

SafeCipher CBOM Audit Service

Building Quantum-Ready Cryptographic Resilience for the Enterprise

Why Cryptographic Visibility Matters

Cryptography underpins every secure digital transaction — from banking APIs and payment platforms to IoT and cloud workloads. Yet most organizations don't fully know what cryptography they use, where it resides, or whether it's compliant or quantum-safe. A Cryptographic Bill of Materials (CBOM) provides complete visibility and control, identifying vulnerabilities, ensuring compliance, and preparing for the post-quantum era.

What Is a CBOM?

A CBOM is a structured inventory of all cryptographic components — algorithms, libraries, keys, certificates, HSMS, and trust chains. It answers critical questions such as which algorithms protect data, whether they are quantum-vulnerable, and whether systems can support post-quantum or hybrid cryptography.

SafeCipher CBOM Audit – How It Works

- 1. Discovery & Inventory** — Identify cryptographic assets across codebases, APIs, HSMS, and KMS systems.
- 2. Analysis & Risk Classification** — Assess compliance, quantum vulnerability, and lifecycle weaknesses.
- 3. Quantum Readiness Evaluation** — Test readiness for FIPS 203 (ML-DSA) and FIPS 204 (ML-KEM), hybrid cert chains, and HSM firmware compatibility.
- 4. Roadmap & Recommendations** — Deliver a tailored remediation and migration plan aligned with compliance and resilience objectives.

Deliverables

- Comprehensive CBOM Inventory Report (JSON/Excel/Dashboard)
- Cryptographic Risk Register with severity ratings
- Quantum Readiness Assessment Report
- Remediation and Migration Roadmap
- Optional GRC and DevSecOps integration

Who Benefits

- Banks & Financial Institutions — meeting ECB and BaFin post-quantum mandates.
- Cloud and SaaS Providers — maintaining trust and compliance in hybrid environments.
- Government & Defense Agencies — ensuring cryptographic sovereignty.
- Critical Infrastructure Operators — addressing OT/IT crypto lifecycle visibility.

Why SafeCipher

- Vendor-Neutral Expertise across Azure, AWS, GCP, and on-prem environments.
- Quantum-Focused Approach leveraging FIPS 203/204 and PKI Consortium guidance.
- Proven Migration Experience implementing PQC pilots with zero downtime.
- Trusted by International Agencies and Financial Institutions worldwide.

Start Your Quantum Journey

Don't wait for the quantum era to force change — build cryptographic resilience now. Contact SafeCipher to schedule your CBOM Audit Assessment and ensure your organization's cryptography is visible, compliant, and quantum-ready.

■ help@safecipher.com

■ www.safecipher.com

■ Your Partner in Cryptographic Assurance and Quantum Transition