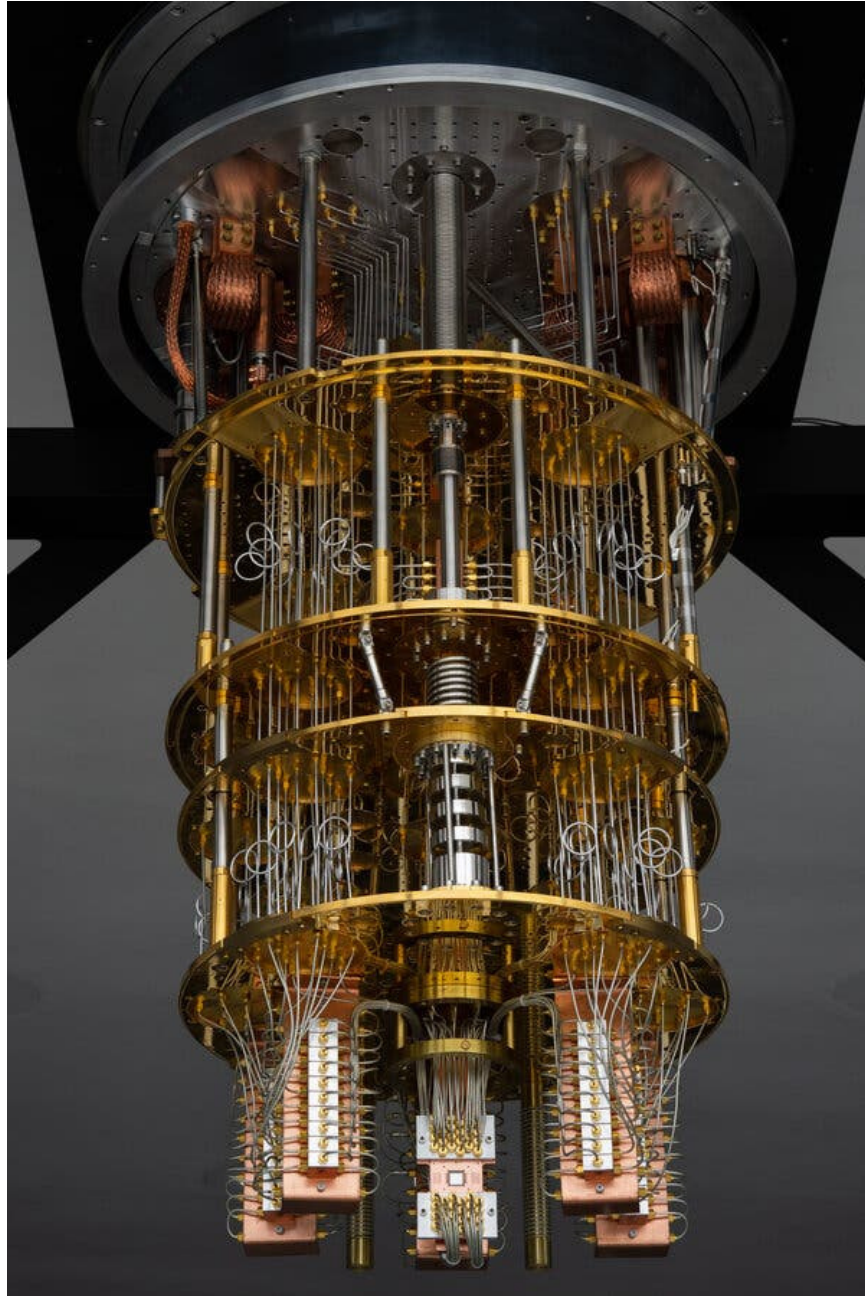


# QUANTUM READY, ARE YOU?



Ray Quattromini – MD  
01256-331614

[ray@fortunadata.com](mailto:ray@fortunadata.com)

<https://www.fortunadata.com>

Published October 2026

During my decades of experience working in the IT industry, it is more exciting now than all the previous years. We are now on the cusp of the next industrial revolution with the global adoption of AI and Quantum computing and this is the primary reason I am writing this article, not because the good it will bring to humanity but the issues organisations will face unless they start to act now.

The idea of a Quantum computer was first introduced by physicist Paul Benioff in 1980! Today his vision is here with global companies and governments having fully operational Quantum technology. There are a number of hurdles to overcome to make them commercially viable, but these things are gradually being addressed. Once these technical issues are solved organisations and governments will be able to buy, own or lease a Quantum computer.

Nuclear Fusion to power cities is realistically probably 20 years away. Commercially viable Quantum computing isn't 20 years away! Within the next 5-10 years, Quantum computing will be here. They will be used for all sorts of things and some of these industries are shown below.

### **How can Quantum computing help humanity survive?**

They will be used by a number of organisations for all the following and many more.

- Molecular and Drug Discovery
- Clean Energy and Agriculture
- Optimisation and Planning Logistics
- Cybersecurity and Encryption
- Metallurgy
- Communications
- Global GPS (no need for satellites)

### **Technology Today**

Quantum proof technologies aren't just about the data storage, it's the encryption, firewalls, networking equipment, software and security. In my opinion this is a bigger (and real) problem than the year 2000 debacle and yet we are not hearing much about it. Unlike Y2K there was a rush to "rip and replace", with Quantum it's more of a ripple and very few understand or know about the impact it could have.

Unless you are a government or financial organisation already embarking on a Quantum journey, it is unlikely that your organisation isn't or hasn't thought about the potential cost Quantum computing could pose to your organisation. It is fair to say that 99% of organisations have no Quantum technology or haven't thought about it.

For example, traditional encryption algorithms such as RSA-256, RSA-2048, ECC, DSA and many others are not Quantum safe including the security standards FIPS-2, FIPS-3.

### **Which brings me to why I am writing this article**

This isn't an article about "What is a Qubit", it's an article about why global organisations need to be "**Quantum Ready**".

Quantum computing is here now and working in labs, solving problems that would take a traditional computer thousands of hours or years to solve, Quantum solves these problems in minutes or hours.

The document with links at the bottom of the article "**Transition to Post-Quantum Cryptography Standards (PQC)**" highlights the threats and identifies the types of encryption organisations require to mitigate the threats Quantum computing brings.

The EEC states that member states must start the migration to Quantum computing by the end of 2026, which isn't that far away. If global governments are starting to act, why aren't organisations?

### **What would I do now?**

I would put an immediate stop to purchasing IT technology that isn't "Quantum Ready"! Yes, this might be painful as you could be midway through a rollout, but it would be far better to take stock of what's happening than regretting things later.

### **My data is encrypted**

This is a typical stance and whilst it's a tick box for auditors and security professionals. A Quantum computer would break that encryption within hours or days, once large-scale quantum computers exist. There are globally, data storage silos storing petabytes of hacked data that is encrypted. Criminals and governments are storing this data in the knowledge that one day Quantum technology will be able to break this encryption and open a pandoras box of information.

### **What should I do?**

Quantum is coming faster than anyone imagined. Global financial institutions must be Quantum secured by 2035. They must start to undertake a Quantum study by 1<sup>st</sup> January 2027 and show that by 2030 they have embarked on procuring Quantum safe technologies. The problem is large financial institutions to embark on these projects typically takes 10-20 years which by my earlier estimation is well past the date when Quantum will be here.

If governments and financial institutions are worried about Quantum technology how comes this messaging isn't being directed to global organisations today?

We all love the cloud. If I were an unscrupulous organisation or government, I would target the cloud providers first as they hold Zettabytes of data from millions of companies around the globe.

The cloud providers are not protecting your data; they are offering you a convenient place to store it. The data is your responsibility and how you protect, backup and secure that data is your problem not theirs. The recent attacks that happened in the Middle East highlighted the issue, where organisations were storing data in the cloud and the attacks caused many organisations to lose their information, gone forever.

As an organisation I would examine the types of data held in the cloud and identify with a weighting if this data is a security risk. If it is I would bring this data back on premise and secure it in a secured environment and maybe store the data on tape on a shelf.

I would create a datacentre, this could now be a broom cupboard or storeroom, due to the amount of data we can cram onto hard drives and flash storage taking up much less space than 5-10 years ago.

### **Hacking and Ransomware**

We all understand that the ongoing and increasing threat from hacking and ransomware is on the rise. The thefts of data are enormous, and this leads to a strategy called "**harvest now, decrypt later**": groups, mostly state-backed, steal encrypted data today and store it until they can decrypt it.

These organisations are stealing all types of data storing it in large data silos and tapes waiting for the time Quantum can unlock the encryption keys this is exactly what "harvest now" targets. The fix already exists. In 2024, the US standards body NIST published **post-quantum cryptography** standards, and the UK's NCSC is urging organisations to migrate over the next several years.

## The Quantum Discussion

Over the years I have worked with many organisations from buying a simple NAS to designing a complete data centre refresh. Any IT project takes time, for any organisation to realistically start looking at the quantum threat and everything involved is a huge undertaking.

## The Global Supply Chain Problems

In 2026, the global semiconductor supply chain is experiencing a structural crisis. Unlike previous cyclical downturns, this shortage stems from an explosion in AI computing demand, placing simultaneous pressure on four core components: CPUs, GPUs, memory, and data storage. The impact has spread from data centres to consumer electronics, automobiles, and the broader economy.

Memory sits at the epicentre. AI data centres' demand for High Bandwidth Memory (HBM) has fundamentally reshaped the memory industry. HBM is far more complex to manufacture than standard DRAM, and only three suppliers can produce it at scale, making supply inherently constrained. Memory makers have shifted capacity toward higher-margin HBM, causing consumer-grade DRAM and NAND flash supply to shrink sharply. According to J.P. Morgan research, DRAM prices have risen 400% from early 2024 through the end of 2026. Some DRAM products have already surged to more than ten times their January 2025 levels, while Omdia forecasts the DRAM market value will nearly double in 2026 and beyond, with NAND potentially quadrupling.

CPUs have shifted from supporting role to bottleneck. The rise of agentic AI has changed computing architecture; AI data centres are moving from the traditional "eight GPUs per CPU" configuration toward a more balanced 1:1 ratio. This shift has caused CPU demand to spike, while TSMC's 3nm capacity has been fully booked by customers including NVIDIA, AMD, Broadcom, and Apple. Intel has implemented two rounds of price increases in 2026, and AMD's server chip prices have risen 16% to 17% cumulatively. Server CPU lead times have stretched from a typical one to two weeks to six months. Acer Chairman Jason Chen noted that CPUs have become the most severe shortage in the PC supply chain.

For GPUs, the bottleneck isn't manufacturing, it's packaging. NVIDIA's data centre GPU lead times run 36 to 52 weeks, and Rubin chips aren't commercially available until 2028 due to manufacturing delays. The real constraint is TSMC's CoWoS advanced packaging capacity, which is fully booked for all of 2027-2028, with NVIDIA alone securing roughly 60% of capacity through 2027. MSI has warned that GPU shortages will persist through the end of 2027, with RTX 50 series graphics card supply already dropping by 50%.

Data storage faces the same squeeze. NAND flash prices are climbing alongside DRAM, and Gartner estimates combined DRAM and SSD prices are continuing to rise 10-15% QoQ. Seagate and Western Digital have warned that their hard drive products are completely sold out for 2027. An Omdia survey of IT infrastructure leaders found that 87% of respondents said memory and storage price increases have moderately or severely impacted their IT budgets, while 74% said shortages are delaying their on-premises AI infrastructure deployments.

The essence of this supply constraint is a structural mismatch in capacity. The top five hyperscale cloud providers will spend roughly \$1.4 trillion in capital expenditure in 2027, about twelve times more than in 2022, while hardware suppliers' capital spending has grown only about 50%. Demand is outpacing supply elasticity, and there is no short-term fix. Most analysts believe relief will not arrive until at least 2028/29. In the meantime, from smartphones to cars, from PCs to cloud services, rising costs and delivery delays will become the norm for the global technology industry.

## The Procurement Process

As mentioned previously with AI consuming the global supply of CPU's, GPU's, memory and data storage and a roadmap out 5 years. Any equipment ordered today is taking on average 18 months to 2 years to deliver. Joining an ever-expanding queue in a global supply chain problem.

In the past organisations ordered a storage chassis and sweated the asset for 5-10 years, knowing that they could buy spare drives, fans or power supplies. This is no longer the case as you can't buy new drives from any vendor unless they are refurbished and even these are becoming scarce.

## Selecting The Right Technology

Having dealt and spoken with 100's of organisations over the years, they all have their preferred vendor. This could be because of vendor relationship, reliability, features, functionality, price etc. Here is a scenario based on what you have read here, Googled and fact checked.

Your organisation is about to invest £1m on a new storage array that will typically last 5-10 years as you sweat the asset.

The storage array:

- Manufacturer (A) is your choice for £1m, but this doesn't have "Quantum Ready" functions or functionality.
- Manufacturer (B) does have "Quantum Ready" functions and functionality, but the price is £1.3m.

Reading and understanding what you have read here, would this influence your organisation enough to change your purchasing decision to be Quantum compliant in 2026/27, knowing that these storage systems are available today?

You could spend the £1m today then spend £1.3m in 5 years when your technology refresh comes around, but is this the smart choice?

## Quantum & AI

AI is here and is already being used on the desktop, mobile phone, and for back-office tasks and intrusion detection systems. Quantum is further away and its impact is hard to understand now.

The combination won't flip a switch - it will arrive in stages, and the biggest near-term disruption is not "sentient super-AI" but the quiet collapse of today's encryption. And yes, criminals are already positioning for it, though mostly in ways that don't require a quantum computer yet.

## Further links and information to digest

Below is the timeline outlined by “G7 Cyber Expert Group”

### Phased Approach:

- **2025 - 2027:** Increase quantum threat awareness, map critical systems, and identify sensitive data.
- **2025 - 2028:** Build extensive inventories of software, hardware, and third-party vendor dependencies.
- **2026 - 2029:** Commence migration planning and pilot implementations for high-priority or non-critical systems.
- **2027 - 2034:** Execute progressive, enterprise-wide migration to quantum-resistant algorithms.

Below is a link titled “Transition to Post-Quantum Cryptography Standards” published by

National Institute of Standards and Technology (NIST) - is a non-regulatory federal agency within the U.S. Department of Commerce that develops technology, metrics, and standards to promote innovation and industrial competitiveness

<https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

<https://www.ncsc.gov.uk/paper/preparing-for-quantum-safe-cryptography>

<https://www.gov.uk/government/publications/advancing-a-coordinated-roadmap-for-the-transition-to-post-quantum-cryptography-in-the-financial-sector/g7-cyber-expert-group-statement-on-advancing-a-coordinated-roadmap-for-the-transition-to-post-quantum-cryptography-in-the-financial-sector-january-20>

## Summary: How Fortuna Data can help you become Quantum Ready

Quantum readiness isn't a single purchase. It's a journey of many years, and the IT equipment you buy today will either help it or hold it back for the next decade. Fortuna Data can supply the equipment and infrastructure your business needs to become Post-Quantum Cryptography (PQC) ready. We've done this work for years, from a single NAS to a full datacentre refresh.

1. **Equipment that is PQC ready.** We can supply storage arrays, servers, networking and security equipment that support the NIST post-quantum standards (FIPS 203, 204 and 205). We choose equipment that is crypto-agile, so it can take new encryption standards as they arrive. The equipment you put in now will still protect you in 2035, so you don't have to pay twice.
2. **Know what you hold and where it lives.** We can help you review the data you store on premise, in the cloud and on backup media. Together we can rank it by sensitivity and by how long it must stay secret. That shows which data is most exposed to "harvest now, decrypt later" attacks, and where new infrastructure should go first.
3. **Bring critical data back under your control.** For data too sensitive to leave with a third party, we can design and supply secure on-premise infrastructure. That could be a full datacentre or a small, high-density room. We can also supply offline, air-gapped LTO tape. Tape on a shelf can't be reached over a network, which makes it one of the strongest defences against ransomware and data theft.
4. **Buy with confidence.** We help you separate real PQC capability from marketing claims. We check which standards each product actually supports, how it works with your current systems, and whether the vendor has a credible roadmap. Your money goes on equipment that meets the NCSC and NIST deadlines.
5. **Work around the supply chain crisis.** Drives, memory, CPUs and storage arrays now take many months to arrive. Our supply network helps you plan purchases early and find stock that's available. We can also keep your existing systems running safely during the move to PQC, with spare parts, maintenance and options to extend their life.
6. **Expert consultancy for every step of your journey.** Many organisations don't know where to start with quantum readiness, and the skills to deliver it are in short supply. Fortuna Data offers consultancy to guide you from the first conversation to the final migration. We can assess where you are today, help build your cryptographic inventory and identify your highest-risk data and systems. From there we can help you create a phased roadmap in line with the NCSC and NIST deadlines

Large organisations will need many years to get there, so the time to start is now. **Talk to Fortuna Data about the equipment and infrastructure you need to become PQC ready.**

## Planning and Procuring Quantum-Ready Solutions: A Strategic Guide for Large Multinationals

### Executive Summary

For a large multinational, achieving quantum readiness is not a single IT project but a multi-year strategic programme requiring executive sponsorship, cross-functional coordination, and careful supply-chain management. The journey spans four phases, Discovery and Assessment, Strategic Planning and Policy, Procurement and Vendor Evaluation, and Implementation and Validation underpinned by external regulatory deadlines that set hard boundaries and internal complexity that dictates the realistic pace of delivery. The consensus is that a full migration for an organisation of this scale will likely span 12 to 15 years or more, meaning planning must begin immediately.

### Part 1: The Four-Phase Journey

#### Phase 1: Discovery and Assessment (Build Your Foundation)

Before you can plan, you must know exactly what needs protecting. This phase is about building a comprehensive picture of your cryptographic landscape.

- **Appoint an Owner and Secure Sponsorship:** Assign a single accountable leader for the PQC transition, reporting to your CISO or CTO. A strong senior sponsor is critical for securing budget and driving change across the organisation.
- **Conduct a Cryptographic Inventory (Discovery):** This is the foundational step. You must identify where and how cryptography is used across your estate, including data in transit, at rest, and in execution. Use automated discovery tools where possible to build a Cryptographic Bill of Materials (CBOM), but also account for legacy, air-gapped, and undocumented systems.
- **Assess Risk and Prioritise Assets:** Not all data is equal. Identify which data is most sensitive, business-critical, or long-lived. Systems protecting data with a long secrecy lifetime are most vulnerable to "Harvest Now, Decrypt Later" (HNDL) attacks, where adversaries steal encrypted data today to decrypt it later with a quantum computer.

#### Phase 2: Strategic Planning and Policy (Define Your Path)

With a clear picture of your assets, you can create a realistic roadmap and set the rules for procurement.

- **Build a Phased Migration Roadmap:** Align your plan with recognised timelines, such as the UK NCSC's guidance to complete an initial plan by 2028 and finish migrating highest-priority systems by 2031. Your roadmap should sequence work based on risk and system complexity.
- **Set Procurement Policy Floors:** Update your procurement policies immediately. Require new hardware and software purchases to support PQC. For critical suppliers, you may need to require a minimum maturity level, such as a credible roadmap for NIST-standardised algorithms or third-party assessment for business-critical vendors.
- **Engage Your Supply Chain Early:** Your quantum readiness is dependent on your vendors. Engage key suppliers (especially cloud, identity, VPN, HSM, and SaaS providers) to understand their PQC roadmaps. Make your requirements known to influence their development cycles.

#### Phase 3: Procurement and Vendor Evaluation (Select Your Partners)

When it is time to buy, you need to ask the right questions to separate genuine capability from marketing.

- **Build a Detailed RFP:** Go beyond a simple "do you support PQC?" question. A robust RFP should cover discovery capability, support for specific NIST standards (like FIPS 203/204/205), hybrid modes, HSM integration, and audit-ready evidence trails.

- **Verify Vendor Claims:** Ask vendors to name the specific FIPS standards and parameter sets they implement. Be wary of "PQC mode" that is simply a wrapper over existing RSA. For critical infrastructure, look for vendors using multiple independent libraries for cross-verification.
- **Use Formal Maturity Models:** Consider adopting a framework like the PQC Maturity Model (PQCMM) to formally score and track supplier readiness. This turns a one-off procurement decision into an ongoing supply-chain control.

#### **Phase 4: Implementation and Validation (Deploy and Verify)**

Once solutions are selected, the focus shifts to integration and proving it works.

- **Prioritise Implementation:** Begin deploying PQC solutions for your highest-priority assets identified in Phase 1. Plan for parallel operation where classical and PQC systems must coexist during the transition period.
- **Validate Interoperability and Performance:** Before full rollout, test PQC implementations for interoperability with your existing systems and third parties. Benchmark performance, as some PQC algorithms are more computationally intensive than their classical counterparts.
- **Update Inventory and Monitor:** As you deploy, update your cryptographic inventory to reflect the new status of each system. Establish continuous monitoring to ensure PQC remains correctly implemented and to track future algorithmic developments.

### **Part 2: Timeframes for a Large Multinational**

For a large multinational, the timeframes involved are driven by both external regulatory deadlines and the internal reality that these transitions take many years.

#### **Regulatory and Industry Deadlines**

These external timelines set the hard boundaries your organisation will need to work towards. The most influential are from the US NIST and UK NCSC.

##### **United States (NIST & NSM-10)**

- **Deprecation Deadline (2030):** Algorithms like RSA-2048 and ECC P-256 are no longer suitable for new deployments.
- **Full Phase-out (2035):** Quantum-vulnerable algorithms are disallowed for federal systems.
- **National Security Systems (2027):** NSA's CNSA 2.0 requires new NSS products to support quantum-resistant algorithms by January 2027.

##### **United Kingdom (NCSC)**

- **Plan Complete (2028):** Finish an initial migration plan covering your entire estate.
- **High-Priority Migration (2031):** Migrate your highest-priority services and refine the initial plan.
- **Full Migration (2035):** Complete migration for all systems, services, and products.

#### **Internal Reality for a Multinational**

The external dates are the target, but the internal complexity of a large organisation dictates the actual journey. Industry analysis suggests that for large, distributed environments, a realistic baseline timeline is 12 - 15+ years.

This extended timeframe is a result of several factors unique to multinational scale:

- **Massive Attack Surface:** The cryptographic attack surface has grown 10 - 100× since the last major migration (e.g., SHA-1 to SHA-2), due to APIs, microservices, containers, IoT, and edge devices.
- **Low Visibility:** A significant portion (estimates range from 40 - 60%) of cryptographic use in large enterprises is undocumented, often hidden in third-party platforms, SaaS, and cloud dependencies.
- **Vendor Dependency:** Your timeline is inextricably linked to your supply chain. Migration often depends more on vendor roadmaps for hardware, firmware, and software than on internal engineering work.
- **Resource Constraints:** There is a severe global skills shortage; 97% of organisations report significant PQC-related skills gaps, which will constrain implementation capacity.

### Part 3: Key Considerations and Strategic Implications

Regardless of where you are in the journey, several principles should guide your approach.

- **Crypto-Agility:** Design your systems to allow for easy replacement of cryptographic algorithms in the future. This ensures you can adapt quickly if a current PQC standard is ever broken or a new one is introduced.
- **Budget for Multi-Year Effort:** PQC migration will span multiple budget cycles. Use the phased roadmap to build a business case that spreads costs over time and highlights the long-term risk of delay.
- **Leverage Managed Services:** For many SMEs, the transition will be handled by their existing service providers. For larger organisations with bespoke systems, the effort will be more significant and may require specialist consultancy.
- **Start the Foundational Work Now:** Given the multi-year horizon, the most critical action for a multinational is to start the technology-agnostic work immediately. This includes building a comprehensive cryptographic inventory, developing crypto-agility in your systems, and engaging your supply chain to understand their roadmaps. Delaying this planning work compresses the implementation timeline, leading to higher costs, resource scarcity, and less flexibility.

### Summary Timeline at a Glance

