EUROPEAN SBOM USER GROUP

CBOMs in the PQC process

Cryptographic Bill of Materials

Overview, missing evidence and next steps - oej@edvina.net 2026-10-29

PQC creates a long transition

Confidentiality can be at risk before migration finishes

Information lifetime	Captured ciphertext may remain valuable for many years (Harvest now, decrypt later)
Migration lead time	Products, peers and providers must change together
Different security purposes	Confidentiality, authentication and signing need separate assessments

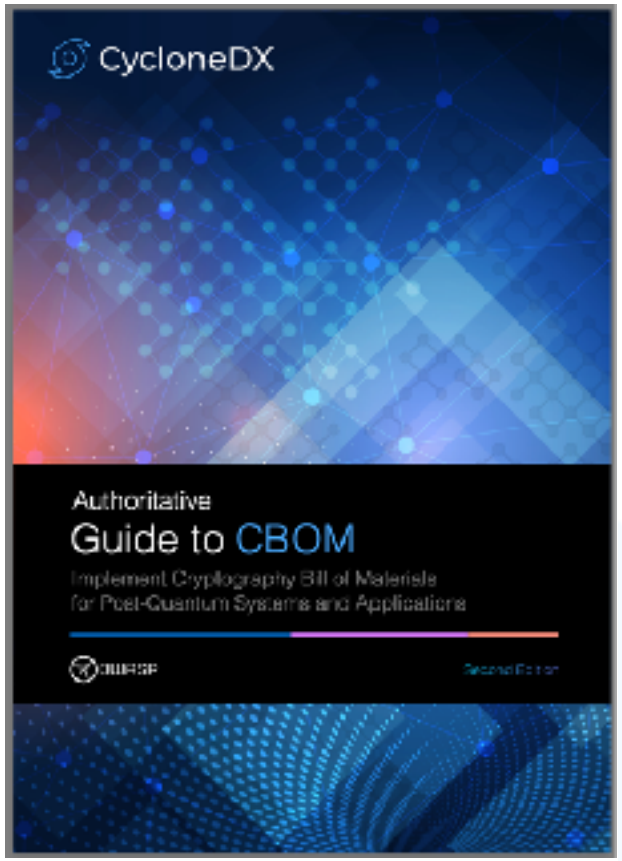
Long-lived sensitive information deserves early attention

What a CBOM contributes

An inventory of cryptographic assets and relationships

Assets	Algorithms, protocols, certificates and key metadata
Usage	The software, services and protection purposes involved
Evidence	Where each claim came from, its scope and its age

Useful decisions require context, ownership and explicit unknowns



Structure and Cryptographic Asset Types

Component (type = cryptographic-asset)

Crypto Properties

- Algorithm Properties
- Certificate Properties
- Protocol Properties
- Related Crypto Materials Properties

Public Key	Key	Salt	Credential	Password	Ciphertext
Private Key	Digest	Shared Secret	Token	Signature	Seed
Secret Key	Initialization Vector	Tag	Additional Data	Nonce	Other

https://cyclonedx.org/guides/

CBOMs throughout PQC migration

01	02	03	04	05
Scope	**Discover**	**Prioritize**	**Migrate**	**Verify**
Systems, data and owners	Asset evidence	Risk and dependencies	Test and coordinate	Observe and refresh

The inventory evolves with each deployment and migration

Evidence answers different questions

Implemented	What the software contains or can invoke
Configured	What the deployment’s effective settings allow
Offered	What a peer advertises or accepts in context
Negotiated	What a particular session actually selects

“Observed” describes the evidence, not a fifth capability stage

The tool landscape provides separate roles

Collect	Source and binary analysis, artifact discovery, probes and tracing
Interpret	Inventory enrichment, policy checks and risk assessment
Manage	Repositories, lifecycle workflows, viewing and document signing

Combining tools still requires a shared evidence contract

Four evidence gaps need deliberate work

Effective configuration	Loaded policy, defaults, inheritance and overrides
Negotiated behaviour	Both peers, real sessions, fallback and rare clients
Non-TLS cryptography	SSH, VPNs, signing, PKI, storage and backups
External paths	Intermediaries, providers and confidentiality lifetime

The reviewed documentation establishes partial contributions

External communication needs a complete path

Example: a local client uploads sensitive records

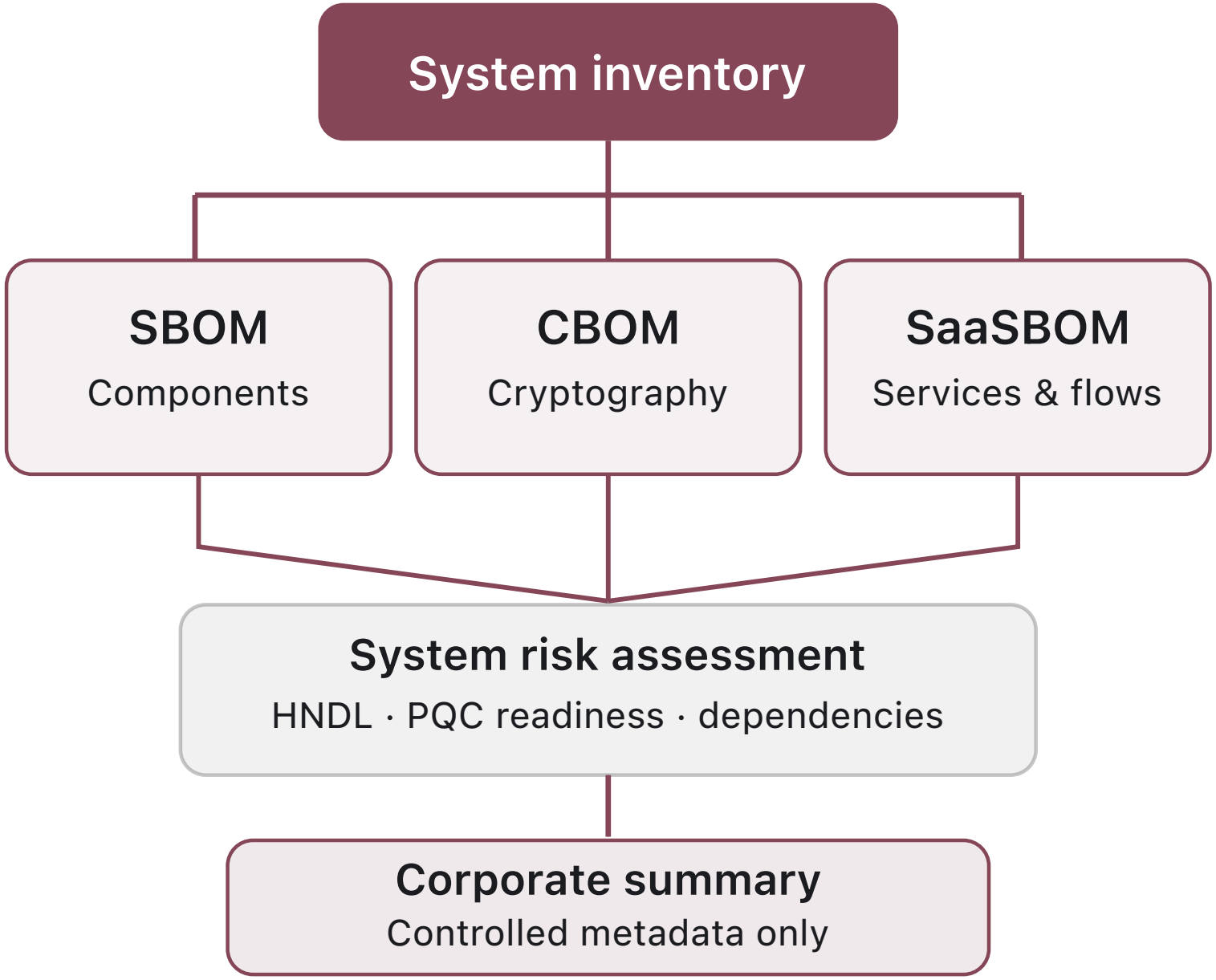
Local client and gateway	Who initiates the connection? Where does encryption terminate?
Provider edge and backend	What protects each onward segment? Which evidence is unavailable?
Storage and backups	Who holds the keys? How long must the information stay confidential?

A modern first connection cannot establish protection for the full path

Governance makes the inventory usable

Detailed evidence stays scoped	System owners govern access, freshness and corrections
Corporate reporting uses less detail	Common risk and progress metadata, with unknowns visible
Dependency coordination	Named owners, controlled evidence links and provider commitments

Inventories and aggregated summaries both carry disclosure risk


System inventory
SBOM
Components
CBOM
Cryptography
SaaSBOM
Services & flows
System risk assessment
HNDL · PQC readiness · dependencies
Corporate summary
Controlled metadata only

Summary and proposed next step

CBOMs support PQC decisions	Their value depends on evidence, deployment context and ownership
Missing evidence needs targeted collection	Adapters, session telemetry, workflow tests and provider assurance
A focused pilot can establish the approach	Representative systems, explicit gaps and one verified migration

Decision: sponsor a 90-day pilot with named owners and acceptance tests