EXECUTIVE BRIEFING . AUGUST 2026

The CEO's Role in *Quantum Resilience*

A short note for chief executives in regulated and critical sectors.

Quantum resilience is a strategic risk, not an IT project. Encrypted data stolen today can be read once a sufficiently capable quantum computer exists, so the exposure clock is already running on anything that must stay confidential for years. Deciding which data that is, and what to spend protecting it, is a call only the chief executive and the board can make.

The CEO's role is direction, accountability and resourcing rather than technical selection. Six actions cover it.

1. **Set the deadline.** Regulators publish target dates[1]; the UK NCSC sets 2035 for completed migration. Adopt an organisational date, put quantum risk on the enterprise risk register and hold the executive team to the timeline.
2. **Name a single accountable owner[2].** Usually the CISO or CTO, with CEO sponsorship, a mandate that crosses IT, procurement, legal and product, and a sustained multi-year budget line. Shared ownership without a single owner delivers a slide deck, not a programme.

---

[1] CEOs of multinational organisations should note that so far authorities in 17 countries have published milestones for quantum migration. Many countries distinguish between the deadlines for critical sectors and others. Countries like France have different regimes.

[2] If you are responsible for a multinational business, a hub-and-spoke approach to quantum resilience is likely to optimise your RoI.

3. **Fund discovery before migration.** Commission a cryptographic inventory across cloud[3] and on-premises estates before approving migration spend. Classify data by how long it must stay confidential and move the longest-lived assets first.
4. **Demand cryptoagility, not a one-off swap.** The measure of success is the ability to replace algorithms again without another multi-year programme. This is the resilience capability regulators are likely to test.
5. **Push the requirement into the supply chain.** Require written quantum-readiness roadmaps and the contractual right to change algorithms from cloud providers, vendors and critical partners. New purchases should contain quantum readiness provisions. France is asking for this from 2027 for new security products entering its national certification process.
6. **Measure progress and communicate posture.** Review a small set of indicators at board cadence: systems inventoried, systems migrated, supplier commitments secured. Communicate the posture to customers, regulators and insurers; it is now a trust and due-diligence question.

> *The CEO sets the deadline, names the owner, funds the inventory and treats quantum resilience as operational resilience.*

About Santosh Pandit

Santosh Pandit is the Founder of BeatQuantum. He is a former regulator from the Bank of England, Prudential Regulation Authority and Board Director of subsidiaries of the BNP Paribas Group. He is an Advisory Board Member of Cyber London's Quantum Security Think Tank and an Executive Fellow of the Digital Growth Collective. Santosh's topics of expertise include cyber and operational resilience, frontier AI defences and quantum security.

About BeatQuantum

BeatQuantum is the world-leading centre of excellence for applied post-quantum cryptography and technology resilience. As of August 2026, the BeatQuantum platform has already implemented the post-quantum cryptography that businesses aspire to reach by 2030 to 2035. This gives BeatQuantum the confidence to provide credible and pragmatic advice to boards, C-suites and CROs and CISOs at regulated businesses and critical national infrastructure. Its motto, "Prove First, Speak Later", is a working method as well as a slogan.

---

[3] Cloud service providers operate a model of shared responsibility, and therefore your organisation's ownership of quantum resilience is inevitable. Your contracts with those who manage services on your behalf are unlikely to include quantum migration either. Please ask your COO / Procurement Head.