WHITEPAPER

Post-Quantum Readiness for Regulated Industries

Financial services, healthcare, and government each carry different data-longevity requirements and regulatory expectations — and that changes what "ready" actually means for each.

Why Sector Context Changes Everything

Post-quantum readiness is often discussed as a single, generic problem, but the right level of urgency and the right migration priorities differ substantially by sector — driven primarily by how long the data an organisation holds actually needs to stay confidential, and what a regulator will expect to see if asked. Generic advice tends to under-serve organisations with genuinely long data-longevity requirements and over-alarm those without them.

Financial Services

Banking and financial services hold transaction, account and Know-Your-Customer records that frequently require confidentiality across decades, alongside real-time payment infrastructure where availability and interoperability during any migration are non-negotiable. The sector also faces some of the most active regulatory attention on this topic globally, with supervisory bodies increasingly asking institutions to demonstrate cryptographic inventory and migration planning, not just intent.

Priority areas typically include payment gateway TLS, HSM-protected signing keys for transaction authorisation, and long-term archival systems holding historical customer data.

Healthcare

Patient records commonly require protection for the patient's lifetime, and in many jurisdictions considerably longer. Healthcare environments also carry a distinct operational constraint: a large installed base of medical devices and clinical systems with long refresh cycles and limited cryptographic configurability, which makes network-level and gateway-level mitigation strategies disproportionately important compared with sectors that can update application code more freely.

Priority areas typically include electronic health record systems, any interoperability APIs exchanging patient data externally, and long-term clinical archives.

Government and Defence

Classified and sensitive government information can require confidentiality for fifty years or more, placing this sector at the sharpest end of the “harvest now, decrypt later” risk of any vertical. This is also the sector where national algorithm-suite guidance — such as the US National Security Agency’s CNSA 2.0 timeline — most directly applies, alongside equivalent guidance from bodies like the UK’s NCSC, giving government organisations a more prescriptive external timeline than most other sectors currently have.

What’s Common Across All Three

Despite the differences, the starting point is identical everywhere: none of these sectors can prioritise correctly without first knowing where cryptography actually exists in their environment. A financial institution, a hospital network, and a government agency all need the same foundation — a current, accurate CBOM — before sector-specific prioritisation is even possible. The differences show up in what gets prioritised first and how fast, not in whether discovery comes first.

© 2026 Quantum Sentinel™. All rights reserved.
Registered as a limited company in England and Wales under company number: 17317113. Registered office: 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ, United Kingdom.