QUANTUM CORE INSTITUTE

Cryptographic Discovery Tools

Assembling the inputs to a QASI inventory

Field	Value
Document ID	QCI-QS1-C1
Version	V1.4 – September 23, 2026. Clause references are QCI requirement identifiers from QCI-QS1 v2.3 (September 23, 2026).
Applies to	QCI-QS1 Clause 5 (inventory and visibility), QCI-5.4-01 to 5.4-03 (discovery and vendor evidence), Annex G domain 1
Status	Informative client handout. Nothing in this handout creates, modifies, or interprets a requirement. Where this handout and the standard differ, the standard governs.
Companion	QCI-QS1-C2, PQC Remediation and Migration Providers
Endorsement	None. The tools listed are unranked. Quantum Core Institute does not endorse, resell, or certify any tool on this list and has not independently tested them.
License	Free. Attribution required. May not be modified and redistributed.
Publisher	Quantum Core Institute Inc.

1 Read this first

No single tool produces a cryptographic inventory. Each one sees one surface: code, network, certificates, hosts, or cloud. This handout lists options per surface so you can assemble the inputs to your QASI (Quantum Attack Surface and Cryptographic Dependency Inventory) under QCI-QS1 Clause 5.

Three rules precede every table in this handout.

1. **A scan is an input to the inventory, not the inventory.** Tools find algorithms, certificates and endpoints. They do not find owners, data longevity or vendor-held keys. Every QASI row still needs validation by its named system owner.
2. **Start with what you already own.** Most organizations have a certificate lifecycle tool, cloud key-management APIs and a code-scanning pipeline. Export from those before buying anything.
3. **Cover your critical systems first.** A complete picture of your top 20 systems is worth more than a partial picture of everything.

> **COMMON MISTAKE**
> Reporting a tool's "coverage" figure as QASI coverage. A scanner's coverage describes how much of a directory or network range it read. QASI coverage under QCI-5.1-03 counts validated critical records over the identified critical population, separately for systems and flows, with numerator and denominator published. A 67% scan-reach figure in the governing-body insert is inventory theater with a decimal point.

2 How discovery surfaces map to the Annex G domains

This handout is organized by what a tool can read: code, network, certificates, hosts, or a platform. QCI-QS1 Annex G organizes dependencies by cryptographic domain, and QCI-5.2-02 requires every record to carry domain tags. The table joins the two, so a finding from any chapter can be placed in the QASI's cryptographic domains field.

Discovery surface (chapter)	Annex G domains it evidences	What it cannot see
Source code and build pipelines (3)	8 libraries; parts of 3, 4, 5 where configuration lives in the repository; 13 for chain code	Anything deployed from a vendor binary; certificates and keys outside the repository
Network endpoints (4)	3 transit; 4 VPN, SSH and remote access; 12 third-party endpoints you connect to	Internal key wrapping; anything not listening on a port
Certificates, keys, PKI and cloud key services (5)	5 PKI and signing; 6 key management; 7 data at rest via the key wrap; 9 identity via token-signing certificates	Vendor-held keys; hardware roots of trust

Discovery surface (chapter)	Annex G domains it evidences	What it cannot see
Hosts, containers and binaries (6)	8 libraries as deployed; 11 device and firmware images; parts of 6	Running-process key use unless an agent hooks it
Multi-method platforms (7)	Most of 3 to 9 and 12, joined to an inventory	Domains 10, 11 and 13 unless the platform has a specific connector

No surface evidences domains 2 (governance) or 10 (messaging) directly, and domain 13 only through code. Those come from owner validation and the Vendor Roadmap Request Pack.

3 Source code and build pipelines

Feeds the QASI fields for algorithms in use, cryptographic libraries and hard-coded primitives.

Tool	Type	What it does
CBOMkit with sonar-cryptography	Open source (Post-Quantum Cryptography Alliance, formerly IBM)	Parses Java, Python and Go code structure, emits a CycloneDX CBOM, runs in CI
qrp-mcp	Open source, single maintainer, early stage	Pattern-based scan of about 20 languages plus configuration, CI and infrastructure files; reports what it did not read inside the CBOM
open-quantum-secure	Open source	14+ languages, CycloneDX 1.7 output, CNSA 2.0 checks
CodeQL or Semgrep cryptography rules	Open source rules	Useful if you already run them; no CBOM output without extra work
IBM Quantum Safe Explorer	Commercial	Scans source and object code, portfolio view, risk scoring
AppViewX AVX ONE PQC Assessment Tool	Commercial	Scans code, dependencies, configurations and certificates; produces a CBOM and a readiness score

WHAT THE ASSESSOR WILL ASK
Show me the triage. Pattern-based scanners report false positives, and a raw scanner export pasted into the QASI carries them all. Budget analyst time to triage findings before they become evidence.

4 Network endpoints (TLS, SSH, VPN)

Feeds the QASI fields for cryptographic functions, external interfaces and PQC support status. Active scanners probe servers you name. Passive monitors watch live traffic.

Tool	Type	What it does
pqcscan (Anvil Secure)	Open source, active	Scans SSH and TLS servers for post-quantum and hybrid algorithm support
AC-Scanner	Open source, active	TLS and SSH scan that emits a CBOM aligned to NIST IR 8547
pqc-posture	Open source, active	Tests whether an endpoint actually negotiates hybrid key exchange; needs OpenSSL 3.5 or later
testssl.sh, SSLyze, ssh-audit, nmap ssl-enum-ciphers	Open source, active	Mature inventories of classical protocols, cipher suites and key types
Zeek	Open source, passive	Logs TLS versions, cipher suites and certificate chains from traffic
Keyfactor CipherInsights	Commercial, passive	Real-time monitoring of cryptographic risk in network traffic
CryptoNext COMPASS	Commercial, passive	Parses 100+ IT and operational-technology protocols

Get written authorization before actively scanning any network range, including your own.

5 Certificates, keys, PKI and cloud key services

This is where most exposure sits, and code scanners do not see it. Feeds the QASI fields for certificate dependencies, human and workload identity dependencies, and key management method.

Tool	Type	What it does
Keyfactor Command, CyberArk Venafi, DigiCert Trust Lifecycle Manager, AppViewX, Entrust	Commercial certificate lifecycle management	The authoritative certificate estate: owners, expiry, issuers, algorithms and key sizes. Start with an export if you already own one
crt.sh, Censys	Free and commercial certificate-transparency search	Finds public certificates issued for your domains that you did not know about
AWS Certificate Manager, KMS and Config	Included with AWS	Key types, algorithms and rotation state through the API
Azure Key Vault and Resource Graph	Included with Azure	Keys, certificates and secrets across subscriptions

Tool	Type	What it does
Google Cloud Asset Inventory with Cloud KMS	Included with Google Cloud	Key algorithms, protection level and rotation

WHY THIS SECTION EXISTS
Hardware security modules and vendor-held signing keys rarely appear in any of these exports. Record them by hand and confirm them through the Vendor Roadmap Request Pack. The Handbook's worked SSO example, with 47 service certificates of unclear ownership, is the typical finding here.

6 Hosts, containers and binaries

Finds cryptography in what is deployed, including third-party software you have no source code for.

Tool	Type	What it does
cbomkit-theia	Open source	Finds certificates, keys, secrets and cryptographic configuration in container images and directories; emits CycloneDX CBOM
cdxgen (OWASP)	Open source	Generates software and cryptographic bills of materials for supported ecosystems
Keyfactor AgileSec Analytics (formerly InfoSec Global)	Commercial, host sensors	Keys, certificates and cryptographic libraries on endpoints and servers
Tychon Quantum Command (ACDI)	Commercial, host agent	Certificates, libraries, protocols and algorithms on endpoints, mapped to business criticality; NIST NCCoE PQC consortium member
PQStation QVision	Commercial	Scans applications, networks, APIs and cloud for cryptographic assets; real-time visibility and compliance reporting (Singapore)

7 Multi-method platforms

These combine several discovery methods with a central inventory and risk scoring. They suit large estates and carry enterprise pricing.

Platform	Discovery methods
IBM Guardium Cryptography Manager and Guardium Quantum Safe	Code, network and runtime discovery, CBOM, risk prioritization
SandboxAQ AQtive Guard	Network analysis, application runtime instrumentation, filesystem scanning
Keyfactor (AgileSec, CipherInsights and certificate lifecycle management)	Host sensors, passive network monitoring and certificate inventory, consolidated after May 2025 acquisitions
Entrust Cryptographic Security Platform	CBOM import and export added September 2026, joined to certificate automation and PQC migration planning
ISARA Advance	Agentless; ingests cryptographic data your existing NDR and EDR tools already collect
QryptoCyber	Agentless, connects to existing tools; CBOM plus a sequenced remediation roadmap through its COAR framework

COMMON MISTAKE
Reporting a platform's risk score as the Q-Risk Score. A platform's score is the vendor's model. The Q-Risk Score is computed from the five QCI-QS1 pillars with the gates of QCI-6.3-01, and the two are not interchangeable.

8 What no tool finds, and where to start

No tool on this list will tell you:

- who owns each system, and how critical it is
- how long each system's data must stay confidential or verifiable
- which keys your vendors hold on your behalf, and what their PQC roadmap is
- which service accounts and operational credentials depend on vulnerable algorithms
- whether you can change an algorithm without replacing the platform

Those answers come from owner validation sessions, the Vendor Roadmap Request Pack and a tested crypto agility proof.

8.1 A starter stack for the first 90 days

This stack costs nothing beyond staff time and maps to weeks 3 to 6 of the establishment sequence in Clause 9.1.

1. One code scanner from chapter 3, run on the repositories of your top critical systems.
2. One active network scanner from chapter 4, run against your external and internal endpoints.
3. An export from the certificate lifecycle tool you already own, plus a certificate-transparency search.
4. Key-management exports from each cloud provider you use.

5. The QASI sheet, where every row carries an owner and an evidence link.

9 What a credible CBOM must state

Whichever tool you choose, accept its output as evidence only if the evidence reference carries what QCI-5.4-01 requires:

- the tool and exact version, and the ruleset or configuration it ran with
- what was examined, as repository and commit, image digest, host, endpoint or network range, with the run date
- what was not examined and why, or a statement that the tool cannot report omissions
- a stable finding identifier and a location for every finding relied upon
- where the output is kept, with the digest algorithm and digest of the file
- the mapping from each finding to the QASI field it populates, and who produced and reviewed it, with the disposition and validation date

Use CycloneDX 1.6 or later as the format. It is vendor-neutral, and most tools above can emit it. A CBOM a vendor sends in answer to Annex C is held to the same objectives under QCI-5.4-03, with the generation method, schema and producer standing in for the scan-tool fields. A tool's own figure for what it read may be recorded beside the evidence reference as scan reach (QCI-5.4-02); it is never the coverage metric. QCI-T1 is the checklist.

> **WHAT THE ASSESSOR WILL ASK**
> Pick any algorithm in your QASI at random and walk me to the scan that found it, the version of the tool that ran, and the list of what that scan did not read. A CBOM that cannot answer the third question is a component list, not evidence.

Sources

Tool descriptions come from each publisher's own materials and two vendor surveys, as of the date on the cover. Quantum Core Institute has not independently tested the tools listed. Verify capabilities, licensing and pricing with the publisher before you commit.

- Cryptographic Inventory Vendors and Methodologies, postquantum.com
- Top Cryptographic Inventory Vendors, Encryption Consulting
- PQCA CBOMkit Architecture
- Keyfactor acquires InfoSec Global and CipherInsights
- IBM Guardium Cryptography Manager
- Entrust adds CBOM capabilities, The Quantum Insider, September 15, 2026
- Tychon cryptographic inventory · PQStation · ISARA Advance · QryptoCyber · AppViewX AVX ONE PQC
- QCI-QS1 Quantum Readiness and Post-Quantum Cryptography Governance Standard, v2.3 (September 23, 2026), and the QCI Practitioner Handbook, at quantumcoreinstitute.com

Independent assessment against QCI-QS1 is performed by the Quantum Core Institute. Scope one at quantumcoreinstitute.com/independent-assessment. An independent assessment is not QCI certification (QCI-1.2-03).