the CISO only "is informed," the build will stall. Hold both A's on the wave plan. Escalate the first month that a wave has no named security lead or no named CQO sponsor.

Inventory the CQO sponsors

The inventory is the program's first artifact. The CQO sponsors it; security engineering collects; the business units name confidentiality lifetime. ANSSI's own FAQ tells organisations to inventory products and business uses that embed cryptography, the algorithms in use, and the data whose confidentiality or authenticity must still hold after 2030, with that duration written down. NCSC's 2028 milestone, where that guidance applies, is a full discovery exercise and an initial plan. Neither issuer is asking for a physics seminar.

Record, for each surface:

Surface	What the row must contain	First question the CQO asks
TLS	Termination points, library, version, cipher suites, certificate chain	Can this terminator run hybrid key establishment against FIPS 203?
VPN	Concentrators, clients, protocol family, firmware, management plane	Dated vendor PQC / hybrid roadmap, or a replacement path?
SSH	Fleet, versions, key types, certificate or authorized-key model	Where do host and user keys still sit on RSA or ECC?
Public-key infrastructure (PKI)	Roots, intermediates, profiles, issuance paths, relying parties	Parallel PQC or hybrid chain planned, or a single cutover fantasy?
Code signing	Signers, timestamping, update channels, embedded verifiers	What still trusts today's signatures after a key-compromise story?
Identity	Identity providers, client certificates, smart cards, device identity	Which logins and device joins die if the current signature scheme is withdrawn?
Certificates	Every profile that is not already in the PKI row — machines, users, partners	Expiry and re-issuance cycle vs. the wave plan
Application programming interfaces (APIs)	External and partner endpoints, mutual TLS, application-level signatures	Who terminates cryptography — us, them, or a gateway we do not own?
Third-party products	Software-as-a-service (SaaS) products, appliances, libraries, managed services	Questionnaire issued; answer signed; hybrid and agility stated?
HSMs and roots of trust	Modules, firmware, algorithms, replacement lead time	Can the module take ML-KEM / ML-DSA / SLH-DSA, or is it a capital event?
Archives and backups	What is wrapped, with which keys, where the ciphertext lives	Is a migrated front door sitting in front of a harvestable store?

A row without an owner is incomplete. A row that says "uses encryption" without an algorithm family is incomplete. Do not declare the estate "PQC-certified." Require coverage, algorithm names, and a completed questionnaire. Named national qualification schemes, where they exist, stay in the CISO's language. The CQO's language is coverage, dates, and residual risk.

Coordinate discovery tools with the CISO as a complement to this process. A scanner does not replace the business-use and data-lifetime pass ANSSI describes. Sponsor both.

Long-life data and the RSA / ECC map

Classify records by confidentiality lifetime before you classify systems by glamour. Anything that must remain confidential — or authentic — past the horizon the firm is using (ANSSI's "after 2030" line for French buyers is one such horizon; NCSC's 2035 completion line is another, where it applies) is already an

HNDL item. Write the duration on the row. A system that protects thirty-year data and cannot be updated in this refresh cycle is a residual-risk item the council sees, not a footnote in a lab notebook.

Then map public-key dependence. For each inventoried surface, mark whether RSA, ECC, or both still perform key establishment, signatures, or both. That map is the migration object. It is also the object you take to vendors: “show us where this product still does RSA or ECC for key establishment or signatures, and what replaces it.” Symmetric-only rows stay on the inventory; they do not consume the first wave.

Prioritize by exposure and shelf life

Exposure is interception ease plus value. Shelf life is confidentiality lifetime plus update friction. The CQO prioritizes waves from that product, not from a vendor’s favorite protocol.

Wave	Criteria	Typical contents	What the CQO decides
0 — already recorded	Long shelf life, easy to intercept, high value	External TLS and partner APIs that carry long-life data; off-site backups of those stores; archived mail and file stores	Fund discovery and a hybrid path now; do not wait for a statute
1 — identity and updates	Compromise would let an adversary sign or enter	PKI, code signing, SSH, administrator VPN, device identity	Joint wave plan; hybrid default; rollback written
2 — refresh-cycle products	Third parties and applications the firm can move on a normal cycle	SaaS, APIs, libraries, HSMs with a dated roadmap	Questionnaire + contract demand; refuse a buy that has no PQC path
3 — hard to touch	Embedded, industrial, fielded, sovereign, or vendor-frozen	Industrial controls, field devices, long-life appliances	Document residual risk; align with the replacement cycle; escalate a silent tolerate

Wave 0 is an HNDL decision. Wave 1 is an integrity and control-plane decision. Mixing them into a single “crypto upgrade” hides the reason Wave 0 cannot wait. Define the waves on one page. Prioritize in the council, not in a vendor workshop.

Hybrid as the default migration mode

Demand hybrid (classical + PQC) as the default migration mode. ANSSI recommends hybridisation wherever a post-quantum protection is needed, in the near and medium term, and does not recommend systematic hybridisation only for hash-based signatures (SLH-DSA among them). Do not invent a hybrid profile, a concatenation recipe, or a parameter set. Tell engineering and vendors: classical and PQC together for key establishment and for signatures, unless the CISO’s cryptographers have written an exception for a hash-based signature path.

Hybrid is how the firm avoids a one-way bet on a young algorithm *and* a one-way bet on a scheme a CRQC would open. It is also how two parties migrate on different clocks: a protocol that can negotiate is a protocol that can move. Govern the dual-stack period. Define, before cutover, the criterion for turning the classical-only path off. A hybrid deployment that can silently fall back to RSA or ECC, and that no one measures, is not a migration.

Hash-based signatures (FIPS 205) are the exception ANSSI already carved. Treat that exception as written, not as a general license to skip hybridisation on ML-KEM or ML-DSA.

Testing, interoperability, and rollback

A wave without a test is a hope. The CQO does not design the lab. The CQO requires that a wave have one.

- Interoperability: both ends of every in-scope channel, including partners and mobile clients. A terminator that speaks hybrid to itself is not a test.
- Negotiation: confirm the session actually selected the hybrid or PQC suite, and that it cannot be forced back to classical-only without an alarm. Incorrect cryptography can look like a healthy service.
- Performance and size: measure on the firm's real certificate profiles and message sizes. File the numbers the receiving team will defend. Do not import a vendor slide.
- Rollback: a written path back to the last known-good suite, with an owner and a time box.
- Metrics the council can read: share of in-scope clients and terminators on the new suite; share still classical-only; open vendor exceptions.

Validate the write-up the way Chapter 11 validates a compute proof of concept (PoC): the document, not the slide. Test partners early; a third party that cannot negotiate is a Wave 0 finding, not a late surprise. Escalate a wave that entered production without rollback or without a negotiation check.

Vendor questionnaire — checklist

Issue one questionnaire. Accept signed answers. A marketing page is not an answer. Run PQC-product vendors through the same panel discipline as Chapter 10, with the obvious swaps.

#	Ask	Acceptable evidence	Fail
1	Which algorithms are implemented, and in which role (key encapsulation, signature, other)?	Named FIPS 203 / 204 / 205 (or a written "none yet") and parameter sets	"Quantum-safe" with no algorithm name
2	Is hybrid (classical + PQC) supported, on which protocols, and can classical-only be disabled?	Protocol list; configuration that a test can reproduce	Hybrid promised "on the roadmap" with no date the vendor will sign
3	Can algorithms, parameter sets, and certificates be changed without a major product rewrite?	A documented agility path	Firmware-frozen algorithm; "wait for the next appliance"
4	What is the effect on certificates, PKI, and message size?	A note the firm's PKI owners can read	"No impact" on a signature-size change
5	Against whom has interoperability been tested?	Named counterparts, versions, dates	"Compliant with the standard" and no peer
6	What is the dated roadmap, as the vendor states it?	A dated, signed statement	A slide implied date; a verbal "soon"
7	Which claims are completed evaluations, and which are intentions?	Named scheme and status, if any	"Certified" with no scheme, or a scheme that does not exist
8	What libraries, versions, and embedded products terminate cryptography inside this product?	A list the inventory can absorb	"Industry-standard crypto"
9	What is the rollback and dual-stack story?	A procedure the CISO will accept	Cutover with no return path
10			Silence

#	Ask	Acceptable evidence	Fail
	What happens if a parameter set is withdrawn?	A change process and a notice commitment	

Coordinate issuance with procurement so the questionnaire is a condition of purchase and of renewal, not a favour. File answers in the decision log. Challenge any “quantum-safe” claim that cannot survive row 1.

A dated roadmap the council can fund

The roadmap is waves plus clocks, not a vision statement.

Horizon	What CQO + CISO produce	What the council decides
First 90 days	Inventory started; HNDL sort live; Wave 0 / 1 candidate list; questionnaire issued to in-house and top third parties	Scope of Wave 0 / 1; freeze on buys that fail row 1 of the questionnaire
This year	Hybrid on at least one scoped Wave 0 or Wave 1 surface; first interoperability write-up; residual-risk note on Wave 3	Whether to widen; envelope for the next wave
Current refresh cycle	PQC and hybrid language in every in-scope request for proposal (RFP); HSM and PKI plan; partner deadlines	Capital that is really a cryptographic replacement
Applicable national clocks	Coverage against ANSSI qualification / 2030 reasonableness, NCSC 2028 / 2031 / 2035 where they apply, CNSA 2.0 if NSS is in scope	Residual risk the board will accept in writing

Measure coverage, not workshops: inventory rows complete, questionnaires returned, surfaces on hybrid, Wave 3 exceptions still open. Reassess after each wave and when an issuer dates a requirement. Sponsor one PQC squad (Chapter 4) and do not let a compute PoC steal its lead.

CQO actions

- Sponsor the inventory and the HNDL sort in week one of any new mandate year, and keep the Chapter 2 owns / coordinates split on the wave plan.
- Define Wave 0 / 1 / 2 / 3 from exposure and shelf life; refuse a single undifferentiated “crypto upgrade.”
- Coordinate questionnaires through procurement; escalate any in-scope buy that cannot name an algorithm.
- Test interoperability and negotiation, not just “the library linked”; validate rollback before cutover.
- Measure coverage each quarter (rows, answers, hybrid surfaces, open Wave 3 exceptions) and communicate residual risk in the board pack; reassess when a clock or a partner changes.

---

16. Crypto-Agility as the Real Enterprise Target

A one-time cutover to today’s PQC suite will have to be done again the next time a parameter set is withdrawn, a protocol profile changes, or a second signature standard is issued. Falcon is already in NIST’s “ongoing standardization” column. HQC is there too. IR 8547 is still a draft. The lasting target is the firm’s ability to change cryptography again without a decade-long program. The first PQC wave is the first exercise of that ability.

ANSSI defines crypto-agility as the ability to extend and/or replace cryptographic components within IT-systems, without affecting their functionality, while minimising the downtime of the provided service during

the update. Demand that ability in contracts and architecture reviews: algorithm, certificate, and protocol. Write the criterion for ending support of the traditional algorithms.

Algorithm, certificate, and protocol agility

Three layers. All three have to move.

Algorithm agility. The product or service can change the algorithm or the parameter set — ML-KEM to a later approved key-encapsulation mechanism (KEM), ML-DSA to SLH-DSA or to a later approved signature, a parameter set to a stronger one — without a rewrite of the business application and without a forklift of the appliance. Demand this in the questionnaire (Chapter 15, row 3) and in the contract. A firmware-frozen algorithm is a Wave 3 item from the day it is purchased.

Certificate agility. PKI can issue, validate, and retire a new profile — including a hybrid or parallel chain — without a year of relying-party archaeology. The CQO engages the PKI owners on: a PQC or hybrid issuance path, a plan for roots and intermediates, a re-issuance cycle that fits the wave plan, and a way to find every relying party. A new algorithm that no certificate profile can carry is a science project.

Protocol agility. TLS, VPN, SSH, and the APIs that wrap them can negotiate a new suite and can disable an old one on a date the council has seen. Negotiation without a disable date is how classical-only lives forever. Govern the dual-stack window. Document the kill date for classical-only on each in-scope protocol, even if the date is “not before X, and only after coverage metric Y.”

The CQO challenges any architecture review that adds a new terminator, a new identity path, or a new partner API without stating how those three layers will change. The review is incomplete until it does.

Cryptographic Bill of Materials — an operating object

Sponsor a Cryptographic Bill of Materials (CBOM) as an operating object the firm keeps current. A CBOM here is not a named CISA or NIST specification, and this handbook does not claim one. It is the list the inventory was always trying to become: algorithms, keys, certificates, and the products that embed them, in a form procurement, architecture, and the CISO can query.

CBOM field	Why the CQO requires it
Algorithm and role (KEM, signature, symmetric, other)	So a withdrawal or a new FIPS has a blast radius
Protocol and product / library / version	So a questionnaire answer can be joined to a running system
Key and certificate locations and identifiers	So rotation and re-issuance have an owner
Data protected and confidentiality lifetime	So the HNDL sort stays attached to the object
Hybrid status and disable-classical date	So dual-stack does not become permanent
Agility path (algorithm / certificate / protocol)	So a buy that cannot change is visible at purchase
Owner and next review date	So the object does not die in a spreadsheet

Govern the CBOM as a living artifact, not as a one-off discovery report. Assign an owner in the core office (the security architect in Chapter 4) and a refresh cadence — at least at each wave, each material vendor change, and each new cloud or SDK account. Discovery that is not joined to the CBOM is theatre. A CBOM that is not used in architecture review is a filing.

Discovery that stays current

The first inventory is a project. The second year is an operation. New accounts, new SDKs, new partner APIs, new HSMs, and new “temporary” terminators will appear. Chapter 9 already required that every new quantum-stack component enter the cryptographic inventory before use. Extend that rule to every new cryptographic surface, quantum or not, that the PQC program would have to live with.

Ensure automated discovery, where the CISO already has it, feeds the CBOM. Ensure a human pass still covers business use and data lifetime — the part no scanner owns. Monitor for shadow terminators the same way Chapter 4 monitors side-door pilots: the first one is escalated to the council, not absorbed as folklore.

What the CQO demands in contracts and architecture reviews

Put the demand on paper before the second vendor meeting. Legal and procurement hold the clauses; the CQO holds the evidence bar.

Demand	Contract language the CQO insists on	Architecture-review fail
Named algorithms	Algorithms and roles listed; “quantum-safe” is not a term of art	A new terminator with no algorithm row
Hybrid default	Classical + PQC available; classical-only disableable on the firm’s date	Hybrid in a slide, classical-only in the default config
Algorithm agility	Parameter-set and algorithm change without a major version, or a priced change path	Appliance that can only move at replacement
Certificate agility	Support for the firm’s next PKI profile, including hybrid or parallel chains	A client that pins one root shape
Protocol agility	Negotiation plus a committed path to disable legacy suites	A partner API that cannot negotiate and has no end date
CBOM delivery	On boarding and on each material release: algorithms, keys, certs, embedded products	“We use standard crypto”
Notice of withdrawal	Written notice if an algorithm or parameter set is withdrawn or deprecated	Silence; the firm learns from a blog
Exit	Data, configurations, and key material leave; a successor product can be stood up	A suite that can only be changed by staying

Challenge any exception. A Wave 3 embedded device may fail several rows; that failure is documented residual risk, not a rewrite of the standard. Reassess the contract appendix when NIST issues another FIPS or when ANSSI or NCSC updates buyer language. The agility program is how the firm survives that update without another multi-year invention.

CQO actions

- Ensure every in-scope contract and architecture review carries the agility appendix (algorithms, hybrid, three-layer change path, CBOM, notice, exit).
- Govern the CBOM as a living object with an owner and a refresh cadence; document data lifetime on every row.
- Challenge new terminators, identity paths, and partner APIs that cannot state how algorithm, certificate, and protocol will change.

- Define the disable date for classical-only on each in-scope protocol, and monitor dual-stack so it does not become the estate.
- Reassess agility after each new FIPS or national update; escalate the first shadow terminator to the council.

---

17. QKD: Where It Fits and Where It Does Not

QKD does not replace the PQC program. It is a physics-based way to establish keying material on a constrained link. The PQC program covers the estate — identity, updates, partners, archives, the open internet. Most QKD proposals the CQO will see are trying to solve a PQC problem with a fibre project. Assess the proposal against the control the PQC program does not already cover. If that sentence cannot be written, refuse the project.

No vendor religion. Constraints below are premises. Distance, trusted nodes, dedicated infrastructure, cost, and operational complexity will be whatever the vendor and the firm's own engineers measure on the actual path. File those measurements. Do not import a brochure.

Where a physics-based link can add a control

QKD can be relevant when the firm needs high-assurance keying on a point-to-point path it already understands as a path — not as "the network." Typical places to assess:

- High-assurance point-to-point links the firm already treats as special (a named pair of sites, a named classification or sovereignty constraint).
- Critical-infrastructure control or safety paths where the physical plant is already a managed object.
- Telecom backbones and datacenter interconnects the operator already builds as dedicated capacity.
- Government and defense circuits that sit inside a sovereignty or classification story the legal team will defend.
- Financial-market infrastructure links (matching, settlement, market-data spines) where a dedicated interconnect already exists.
- Sovereign-security cases in which the firm or the state wants a keying mechanism whose security story is not only computational.

The common structure: two ends, a path the firm can point at, a data class that already has a special handling rule, and a reason computational PQC on that same path is judged insufficient — diversity of mechanism, a national requirement, a classified profile, or a residual risk the board has already accepted on computational cryptography. Write that reason. A reason that reads "quantum is more secure" is not a reason.

QKD stays in assessment (Chapter 6, Bucket D) until the link, the path, the operational model, and the PQC alternative on the same link are on one page. Fund it, if at all, as a named link. Do not let it stand in for a PQC wave.

Constraints that stay on the table

Treat the following as premises the proposer must answer. Do not let a slide delete a row.

Constraint	What the CQO requires on the page
Distance and path	The actual path, including every hop. No invented range.

Constraint	What the CQO requires on the page
Trusted nodes	Every node that must be trusted if the path is longer than a single protected span; who owns it; what a compromise of that node does
Dedicated infrastructure	Fibre or equivalent the firm will actually provision or lease; what is shared; who else sits on it
Cost	The ask in units the CFO already accepts (people, lease, integration, operations). State the ask; do not import a brochure.
Operational complexity	Who monitors, who patches, who replaces a box, who holds keys at the ends, what happens at 3 a.m.
Integration	How the keying material enters the existing encryptors, HSMs, or key-management system; what has to change in identity and logging
Internet-scale fit	A written admission that this does not protect general internet, mobile, partner-SaaS, or the archive problem
PQC alternative	What hybrid PQC on the same link would (and would not) cover, at what operational cost

A proposal that cannot fill the trusted-node row has not started. A proposal that claims to solve HNDL for partner APIs and SaaS has described the PQC program and then attached a fibre invoice. Challenge that in the room. Thank the presenter, refuse the slide to the council, and ask for the decision card.

Sovereign and defense cases can still fail these rows. They do not get a waiver; they get a residual-risk note and a legal opinion. Cost and complexity are not arguments against QKD in those cases; they are arguments for writing the ask.

A decision card for any QKD proposal

One card. The CQO puts it on the table. If it is empty, the assessment has not started.

Field	Entry
Link	Named endpoints, owner, data class, existing encryptor
Why PQC on this link is insufficient	A written reason, or the card stops here
Path	Distance as measured; fibre or other; every trusted node
Operations	Monitor, patch, replace, 3 a.m.; identity and logging
Cost ask	Units the CFO accepts; people and lease, not a brochure
Residual risk if we refuse	What remains after the PQC program runs on this link
Residual risk if we build	Lock-in, trusted-node exposure, ops load, what still sits on PQC
Decision	Assess further / time-boxed pilot / refuse
Reopen condition	What evidence would bring a refused card back

Decide in the council, with the CISO in the room. A QKD pilot that bypasses the CISO is a side-door. A QKD purchase that lands in the innovation budget so it can avoid the PQC squad is a governance failure. Monitor any accepted link as production infrastructure (Chapter 13): identity, logging, fallback, cost, owner. The fallback on a QKD link is the PQC or classical encryptor the firm already knows how to run. If operations will not accept a dual path, the card is a refuse.

CQO actions

- Assess every QKD proposal against the control the PQC program does not already cover; refuse a card that cannot write that sentence.
- Challenge missing trusted-node, path, operations, and PQC-alternative rows in the room; do not take the brochure to the council.
- Decide assess / pilot / refuse on the card, with the CISO present; validate any pilot as a link, not as a brand.
- Engage legal on sovereignty or classification claims; document residual risk either way.
- Monitor an accepted link as production infrastructure with a PQC or classical fallback; reassess if the path, the node owner, or the data class changes.

---

18. QRNG and Quantum-Enhanced Security Components

A QRNG is an entropy component. It can feed key generation, sit inside or beside an HSM, and matter in high-assurance or regulated environments where the CISO already treats the entropy source as a control. It does not close RSA or ECC. It does not move the HNDL sort. It does not replace QKD on a link, and it does not replace the PQC program on the estate.

Treat the purchase as a component evaluation. The question is whether this source improves the entropy the firm already uses, under the same review the CISO applies to any entropy source — design, health tests, failure mode, output handling, and where the bits actually go. A QRNG whose bits disappear into a vendor story, or whose only output is a slide titled “quantum security,” has failed that review.

Useful placements the CQO may sponsor, with the CISO:

- Key generation for the firm’s own certificate authorities (CAs), code-signing keys, and HSM-protected keys, where the entropy path is documented.
- High-assurance or regulated environments that already require a named, reviewable entropy source.
- Cryptographic infrastructure the CISO is willing to operate as infrastructure, not as a demo.

Gaming, simulation, and other non-cryptographic consumers of randomness are out of this chapter’s scope unless they share an HSM or a key-generation path with the PQC program. If they do, they enter the inventory. If they do not, they are not a security architecture.

Decide QRNG on a one-page note: where the bits go, which keys they feed, what review the CISO has completed, and what remains after PQC and (if relevant) QKD are accounted for. Ensure the note cannot be recycled as “the firm is quantum-safe.” Engage procurement so a QRNG line item cannot be substituted, in a budget narrative, for a Wave 0 hybrid path or for an inventory the firm has not finished.

CQO actions

- Engage the CISO before any QRNG conversation matures; validate the entropy path the same way any other source is validated.
- Decide on the one-page note (where the bits go, which keys, what review); refuse a purchase offered as a substitute for PQC or QKD.
- Document accepted QRNGs in the CBOM and the inventory as components, with an owner.
- Ensure budget narratives cannot replace a migration wave with a randomness line item.

• Reassess if the bits begin to feed a new key class or leave the reviewed path.

Part V — Governance, Procurement, and Ecosystem

The vendor bar, the filter, and the evaluation table already exist. This part is what they require once a third party, a lawyer, or a leadership meeting is in the room. The CQO steers the technical bar; procurement still contracts; legal owns paper; the CISO owns control design. Education is the third instrument: a firm that cannot say kill in a shared vocabulary will buy a tour. Part V is the questionnaire, the counsel brief, and the three tracks that keep the mandate from becoming a speaker series or a purchase order.

---

19. Vendor Management and Quantum Procurement

Hardware manufacturers, Post-Quantum Cryptography (PQC) vendors, and software services all sell a future. Some of that future is a product. The CQO is the enterprise's technical gatekeeper: the person who opens the single intake door, scores evidence, and refuses a platform deal that cannot survive Chapter 7. Procurement still contracts. Legal owns paper. The CISO owns control design. That split is the Chapter 2 table. Do not collapse it. Purchasing is unequipped to audit deep-tech alone. Steer the landscape in person.

Three pillars — one sheet each

Run every third party through one of three sheets. A vendor that sells two pillars gets two sheets.

Hardware providers. Cloud access or a special on-premises offer. Ask what machine, on what day, under whose identity, and whether the job is simulated or real. Named public channels already in the stack — IBM Quantum, Amazon Braket, Azure Quantum — belong on the questionnaire as access paths. Ask what hardware they actually provide. Ask for error rates and roadmap assumptions on the specific device the firm would use. File the vendor's number with the date you opened the source. Do not reprint a press figure in the council pack.

PQC solutions. Algorithms, hybrid mode, agility, and a completed questionnaire. Ask whether they support hybrid key establishment and the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 203 (ML-KEM), 204 (ML-DSA), and 205 (SLH-DSA). Name the clocks that apply to this firm — Chapter 14 — on the questionnaire: ANSSI qualification and purchase-reasonableness where that clock applies; the NIS Cooperation Group roadmap for EU-facing surfaces; Commercial National Security Algorithm suite (CNSA) 2.0 existence for national-security-system vendors. Do not reprint a milestone table. Quantum Key Distribution (QKD) and quantum random number generator (QRNG) products stay on Bucket D discipline.

Software services. Consultancies, algorithm houses, workflow layers, and "quantum-inspired" solvers. Ask for the integration model: which software development kit (SDK), which compiler, whether circuits and results export, whether the firm's own solvers remain the baseline. Label quantum-inspired work classical.

Apply the Chapter 7 filter to the contract

Do not rewrite the six questions. Apply them to the paper before the second meeting.

- **Formulation (hard gate).** The contract names the problem, the instance class, and what "better" means. A platform subscription "to explore quantum" has failed the gate.
- **Classical baseline (hard gate).** The vendor does not own the only comparison. The firm's applied scientist runs the baseline, or a named equivalent the science lead will defend (Chapter 12).
- **Quantum relevance.** The statement of work contains a written reason the method could matter, or the work is labeled research and paid from a research line.
- **Testability now.** If the only honest test is an unbuilt machine, do not sign a multi-year capacity commit. Simulators, cloud access, and hybrid solvers count.
- **Path to production.** Exit, data return, reproducibility, and the integration surface sit in the contract, not in a slide appendix.
- **Outcome owner (hard gate).** A named business owner signs the Proof of Concept (PoC) start. Innovation is not an owner.

Fail a hard gate and the paper does not go to procurement. The CQO may change weights on questions 3–5. The CQO may not drop a hard gate to save a relationship.

Questionnaire — questions × evidence that counts

Use this table with procurement. It extends the Chapter 10 evaluation sheet into contract language. Score evidence.

#	Question	Evidence that counts	Failure signal
1	What hardware do you actually provide?	Named device or cloud back-end, modality, and a job under the firm's identity	A family name, a future rack, or a logo wall
2	What is simulated versus real?	Job labels, a dry-run that marks simulator vs device, and a rule the invoice follows	Mixed results in one chart
3	Error rates and roadmap assumptions?	Device card or paper on the machine we would use; error-correction assumption stated; dates only if the primary source is dated	A keynote fidelity; a calendar year in a press release
4	What are the security guarantees?	Security paper: residency, encryption in transit and at rest, key holder, admin access, subprocessors, incident path	"We're a research cloud"
5	Can we export results and reproduce them?	Export of circuits, Hamiltonians or Quadratic Unconstrained Binary Optimization (QUBO) instances, results, seeds, and replay metadata	Portal-only workflow; screenshots
6	What happens if the vendor disappears or is acquired?	Exit clause, data-return clock, escrow for anything the firm cannot replay, surviving license for paid work	Silence, or a setup fee that only pays off in year three
7	What are the Intellectual Property (IP) terms?	Background vs foreground; who owns formulations, derived models, and publications; license after exit	Joint-ownership fog; a publication right the firm did not see
8	Can our data leave our environment?	Written egress rule, region, classification, and whether instance metadata is treated as sensitive	"Anonymized is fine" without a review
9			

#	Question	Evidence that counts	Failure signal
	Do you support hybrid / PQC security?	Named algorithms, hybrid mode, agility, completed questionnaire. Point at NIST FIPS 203/204/205 and at the Chapter 14 clocks that apply to this firm (ANSSI, NIS Cooperation Group, CNSA 2.0 existence for national-security-system vendors)	"Quantum-safe" with no algorithm list
10	What is the integration model?	SDK list, identity (single sign-on (SSO)), job control, a dry-run from the firm's account	Personal-email onboarding; a portal that hard-wires one queue

Run the same ten rows for a PQC-product vendor and a software house, with the obvious swaps (algorithms and hybrid mode lead for PQC; export and lock-in lead for software). Chapter 10 still scores qubit quality, connectivity, support, and pricing.

Exit, escrow, and data return

Write the leave before the stay. The Chapter 10 exit row asked whether the firm can leave. This clause is how.

- **Export and replay.** Circuits, instances, scripts, results, and environment locks leave with the firm in a form a second team can run.
- **Data return and deletion.** A clock, a format, a certificate of deletion, and a named contact. Include backups and subprocessors.
- **Escrow.** Portal-only compilers, custom transpilers, or calibrated pulse libraries the PoC depends on go to escrow or to an internal mirror the science lead will defend.
- **Surviving rights.** Paid-for work remains usable after termination, acquisition, or insolvency. Publication and reference-use rights do not survive unless counsel said so.
- **No-punish pivot.** Changing modality or cloud front-end does not trigger a recapture of discounts or a data-hostage fee.
- **Panel.** Year-one default is two access paths or one multi-vendor path (Chapter 9). An exclusive multi-year capacity buy is a council exception.

If the vendor will not put exit, escrow, and data return on paper, the CQO does not take the deal to the council. Procurement then has nothing to contract.

CQO actions

- Open the single intake door and refuse side-door pilots discovered after a conference.
- Score every vendor on one of the three pillar sheets before the second meeting; split mixed-pillar slides.
- Apply the Chapter 7 hard gates to the statement of work; refuse a platform deal that cannot name a problem, a baseline, and an owner.
- Put the ten-row questionnaire in procurement's pack; file evidence with the date opened.
- Require exit, escrow, and data-return clauses as first-class terms; escalate silence to the council.
- Coordinate CISO on the security paper and legal on IP and publication before anyone signs.
- Review the panel quarterly; reassess when a device card, a standard, or a classical solver moves.

---

20. Legal, Risk, Compliance, and IP

Legal owns paper. The CQO owns the brief that makes the paper specific. A template Non-Disclosure Agreement (NDA) and a standard cloud addendum will not see the payload: instance metadata, a molecule, a routing graph, a formulation the firm would not publish, a result the vendor would like to keynote. Route the first vendor conversation through legal (Chapter 2). Do not wait for a draft contract.

Finance, pharmaceuticals, defense, telecom, and the public sector put legal and compliance in the room from day one. The rest of the firm does the same the first time data, a model, or a public claim is in play.

What the CQO puts on the counsel brief

One pack per vendor or collaboration. If a section is empty, send it back. Counsel cannot protect a fact they were not told.

Brief section	What the CQO writes	What counsel owns
Parties and purpose	Named entity, pillar (hardware / PQC / software), problem class, and whether this is NDA-only, a PoC, or a panel seat	Entity check, paper type, signature authority
Data and payload	Classification, residency, whether instance metadata is sensitive, what may leave, what must stay, key holder	Data-processing terms, transfer mechanism, retention and deletion
Access path	Channel (including IBM Quantum, Amazon Braket, or Azure Quantum if those are the path), region the job would run, subprocessors the vendor has named	Jurisdiction map against the firm's residency rules; government-access residual
Security model	Questionnaire result; hybrid / PQC posture if a new surface; identity and logging	Control language in the paper; CISO still owns control design
IP and foreground	What the firm brings (formulations, data, baselines); what must come back (results, scripts, derived methods)	Background vs foreground; license after exit; assignment
Publication and publicity	What the firm will *not* say; whether a joint paper or a logo slide is even on the table	Publication right, trademark, press approval (Chapter 2 external-claims row)
Lock-in and exit	Chapter 19 exit / escrow / data-return ask	Enforceable clauses; insolvency and assignment
Export-control class	Whether the item is hardware, certain software, a cryptographic product, or a defense-adjacent service; who the end user is; whether a national-security system is in scope	Classification, license, restricted-party screen. The CQO flags the class. Counsel names the regime.
Model / method governance	How the method will be versioned, who may change the objective, and the Chapter 13 fallback	Liability, audit right, acceptable-use of the method on a controlled decision
Sector overlay	Which clock or supervisor already applies (table below)	Regulatory notice, filing, and the conversation with the supervisor

Export controls are a class of issue. Quantum hardware, some software tools, and cryptographic products can sit in controlled categories. Cloud jobs can move a payload into a jurisdiction the firm did not choose. The CQO flags the class on the brief — hardware, software, crypto, defense-adjacent, national-security-system vendor — and stops. Counsel classifies.

Cloud jurisdiction is the same discipline. Name the region, the logs, the subprocessors, and the operator of the quantum processing unit (QPU) if it is not the cloud front-end. Counsel maps that list to the firm's residency and government-access rules.

Sector overlay — legal from day one

Sector	What the CQO puts on the brief on day one	What the CQO does not decide
Finance	Data lifetime, model-governance path, whether a controlled decision would depend on an unexplained solver, vendor concentration	Whether the supervisor will accept the method; market-abuse and outsourcing paper
Pharmaceuticals	Molecule and assay sensitivity, publication vs trade-secret choice, clinical or manufacturing data that must not leave	Regulatory submission, trial, and promotional claims
Defense	End-user, facility, nationality of staff who will see the payload, whether CNSA 2.0 is in scope as a named national-security-system programme	Classification, facility clearance, and the license
Telecom	Link vs network, whether QKD is even a Bucket D candidate, lawful-intercept and integrity surfaces	Spectrum, interconnection, and the operator license
Public sector	Which clock applies (Chapter 14): NIST FIPS for U.S. federal or contractor surfaces; ANSSI qualification and purchase-reasonableness for French government and critical operators; NIS Cooperation Group roadmap for EU-facing work	The procurement code and the qualification file

A collaboration with a university or a national lab uses the same brief. Publication rights fail more often here than in a vendor deal. Decide before the first dataset moves: who may publish, who reviews, what is delayed, and what is never a paper.

Lock-in, models, and the risk register

Vendor concentration and harvest-now-decrypt-later already belong on the enterprise risk register (Chapter 3). Add three more lines when a contract is live: inability to export and replay; a publication or logo right the firm did not mean to grant; a method that would sit on a regulated decision without a classical fallback. The CQO writes the residual in the firm's language. Risk owns the register. Legal owns the clause that shrinks the residual.

Model and method governance is the Chapter 13 row brought into the paper: version, limitation map, change control, and the right to audit. Counsel can write an audit right. The CQO has to tell them what to audit.

CQO actions

- Route the first vendor or lab conversation through legal; refuse a side-door NDA.
- Complete the counsel brief before paper is drafted; send empty sections back.
- Flag export-control class, payload sensitivity, and publication intent; stop at the flag.
- Engage compliance on day one in finance, pharma, defense, telecom, and the public sector.
- Put lock-in, unexplained-method, and harvest-now-decrypt-later residuals on the risk register with Risk.
- Coordinate CISO on control design and procurement on the Chapter 19 exit terms.
- Reassess the brief when the access path, the region, or the payload class changes.

21. Internal Education and Executive Communication

Two failures kill the mandate. Overhype turns the office into a speaker series and starves the PQC clock. Indifference leaves the cryptographic replacement unfunded and the compute portfolio without owners. The CQO is the strategic translator: the person who keeps leadership, security, data science, and the business units on the same vocabulary, and who refuses a briefing that cannot survive the decision log.

Chapter 2 already assigned the three-track plan to the CQO and the workshops to practitioners. This chapter is the playbook. Human Resources (HR) and Learning and Development (L&D) coordinate. Communications owns positioning. The CQO owns the facts.

Three tracks

Track	Cadence	The CQO uses it to…	Must produce
Executive briefings	Quarterly, on the firm's risk or technology cycle (Chapter 4)	Ground non-technical leaders in the two clocks and the kill rule, without a hardware tour	A pack of decisions, residuals, and clocks; a sentence each residual a leader can repeat
Technical workshops	Standing calendar; extra sessions against a named gap	Close operational gaps *and* point researchers at commercial outcomes	A completed skill gap or a Chapter 8 form; a one-page return note after any external course
Business-unit discovery	Repeating Chapter 5 interviews	Find pain, owners, and data	Candidate rows for the Chapter 6 portfolio

Executive briefings. The pack is decisions, residuals, and clocks. One sitting: what changed in the portfolio, what the Chapter 7 filter killed or funded, where the PQC wave sits against any dated instrument that applies, what the board is allowed to say. Practical advancements and emerging cybersecurity risk, in the firm's language. If a non-technical leader cannot repeat the residual in a sentence, the pack failed.

A short literacy series for non-technical leaders sits beside the quarterly: three or four sessions, capped, taught by the senior quantum lead and the security architect, on compute readiness, harvest-now-decrypt-later, and the vendor bar.

Technical workshops. Two directions in the same room. First, close operational gaps: hybrid job control, the benchmark card (Chapter 12), data-egress rules, the PQC questionnaire, the go / no-go list. Practitioners teach. The CQO sponsors the calendar and sits in when a workshop is about to become a vendor demo. Second, point researchers at commercial outcomes. Many technical hires arrive from academic tracks. Guide them toward a Return-on-Investment (ROI)-shaped view of their own work: who the owner is, what decision would change, what the current method costs in time or quality, what the Chapter 8 form requires. Do not invent an ROI number. Require the form.

Conferences and advanced courses are a tool for a named gap. The CQO approves the trip against the gap and requires a one-page return note in the decision log.

Business-unit discovery. The Chapter 5 interview, on a repeating cadence. Sit with profit-and-loss owners, operations, research and development, and risk. Lead with pain. Record owner, problem class, data location, current method, and political heat. The output is candidate rows for the Chapter 6 portfolio.

Outputs the CQO measures

Literacy, realistic expectations, and a shared vocabulary. Measure those.

Output	What good looks like	What the CQO refuses as a metric
Literacy	A non-technical leader can state the two clocks and the kill rule; a scientist can complete a Chapter 8 form	Headcount trained; badges issued
Realistic expectations	Board pack matches the decision log; no press line ahead of a signed gate (Chapter 2)	Keynotes given; media mentions
Shared vocabulary	Intake uses the four buckets and the six questions; “quantum-inspired” is labeled classical	A glossary nobody uses in a meeting
Cross-functional dialogue	A monthly working session where a business-unit owner, a scientist, and the security architect argue a row	A town hall

The collaborative friction is the point. Run discovery until a high-value row the filter will actually score appears.

The quarterly pack — what stays out

Keep the executive briefing to a length a non-technical leader will read.

- Portfolio table (Chapter 6), including kills and archives.
- Filter outcomes since last quarter: funded, killed, reopened.
- PQC wave status with the CISO: inventory coverage, hybrid posture, vendor-questionnaire gaps. Date what you can date. Mark what you cannot.
- Vendor panel: who is on it, who left, which exit clause was tested.
- Residuals on the risk register, in one sentence each.
- What the firm will not say externally.

Leave out qubit counts, error-rate tours, roadmap calendars copied from marketing, and a count of talks. The CQO speaks when asked, and only with evidence already in the decision log.

CQO actions

- Establish the three-track calendar with HR / L&D in the first quarter; keep practitioners as the teachers.
- Deliver the quarterly executive pack as decisions and residuals; refuse a hardware tour.
- Sponsor technical sessions that close a named operational gap and require an ROI-shaped Chapter 8 form from research staff.
- Run business-unit discovery as pain interviews; feed the portfolio, not a speaker series.
- Measure literacy, expectation-match, and shared vocabulary; do not count keynotes.
- Engage the CISO on the PQC portion of every executive brief.
- Facilitate the cross-functional working session and escalate a briefing that drifted ahead of the decision log.

Part VI — Roadmap and Execution

Parts I–III gave the office, the filter, and the production gate. Parts IV–V gave the security program, the contract bar, and the three education tracks. This part puts those instruments on a calendar. The first hundred days install the diagnostic, the council, and a first roadmap the firm can fund. The next twelve months run PQC and the first compute initiatives in parallel. Date the work, name the owners, and report the decisions the board used.

---

22. The First 100 Days

The first hundred days show whether the mandate can operate. Days 0–30 map who must be in the room and what is already in flight. Days 30–60 finish the diagnostic Chapter 5 already specified. Days 60–100 turn that pack into a first roadmap, a PQC program charter, a gated budget, and a quantum council that can say no. Hold Chapter 5's rule: the diagnostic stays open through day 60; the first roadmap is a day-60-to-100 product.

Do not rewrite the mandate letter, the Readiness Map, the Chapter 7 filter, or the Chief Information Security Officer (CISO) inventory. Put them on this calendar and run them.

Days 0–30 — who is in the room, what is already moving

Walk the Chapter 3 alliance list before anyone books a vendor workshop. Name the Chief Executive Officer (CEO) or equivalent, the Chief Financial Officer (CFO), the CISO, the Chief Technology Officer (CTO) or Chief Information Officer (CIO), one business-unit (BU) head who already owns a painful classical stack, legal, procurement, and risk. File the Chapter 2 mandate letter if it is not signed. Write the CISO dotted line into that letter in the first two weeks.

Open the CISO inventory in week one (Chapter 5, workstream 4 and the cybersecurity checklist). Begin the confidentiality-lifetime sort: which records must remain confidential past the firm's own planning horizon, and which public-key surfaces still terminate those records. Start the eight workstreams in parallel; specialists collect, the CQO chairs.

List every quantum, "quantum-inspired," and PQC conversation already in flight. Note who invited them, what data they have seen, and whether a contract exists. Side-door pilots found in this window are a finding. Freeze new intake until the Chapter 7 filter is on paper. Chapter 1 already required that order.

Work	Instrument already in the book	Owner	Exit
Stakeholder map	Chapter 3 alliances; Chapter 2 RACI	CQO	Named peers; first meetings dated; missing A flagged
Mandate on file	Chapter 2 letter; owns / coordinates split	CEO signs; CQO files	Letter signed; CISO dotted line written
Quantum / security diagnostic opened	Chapter 5 eight workstreams	CQO chairs; specialists collect	All eight opened; CISO inventory started in week one
Current initiatives listed	Chapter 5 workstream 5	CQO + program manager	Every live test, lab, and PQC ticket named

Work	Instrument already in the book	Owner	Exit
Vendor review and intake freeze	Chapter 5 vendor inventory; Chapter 10 score sheet	CQO; procurement informed	Who is in the building, what they have seen; freeze until the filter exists
Filter on paper	Chapter 7 six questions and hard gates	CQO	Weights frozen for the quarter; no workshop before this page

Days 30–60 — diagnostic pack, not a vision speech

Complete the Readiness Map (Chapter 5). Assign one enterprise rank and, if useful, a rank per domain — compute experimentation, cryptographic migration, skills, governance. Production-ready is rare; treat a jump to that rank as a finding to challenge. Finish the algorithmic and data-pipeline checklist on every candidate that survived the first interview pass. If three or more items are still unknown, the candidate stays at awareness and does not consume Proof of Concept (PoC) budget.

Build the Chapter 6 portfolio table. One row per candidate. Four buckets only. A row without an owner is research; label it that way. Security sits in delivery when a clock applies to this firm; compute novelty does not outrun it.

Turn the CISO inventory into a cryptographic-exposure map the council can read: inventory coverage, first-wave surfaces, long-life data, open vendor questions. Date the clocks that apply; mark the clocks that are still unconfirmed. The education sketch in the day-60 pack is enough for this window: one executive briefing, one technical workshop, one BU discovery series — the three tracks already named in the Chapter 2 mandate table. Part V treats the tracks in depth; days 30–60 only put owners and a first date on each.

Walk into the first full council (Chapter 5's day-60 pack) with ranks, the draft portfolio, the exposure sketch, the vendor freeze, the skills note, the regulatory note, the appetite note, a proposed council charter, and a one-page list of things the CQO recommends not doing next quarter.

Work	Instrument already in the book	Owner	Exit
Readiness assessment	Chapter 5 Readiness Map and both checklists	CQO; named reviewer per surviving candidate	Rank defended with evidence; awareness rows kept off PoC budget
Use-case portfolio	Chapter 6 four-bucket table	CQO; provisional BU owners	Every row placed; empty fashion buckets allowed
Crypto exposure map	Chapter 5 cybersecurity checklist; CISO inventory	CQO sponsors; CISO / security engineering collect	First-wave list; confidentiality-lifetime sort started; residual gaps dated
Education plan (sketch)	Chapter 2 three-track table; Chapter 5 day-60 pack	CQO; Human Resources / Learning and Development informed	First date and owner on each track
Day-60 council pack	Chapter 5 "what the CQO walks in with"	CQO	Decisions required, including the proposed charter

Days 60–100 — first roadmap, charter, envelope, council

Now write the first roadmap. It is short: PQC delivery with the CISO, a concentrated compute list that has passed the Chapter 7 hard gates, and a written refuse list for the next quarter. Attach a scored matrix and a

Chapter 8 form to every compute ask. Name the first PoC *candidates* — not launches. A candidate has an owner, a formulation, a classical baseline, and a test the firm can run now. Launch sits on the twelve-month calendar (Chapter 23) after the Chapter 11 criteria and a Key Performance Indicator (KPI) sheet exist.

Charter the PQC program with the CISO. The CQO owns strategy, inventory sponsorship, board translation, and the dated roadmap. The CISO keeps operational cybersecurity and the migration build. The charter names the reference standards the firm will use — National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 203, 204, and 205 — and the national or sectoral clocks that actually apply. Execution waves, hybrid mode, and rollback stay in the CISO's language; the CQO's language is coverage, dates, and residual risk.

Put a budget proposal in the units the CFO already uses: people-time, cloud access, vendor fees, legal. Gates, not a blank research fund (Chapter 8). Agree the sign-off map before the first ask.

Stand the quantum council (Chapter 4, Tier 2). The CQO chairs. The council decides fund / explore / kill / archive, PQC wave scope, vendor-panel membership, and what the board is told. Advisers advise; they do not vote. Vendors present by invitation and leave before the decision. The meeting is a decision slot, not a seminar, if the core office has done the work. Name the Chapter 13 go / no-go list as the production gate the first roadmap will use; do not run that list on a demo that has not earned a Scale recommendation.

Work	Instrument already in the book	Owner	Exit
First roadmap	Chapters 6–8; Chapter 5 refuse list	CQO drafts; council records	PQC + short compute list + refuse list, dated
First PoC candidates	Chapter 7 hard gates; Chapter 8 form; Chapter 11 start criteria	CQO + named owners	Scored rows; KPI sheet still required before kickoff
PQC program charter	Chapter 2 security row; Chapter 5 inventory	CQO (strategy) + CISO (operations)	Joint charter; first-wave surfaces named; clocks that apply written
Budget proposal	Chapter 8 form and gates	CQO + CFO	Envelope with explore / PoC / kill / archive; no ungated line
Quantum council standing	Chapter 4 Tier 2 cadence table	CQO chairs	Charter adopted; monthly decision slot on the calendar; first three decisions tabled
Production gate named	Chapter 13 go / no-go	CQO + future owners	Checklist identified as the only path to the word production

CQO actions

- File the stakeholder map and the signed mandate in the first two weeks; open the CISO inventory in week one.
- Document every initiative and vendor already in flight; freeze intake until the Chapter 7 filter is on paper.
- Defend the Readiness Map and the four-bucket portfolio at the day-60 council.
- Establish the first roadmap, the PQC charter, and the gated envelope only after the diagnostic pack exists.
- Name the council, table the first three decisions, and keep Chapter 13 off any demo that has not earned Scale.

---

23. The 12-Month Roadmap

Day 100 is the start of the mid-term calendar, not the end of the work. The next twelve months execute the cryptographic transition and launch the first tactical compute initiatives on the same sheet. PQC is current program work. A compute PoC that cannot name an owner or a classical baseline waits. Quantum Key Distribution (QKD) stays in assessment unless Chapter 6, Bucket D, already recorded a point-to-point requirement.

Priority on PQC is a clock problem. Cryptographic replacement takes years. Harvest-now-decrypt-later is the sorting key already used in Chapter 5. Date the clocks that apply to *this* firm — Chapter 14 — and leave the others unmarked. NIST FIPS 203 (ML-KEM), 204 (ML-DSA), and 205 (SLH-DSA) remain the reference algorithm set. Do not treat an aim as a completed obligation.

The deliverables below are a working list the CQO sizes to the firm. “Two to three PoCs” is an envelope for attention and owners, not a researched average and not a benchmark. A firm with one honest owner and one honest baseline launches one. A firm that cannot staff the classical side (Chapter 12) launches none. A firm that already has side-door tests converts them through the filter or kills them; it does not add a third to look busy.

After day 100	Deliverable	Owner	Done looks like
Months 1–3	Quantum strategy approved	CQO drafts; CEO / board approve the envelope	One- to two-page strategy: PQC waves + scored compute list + refuse list; envelope with gates
Months 1–3	Quantum council operating	CQO chairs; members as Chapter 4	Monthly decision meeting; signed fund / explore / kill / archive; advisers off the vote
Months 1–3	Use-case portfolio scored	CQO; BU owners sign their rows	Chapter 6 table + Chapter 7 scores; hard-fail rows killed or archived with reopen conditions
Months 1–3	Cryptographic inventory in motion	CISO / security engineering; CQO sponsors	Inventory started in the hundred days; first-wave surfaces listed; residual gaps dated
Months 1–3	Vendor panel established	CQO (technical bar); procurement and legal on paper	Chapter 10 score sheet in use; exit, reproducibility, and data-egress terms required; freeze lifted only for panel members
Months 1–3	Board-level reporting template created	CQO; corporate secretary / risk committee informed	Pack fields: decision log, Readiness Map, PQC coverage, PoC end-decisions, residual risk; no experiment count
Months 4–6	Working envelope of compute PoCs launched	CQO + owners; CISO if data leaves	One, two, or three starts, sized to owners and classical staffing; Chapter 11 KPI sheet and five criteria on file before kickoff
Months 4–6	PQC migration roadmap drafted	CQO (strategy) + CISO (build)	Waves, hybrid mode, rollback, vendor-questionnaire plan; clocks that apply named; QKD not used as a substitute
Months 4–6	Internal training delivered (first cohorts)	CQO; Learning and Development	Executive briefing, technical workshop, and BU discovery series held for the named first-year lists
Months 4–6	Mid-gates on live PoCs	Squads recommend; council records	Pre-committed metrics unchanged; continue is time-boxed and does not widen the problem

After day 100	Deliverable	Owner	Done looks like
Months 7–9	PoC end-decisions taken	CQO + owners; council records	Kill / continue / scale / archive in the log; write-up exists (Chapter 11); Chapter 13 opened only on Scale
Months 7–9	PQC pilot on a scoped surface	CISO (operations); CQO (translation)	Hybrid or PQC control on a named surface; questionnaire complete; rollback tested; no enterprise-wide “done” claim
Months 10–12	Budget realigned to the roadmap	CQO + CFO	Next envelope matches surviving rows and the next PQC wave; ungated science lines removed
Months 10–12	Board pack used in a live cycle	CQO	At least one quarterly or risk-committee session took a decision from the log, not from a highlight reel

Run both tracks every quarter. A month that moves only compute and parks PQC as “future work” is a governance failure (Chapter 25). A month that only inventories cryptography and never scores a compute row is a different failure: the absorption layer Chapter 1 required does not get built.

Single intake remains in force. A use case, a vendor, or a research collaboration enters through the core office. Pre-committed KPIs still precede kickoff. Security still sees the stack before procurement when data may leave, a new software development kit is installed, or a protocol changes. Squads still dissolve on kill or archive (Chapter 4).

CQO actions

- Put PQC delivery and the first compute initiatives on the same twelve-month calendar, with owners and exits.
- Size the PoC envelope to this firm’s owners and classical staffing; convert or kill side-door tests before adding new ones.
- Draft the PQC migration roadmap against the clocks that apply; leave inapplicable clocks unmarked.
- Establish the vendor panel with exit terms and questionnaire coverage before the freeze lifts.
- Deliver the three-track first cohorts and file the board template before the first quarterly cycle that needs it.
- Reassess the sheet when a regulator dates a requirement or a classical solver improves.

---

24. KPIs and Success Metrics

Do not judge the CQO by the number of quantum experiments. Experiments are activity. The scorecard below measures decisions, coverage, and alignment — the work this book already required instruments for. Adopt this table as the year-one scorecard. Change a metric in writing at a council; do not change it after seeing a result.

“What good looks like” is an instrument state, not a borrowed percentage and not a headcount target. The CQO sets the firm’s own coverage dates on the inventory and the first-wave list. The table does not invent those dates.

Metric	What good looks like	Who reports	What the CQO does if it fails
Number of qualified use cases	Chapter 6 rows that passed Chapter 7 hard gates and have a named owner; empty fashion buckets are allowed	Core office (program manager)	Reopen BU interviews; refuse unowned rows; do not pad the count with workshop themes
Percentage of use cases with classical benchmarks	Every funded compute row has a named best-realistic baseline and, once testing starts, a Chapter 12 card	Applied scientist or quantitative lead	Halt the PoC; staff the classical side as a real workstream; kill if the baseline cannot be named
PoC kill / continue decisions made	Every live PoC has a dated end-decision in the log — kill, continue, scale, or archive	Squad recommends; CQO chairs; council records	Force the end-decision on the original KPI sheet; dissolve the squad; refuse “we learned a lot” as a close
Cryptographic inventory coverage	First-wave surfaces listed; residual gaps dated; questionnaire in circulation on those surfaces	CISO / security architect	Escalate the same week; keep “on track” out of the board pack until coverage is dated
Critical systems classified by quantum risk	Confidentiality-lifetime sort exists for systems the firm already calls critical; harvest-now-decrypt-later is the key	CISO + CQO	Finish the sort before new compute spend; do not let a lab tour outrun classification
PQC pilot completion	A scoped surface completed a hybrid or PQC pilot with questionnaire, rollback, and a residual-risk note	CISO (operations); CQO (strategy / translation)	Re-scope the surface; do not substitute a QKD briefing or a vendor roadmap slide
Vendor-risk reduction	A panel exists; exit, reproducibility, and data-egress terms are in the paper; crypto questionnaires cover the shortlist	CQO (bar); procurement (paper); security (controls)	Freeze new awards; reopen contracts that lack exit terms; do not invent an index
Internal training completion	The three tracks were delivered to the named first-year cohorts; attendance is a roll, not a campaign metric	CQO; Learning and Development	Schedule the missed track; do not substitute a keynote or an external conference
Executive decisions enabled	Decision-log entries the board, risk committee, or council actually used (fund, kill, wave, envelope, public-claim no)	CQO	Write the missing decision; stop status-only packs; escalate a committee that will only hear updates
Budget aligned to roadmap	Envelope and gates match the scored portfolio and the PQC waves; no ungated research line named after a vendor	CFO delegate + CQO	Re-cut the ask; kill the ungated line; bring the next envelope back to the surviving rows

Vendor-risk reduction is those three artifacts — panel, exit terms, questionnaire coverage — measured as present or absent on the vendors that matter. Do not build a composite score to look quantitative.

Executive decisions enabled counts log entries a governing body used. A slide that was shown and filed is not a decision. A kill the council signed is.

Budget alignment is a match between the envelope and the roadmap, including the right to spend nothing on a compute row that failed a hard gate. Underspend on a killed PoC is a success on this line.

Review the scorecard in the monthly council. Report the subset the board asked for on the firm's risk cycle. Six-month reassess is for weights and which rows the firm still calls first-wave — not for moving a target after a demo.

CQO actions

- Adopt the table as the only year-one scorecard; refuse experiment-count as a success metric.
- Measure inventory coverage and PoC end-decisions every month.
- Challenge any "good" that cannot point at a named instrument.
- Escalate a failed PQC, classification, or vendor-risk row the same week it fails.
- Reassess weights with the council at six months; keep them frozen mid-PoC.

---

25. Common Failure Modes

These are the ways the calendar dies. Name the failure in the room when it appears. Do not brief a failure-rate.

Failure mode	What it looks like	What the CQO does
Quantum theater	Workshops, branded labs, and "on the path" slides with no owner, no baseline, and no end-decision	Apply Chapter 7 in the room; refuse the slide to the council; write a kill or archive note if money already moved
Vendor-led strategy	Criteria written after the tour; mixed-modality decks scored as one product; a platform commit before the panel	Freeze intake; split the slide (Chapter 10); bring procurement and legal in before a second meeting
PoCs with no business owner	The scientist or the innovation office is the sponsor; no one will take a negative result	Hard-fail question 6; do not staff the squad; if work started, kill and dissolve
No classical benchmark	A weak or missing baseline; the vendor ran the comparison; "the circuit ran" as the metric	Halt; require the Chapter 12 card, independently countersigned; kill if the baseline cannot be named
Ignoring the CISO	Cloud accounts, SDKs, or data egress opened beside security; PQC parked as a ticket in last year's backlog	Stop the experiment; put the security architect in before procurement; restore the dotted line
Treating PQC as future work	Compute novelty funded while the inventory is unopened; "we will do crypto when the machine exists"	Open the inventory the same week; put a PQC row on every quarterly agenda; hold compute if classification is missing
Overselling QKD	A general-internet replacement story; QKD proposed where a standards-based PQC migration closes the risk	Return the proposal to Bucket D; require the link, distance, operating model, and the PQC alternative on the same page
Building a lab with no production path	Lease, branding, or an on-prem quantum processing unit with no data path, no receiving team, and no Chapter 13 list	Enforce the year-one no-on-prem default unless the council records an exception (Chapter 3); fund access and a harness first
Hiring only researchers and no operators	Publication lists without a program manager or a security architect; a lone scientist with a cloud account	Hire or second the missing Chapter 4 seats in year one; do not drop the architect or the program manager

Failure mode	What it looks like	What the CQO does
Reporting science progress instead of business decisions	Qubit-class updates, conference abstracts, and “momentum” in the board pack	Replace the pack with the Chapter 23 template; report decisions, coverage, and residual risk

Visibility is a separate failure. A CQO’s success is not measured by LinkedIn followers, likes, or the number of keynotes delivered at industry events. Communications owns positioning (Chapter 2). The CQO speaks when asked, and only with evidence already in the decision log. A speaking calendar that outruns the inventory, the filter, and the end-decisions is theater with a travel budget.

Three adjacent mistakes starve the same calendar.

Applied work over unusable research. Theoretical advances matter to the ecosystem. They are not, by themselves, a corporate mandate. Open-ended academic research the firm cannot formulate, baseline, or own stays on the senior quantum lead’s watch list (Chapter 8). Translate what can be tested into a Chapter 8 form; leave the rest labelled research.

Incremental milestones. A roadmap that waits only on fault-tolerant hardware or on QKD has no year-one exit. Date the work the firm can do now: inventory coverage, crypto-agility, a hybrid PQC pilot, a compute test on today’s simulators or cloud access, a kill that teaches the next intake. Near-term hybrid methods belong on the sheet when they survive the filter. They do not wait for a machine the firm does not have.

Ecosystem agility. The PQC regulatory shift is already on the desk — FIPS 203/204/205, the Chapter 14 clocks that apply to this firm, and customer questionnaires already arriving. Similar motion will show up at the intersection of quantum computing and artificial intelligence. Monitor those signals. Pivot the corporate sheet when a clock that applies to this firm moves. Do not pivot because a keynote did.

CQO actions

- Name the failure in the room and write it into the decision log.
- Kill ownerless PoCs and strawman benchmarks; restore the CISO on any stack that moved without a review.
- Keep PQC on the current calendar; challenge QKD proposals that have not survived Bucket D.
- Staff operators beside researchers; refuse a lab lease that has no production path and no exception on record.
- Measure the office by decisions and delivered controls, not by a speaking calendar.
- Reassess the sheet when a clock that applies to this firm moves.

---

26. The CQO as Strategic Translator

The CQO’s job is to translate among quantum science, enterprise architecture, cybersecurity, business strategy, and executive governance. Science produces claims, limitations, and tests. Architecture says what can run inside identity, data, and the classical stack the firm already pays for. Cybersecurity owns operations and the migration build; the CQO keeps the quantum-threat program dated and board-visible. Business units own outcomes. Governance — the council, the CFO’s envelope, the board pack — is where fund, kill, wave, and public-claim decisions are signed.

Translation is operational. Read the limitation section so a vendor cannot own you, then refuse science the firm cannot run. Sit with the CISO on the inventory; leave incident response where it sits. Score the use case

with the owner so the PoC has an end-decision, and leave the build with the teams that already run systems. Brief the board from the log — residual risk, not a belief story.

The companies that win will not necessarily be the ones that “believe in quantum” earliest. They will be the ones that build the capability to evaluate, adopt, secure, and scale quantum technologies rationally. Evaluate: mandate, readiness rank, four-bucket portfolio, Chapter 7 filter. Adopt: a working envelope of honest PoCs and a PQC program that has already started. Secure: inventory coverage, classified critical systems, vendor exit terms, a Chapter 13 list before anyone says production. Scale: only when the receiving team, the fallback, the cost model, and the owner exist — and only on the surface that earned it.

The calendar in this part is how that capability is installed. The first hundred days make the instruments runnable. The next twelve months run both clocks. The scorecard tells the firm whether the office is deciding. The failure list tells the CQO what to kill before it becomes furniture. Hold the translator’s seat, date the work, and let the log — not the tour — speak.

CQO actions

- Hold the translator job in the mandate: science, architecture, security, strategy, and governance.
- Keep that order on the calendar: evaluate before you adopt, secure before you scale. Refuse a skip.
- Communicate residual risk from the decision log.
- Monitor both clocks every quarter.
- Reassess the calendar when a regulator dates a requirement, a classical solver improves, or a governing body starts asking for updates instead of decisions.

About the Authors

Dr. Joe Ghalbouni

Doctor in Quantum Communications from Télécom ParisTech. He works at the intersection of quantum technology, artificial intelligence, and high-performance computing: helping enterprises understand what is coming, what it means for them, and how to turn it into a workable strategic roadmap.

His career runs along three tracks. In academia, he served as Associate Professor of Physics at the Faculty of Sciences of the Lebanese University, where he started a quantum computing research activity. In industry, he spent nearly four years at Point72 Asset Management as Core Innovation Research Lead, directing applied research for finance across quantum computing, post-quantum security, and AI and machine learning. He is also Head of Risk at the Quantum Strategy Institute, a nonprofit that helps enterprises navigate the quantum ecosystem.

He currently runs Ghalbouni Consulting, advising enterprises on the adoption of AI, HPC, and quantum technologies and on the strategic roadmaps that make that adoption durable.

Dr. Oswaldo Zapata

Doctor in Theoretical Physics from Università di Roma Tor Vergata and Master of Science in Particle Physics from Université Paris-Sud. He works at the intersection of quantum technology and finance: helping professionals and institutions understand what's coming, what it means for them, and how to act ahead of their competitors.

His practice runs along two tracks: private training for financial professionals who need to build quantum literacy quickly, and strategic consulting for institutions navigating quantum readiness, cryptographic risk, and the investment opportunity in quantum technologies.

He is Co-Founder of The Quantum Finance Boardroom, a global community connecting quantum technology experts with financial industry professionals. He publishes on the subject for leading organizations such as the CFA Institute, CAIA Association, and Riskmathics Financial Institute.

He has co-authored two books, one for the CFA Institute and Cambridge University Press on quantum and quantitative finance (forthcoming).

References

Numbered entries used as premises. Methods, checklists, scoring weights, and operating-model design are authorial.

Standards & regulators

[1] National Institute of Standards and Technology. *FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard.* Federal Information Processing Standards Publication, published and effective 13 August 2024. https://doi.org/10.6028/NIST.FIPS.203. CSRC: https://csrc.nist.gov/pubs/fips/203/final. PDF: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.203.pdf.

[2] National Institute of Standards and Technology. *FIPS 204, Module-Lattice-Based Digital Signature Standard.* Federal Information Processing Standards Publication, date published 13 August 2024. https://doi.org/10.6028/NIST.FIPS.204. CSRC: https://csrc.nist.gov/pubs/fips/204/final.

[3] National Institute of Standards and Technology. *FIPS 205, Stateless Hash-Based Digital Signature Standard.* Federal Information Processing Standards Publication, date published 13 August 2024. CSRC: https://csrc.nist.gov/pubs/fips/205/final.

[4] National Institute of Standards and Technology. *NIST Releases First 3 Finalized Post-Quantum Encryption Standards.* NIST News, 13 August 2024 (page updated 29 August 2025). https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

[5] Moody, Dustin; Perlner, Ray; Regenscheid, Andrew; Robinson, Angela; Cooper, David. *Transition to Post-Quantum Cryptography Standards.* NIST Internal Report (IR) 8547, Initial Public Draft, November 2024. https://doi.org/10.6028/NIST.IR.8547.ipd. PDF: https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf. Landing: https://csrc.nist.gov/pubs/ir/8547/ipd.

[6] National Institute of Standards and Technology. *What Is Post-Quantum Cryptography?* Created 13 August 2024, updated 27 February 2026. https://www.nist.gov/cybersecurity-and-privacy/what-post-quantum-cryptography.

[7] National Institute of Standards and Technology, Computer Security Resource Center. *Post-Quantum Cryptography (PQC)* project page. Page created 3 January 2017, updated 5 August 2026. https://csrc.nist.gov/projects/post-quantum-cryptography.

[8] Agence nationale de la sécurité des systèmes d’information (ANSSI). *FaQ sur la Cryptographie post-quantique (PQC).* https://cyber.gouv.fr/enjeux-technologiques/cryptographie-post-quantique/faq-pqc/.

[9] ANSSI. *ANSSI views on the Post-Quantum Cryptography transition.* 30 March 2022. “Store now, decrypt later.” https://cyber.gouv.fr/publications/avis-de-lanssi-sur-la-migration-vers-la-cryptographie-post-quantique

[10] European Commission. *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography.* Shaping Europe’s digital future, policy and legislation, 23 June 2025. https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography.

[11] European Commission. *EU reinforces its cybersecurity with post-quantum cryptography.* Press release, 23 June 2025. https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography.

[12] National Security Agency / Central Security Service. *Post-Quantum Cybersecurity Resources.* https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/.

[13] National Security Agency. *CSI: Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) FAQ (December 2024 Update).* Gallery record: U/OO/194427-22, PP-24-4014, December 2024 Ver. 2.1. HTML: https://www.nsa.gov/Press-Room/Digital-Media-Center/Document-Gallery/igphoto/2003071836/.

[14] National Cyber Security Centre (UK). *Timelines for migration to post-quantum cryptography.* Guidance, published 20 March 2025. https://www.ncsc.gov.uk/guidance/pqc-migration-timelines.

[15] National Cyber Security Centre (UK). *Next steps in preparing for post-quantum cryptography.* Paper, originally November 2023, updated August 2024; page publish date 14 August 2024. https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography.

[16] Cybersecurity and Infrastructure Security Agency; National Security Agency; National Institute of Standards and Technology. *Quantum-Readiness: Migration to Post-Quantum Cryptography.* Factsheet, as of 17 August 2023, TLP:CLEAR. https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20(3).pdf.

[17] Cybersecurity and Infrastructure Security Agency. *Post-Quantum Cryptography Initiative.* https://www.cisa.gov/topics/risk-management/quantum.

[18] European Union Agency for Cybersecurity (ENISA). *Cryptography.* https://www.enisa.europa.eu/topics/digital-identity-and-data-protection/cryptography.

Hardware & cloud

[19] IBM Quantum. *Introduction to IBM Quantum services* (IBM Quantum Compute Service / Qiskit Runtime). IBM Quantum Platform documentation. https://quantum.cloud.ibm.com/docs/en/guides/compute-services.

[20] IBM Quantum. *Plans overview.* IBM Quantum Platform documentation. https://quantum.cloud.ibm.com/docs/en/guides/plans-overview.

[21] IBM Quantum. *Processor types.* IBM Quantum Platform documentation. https://quantum.cloud.ibm.com/docs/en/guides/processor-types.

[22] IBM. *Qiskit.* Product page. https://www.ibm.com/quantum/qiskit. Also: https://quantum.cloud.ibm.com/docs.

[23] Amazon Web Services. *What is Amazon Braket?* Amazon Braket Developer Guide. https://docs.aws.amazon.com/braket/latest/developerguide/what-is-braket.html.

[24] Amazon Web Services. *Working with Amazon Braket Hybrid Jobs.* Amazon Braket Developer Guide. https://docs.aws.amazon.com/braket/latest/developerguide/braket-what-is-hybrid-job.html.

[25] Amazon Web Services. *Amazon Braket.* Product page. https://aws.amazon.com/braket/.

[26] Microsoft. *What is Azure Quantum?* Microsoft Learn, `ms.date` 2026-06-17. https://learn.microsoft.com/en-us/azure/quantum/overview-azure-quantum.

[27] Microsoft. *Create an Azure Quantum workspace.* Microsoft Learn, updated 2026-08-13. https://learn.microsoft.com/en-us/azure/quantum/how-to-create-workspace.

[28] Microsoft. *Introduction to Hybrid Quantum Computing.* Microsoft Learn, updated 2026-08-14. https://learn.microsoft.com/en-us/azure/quantum/hybrid-computing-overview.

[29] Google Quantum AI. *Access and authentication.* Cirq documentation. https://quantumai.google/cirq/google/access.

[30] Google Quantum AI. *Google Quantum Computing Service.* Cirq documentation. https://quantumai.google/cirq/google/concepts.

[31] Google Quantum AI. Homepage. https://quantumai.google/.

[32] Google Quantum AI. *Cirq.* https://quantumai.google/cirq.

[33] Xanadu. *PennyLane Documentation* (release 0.45.1 on the page opened in sources-ch09-10). https://docs.pennylane.ai/en/stable/.

[34] Quantinuum. *Getting Started — pytket 2.18.1 API documentation.* https://docs.quantinuum.com/tket/api-docs/getting_started.html.

[35] NVIDIA. *CUDA-Q documentation* (latest). https://nvidia.github.io/cuda-quantum/latest/.

[36] QuEra Computing. *Aquila.* https://www.quera.com/aquila.

[37] Pasqal. *QPUs.* Pasqal documentation. https://docs.pasqal.com/qpu-emulators/qpus/.

[38] Quantinuum. *Quantinuum Systems.* https://www.quantinuum.com/products-solutions/quantinuum-systems.

[39] IonQ. Homepage. https://ionq.com/.

[40] Intel Labs. *Quantum Computing Systems.* https://www.intel.com/content/www/us/en/research/quantum-computing.html.

[41] PsiQuantum. Homepage. https://psiquantum.com/.

Methods & reviews

[42] Preskill, John. *Quantum Computing in the NISQ era and beyond.* Quantum 2, 79 (2018). arXiv:1801.00862. DOI 10.22331/q-2018-08-06-79. https://arxiv.org/abs/1801.00862.

[43] Orús, Román. *A Practical Introduction to Tensor Networks: Matrix Product States and Projected Entangled Pair States.* Annals of Physics 349, 117 (2014). arXiv:1306.2164. https://arxiv.org/abs/1306.2164.

[44] Kjaergaard, Morten; Schwartz, Mollie E.; Braumüller, Jochen; Krantz, Philip; Wang, Joel I-J; Gustavsson, Simon; Oliver, William D. *Superconducting Qubits: Current State of Play.* Annual Review of Condensed Matter Physics 11, 369–395 (2020). arXiv:1905.13641. DOI 10.1146/annurev-conmatphys-031119-050605. https://arxiv.org/abs/1905.13641.

[45] Google Quantum AI. *Suppressing quantum errors by scaling a surface code logical qubit.* Nature (2023). arXiv:2207.06431. https://arxiv.org/abs/2207.06431.

[46] Bruzewicz, Colin D.; Chiaverini, John; McConnell, Robert; Sage, Jeremy M. *Trapped-Ion Quantum Computing: Progress and Challenges.* Applied Physics Reviews 6, 021314 (2019). arXiv:1904.04178. DOI 10.1063/1.5088164. https://arxiv.org/abs/1904.04178.

[47] Saffman, M. *Quantum computing with atomic qubit arrays: confronting the cost of connectivity.* arXiv:2505.11218 (notes finalized summer 2025). https://arxiv.org/abs/2505.11218.

[48] Bluvstein, D., et al. *Logical quantum processor based on reconfigurable atom arrays.* Nature 626, 58–65 (2024). arXiv:2312.03982. DOI 10.1038/s41586-023-06927-3. https://arxiv.org/abs/2312.03982.

[49] Slussarenko, Sergei; Pryde, Geoff J. *Photonic quantum information processing: A concise review.* Applied Physics Reviews (2019). arXiv:1907.06331. https://arxiv.org/abs/1907.06331.

[50] Takeda, Shuntaro; Furusawa, Akira. *Toward large-scale fault-tolerant universal photonic quantum computing.* APL Photonics / perspective (2019). arXiv:1904.07390. https://arxiv.org/abs/1904.07390.

[51] Hauke, Philipp; Katzgraber, Helmut G.; Lechner, Wolfgang; Nishimori, Hidetoshi; Oliver, William D. *Perspectives of quantum annealing: Methods and implementations.* Reports on Progress in Physics 83, 054401 (2020). arXiv:1903.06559. DOI 10.1088/1361-6633/ab85b8. https://arxiv.org/abs/1903.06559.

[52] Burkard, Guido; Ladd, Thaddeus D.; Pan, Andrew; Petta, Jason R.; Taylor, Jacob M. *Semiconductor spin qubits.* Reviews of Modern Physics 95, 025003 (2023). arXiv:2112.08863. DOI 10.1103/RevModPhys.95.025003. https://arxiv.org/abs/2112.08863.

[53] Fowler, Austin G.; Mariantoni, Matteo; Martinis, John M.; Cleland, Andrew N. *Surface codes: Towards practical large-scale quantum computation.* Physical Review A 86, 032324 (2012). arXiv:1208.0928. DOI 10.1103/PhysRevA.86.032324. https://arxiv.org/abs/1208.0928.

[54] IBM. *IBM ILOG CPLEX Optimization Studio.* Product page. https://www.ibm.com/products/ilog-cplex-optimization-studio.

[55] Gurobi Optimization. *Gurobi Optimizer.* Product page. https://www.gurobi.com/solutions/gurobi-optimizer/.

[56] Gurobi Optimization. *Gurobi Optimizer Reference Manual* (v13.0). https://docs.gurobi.com/projects/optimizer/en/current/index.html

[57] NVIDIA. *Introduction — NVIDIA cuOpt (26.08).* https://docs.nvidia.com/cuopt/user-guide/latest/introduction.html

[58] NVIDIA. *cuQuantum SDK* (docs, version 26.06.0 at fetch). Classical GPU simulation, not a QPU. https://docs.nvidia.com/cuda/cuquantum/latest/index.html

[59] Román Orús. *Tensor networks for complex quantum systems.* Nature Reviews Physics 1, 538 (2019). arXiv:1812.04011. https://arxiv.org/abs/1812.04011

[60] S. Kirkpatrick, C. D. Gelatt, Jr., M. P. Vecchi. *Optimization by Simulated Annealing.* Science 220, 4598 (13 May 1983), 671–680. DOI 10.1126/science.220.4598.671. https://hedibert.org/wp-content/uploads/2013/12/1983KirkpatrickGelattVecchi.pdf

[61] Qiming Sun et al. *PySCF: The Python-based Simulations of Chemistry Framework.* arXiv:1701.08223. https://arxiv.org/abs/1701.08223

[62] PySCF documentation. *Density functional theory (DFT).* https://pyscf.org/user/dft.html

[63] Torsten Hoefler, Thomas Häner, Matthias Troyer. *Disentangling Hype from Practicality: On Realistically Achieving Quantum Advantage.* Communications of the ACM 66(5), 82–87 (May 2023). DOI 10.1145/3571725. arXiv:2307.00523. https://arxiv.org/abs/2307.00523

[64] Ryan Babbush et al. *Focus beyond Quadratic Speedups for Error-Corrected Quantum Advantage.* PRX Quantum 2, 010103 (2021). DOI 10.1103/PRXQuantum.2.010103. arXiv:2011.04149. https://arxiv.org/abs/2011.04149

[65] Tomislav Begušić, Johnnie Gray, Garnet Kin-Lic Chan. *Fast and converged classical simulations of evidence for the utility of quantum computing before fault tolerance.* arXiv:2308.05077. https://arxiv.org/abs/2308.05077

[66] V. Černý. *Thermodynamical approach to the traveling salesman problem: An efficient simulation algorithm.* Journal of Optimization Theory and Applications 45, 41–51 (January 1985). DOI 10.1007/BF00940812. https://link.springer.com/article/10.1007/BF00940812.

[67] Edward Farhi, Jeffrey Goldstone, Sam Gutmann. *A Quantum Approximate Optimization Algorithm.* MIT-CTP/4610 (2014). arXiv:1411.4028. https://arxiv.org/abs/1411.4028.

[68] Edward Farhi, Aram W. Harrow. *Quantum Supremacy through the Quantum Approximate Optimization Algorithm.* (2016). arXiv:1602.07674. https://arxiv.org/abs/1602.07674.

[69] G. G. Guerreschi, A. Y. Matsuura. *QAOA for Max-Cut requires hundreds of qubits for quantum speed-up.* arXiv:1812.07589. https://arxiv.org/abs/1812.07589.

[70] Jarrod R. McClean, Sergio Boixo, Vadim N. Smelyanskiy, Ryan Babbush, Hartmut Neven. *Barren plateaus in quantum neural network training landscapes.* arXiv:1803.11173. https://arxiv.org/abs/1803.11173.

[71] M. Cerezo, Andrew Arrasmith, Ryan Babbush, Simon C. Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R. McClean, Kosuke Mitarai, Xiao Yuan, Lukasz Cincio, Patrick J. Coles. *Variational quantum algorithms.* arXiv:2012.09265. https://arxiv.org/abs/2012.09265.

[72] John Preskill. *Beyond NISQ: The Megaquop Machine.* Keynote, Q2B 2024 (11 December 2024); arXiv:2502.17368 (February 2025). DOI 10.1145/3723153. https://arxiv.org/abs/2502.17368.

[73] Ryuji Takagi, Suguru Endo, Shintaro Minagawa, Mile Gu. *Fundamental limits of quantum error mitigation.* arXiv:2109.04457. https://arxiv.org/abs/2109.04457.

[74] Feng Pan, Pan Zhang. *Simulating the Sycamore quantum supremacy circuits.* arXiv:2103.03074. https://arxiv.org/abs/2103.03074.

[75] Thomas Lubinski, Sonika Johri, Paul Varosy, Jeremiah Coleman, Luning Zhao, Jason Necaise, Charles H. Baldwin, Karl Mayer, Timothy Proctor, and the QED-C TAC on Standards and Performance Benchmarks. *Application-Oriented Performance Benchmarks for Quantum Computing.* arXiv:2110.03137. https://arxiv.org/abs/2110.03137.

[76] Thorsten Koch, David E. Bernal Neira, Ying Chen, Giorgio Cortiana, Daniel J. Egger, et al. *Quantum Optimization Benchmarking Library: The Intractable Decathlon.* arXiv:2504.03832. https://arxiv.org/abs/2504.03832.

[77] Maria Schuld, Nathan Killoran. *Quantum machine learning in feature Hilbert spaces.* Phys. Rev. Lett. 122, 040504 (2019). arXiv:1803.07128. https://arxiv.org/abs/1803.07128.

[78] Vojtěch Havlíček, Antonio D. Córcoles, Kristan Temme, Aram W. Harrow, Abhinav Kandala, Jerry M. Chow, Jay M. Gambetta. *Supervised learning with quantum-enhanced feature spaces.* Nature 567, 209 (2019). arXiv:1804.11326. https://arxiv.org/abs/1804.11326.

[79] Yunchao Liu, Srinivasan Arunachalam, Kristan Temme. *A rigorous and robust quantum speed-up in supervised machine learning.* arXiv:2010.02174. https://arxiv.org/abs/2010.02174.

[80] Hsin-Yuan Huang, Michael Broughton, Masoud Mohseni, Ryan Babbush, Sergio Boixo, Hartmut Neven, Jarrod R. McClean. *Power of data in quantum machine learning.* arXiv:2011.01938. https://arxiv.org/abs/2011.01938.

Authorial (no citation required)

Threat-model sort; PQC program tables and vendor questionnaire; crypto-agility / CBOM as an operational object (not claimed as a named CISA/NIST specification); QKD fit/not-fit assessment; QRNG as a component; procurement playbook and three pillars; counsel brief; three education tracks; 100-day calendar; 12-month deliverable list; KPI table; failure-mode list; conclusion.
