

You cannot migrate cryptography you cannot see.

Every bank knows it will have to move to post-quantum cryptography. Almost none can answer the first question a regulator will ask: **which algorithms are you running, in which systems, protecting what**. That inventory does not exist, because no scanner has ever produced it — they look for vulnerabilities, not for cryptography.

THE PROBLEM

01

The data is already taken

Encrypted traffic is being captured now to be decrypted later, when the hardware exists. Anything that stays sensitive for a decade — mortgages, KYC files, payment records — is already exposed by today's RSA and elliptic-curve cryptography.

02

Nobody has the inventory

Cryptography is not in a register. It is a line in a library, a TLS cipher list, a curve name in a config file, a hardcoded algorithm in a twelve-year-old service. It cannot be surveyed by asking people.

03

Migration takes years

Replacing an algorithm means finding every use, judging which matter, and changing them without breaking payments. Institutions that start when the mandate lands will start several years too late.

WHAT 0DQ DOES

- **Quantum readiness**

Every algorithm, where it is used, and what it protects

- **Secrets**

Credentials committed and still live

- **Dependencies**

Known vulnerabilities, with the path that reaches them

- **Infrastructure**

Misconfiguration in what you deploy onto

- **Code**

Insecure patterns in the source itself

- **Licences**

Obligations you have taken on unknowingly

Five of these you already have. **The first one you do not**. 0dq produces a cryptographic bill of materials from your source code — the inventory a post-quantum programme starts with — and scores it beside the five findings types your existing tools report, as one number with the arithmetic shown.

WHY THIS IS A BOARD QUESTION NOW

- **The standards are final.** NIST published ML-KEM, ML-DSA and SLH-DSA in August 2024. The algorithms to migrate to are no longer in question.
- **CBUAE already regulates cryptography.** Cryptography and key management are named control domains under the Information Security Regulation and the Operational Risk Standard, which apply to every licensed institution.
- **Post-quantum guidance is expected.** UAE authorities are widely anticipated to require a PQC migration roadmap. A roadmap begins with an inventory.

Operational resilience is the ability to keep critical services running, and to evidence it. **An institution that cannot say which cryptography protects which service cannot evidence either its resilience or its migration.**

Point 0dq at a repository and it answers in minutes. No agent, no integration project, no change to how your teams work — connect GitHub and read the first cryptographic bill of materials your organisation has ever had.