PQ-VES 1.0

Choosing a Post-Quantum Cryptography Vendor

The 2026 Buyer's Standard

A vendor-neutral method for evaluating post-quantum cryptography products and services. Hard gates, evidence-capped scoring across twelve criteria, a verification playbook, a falsifiable pilot design and the contract clauses that hold it together.

VERSION

1.0
Published 12 August 2026

FOR

Procurement leads, CISOs, chief architects, risk officers and technical assessors

Published by ExeQuantum

SOVEREIGN · TRANSPARENT · AGILE · COMPLIANT

Disclosure: ExeQuantum is a post-quantum cryptographic engineering company and a vendor in the market this document describes. This standard names no products, including its own, and is written to be applied to ExeQuantum on the same terms as any other supplier.

About this standard

PQ-VES is a vendor-neutral method for evaluating post-quantum cryptography (PQC) products and services. It exists because the existing material does not go far enough. Migration roadmaps tell you what to do. Capability matrices tell you what vendors say they support. Neither tells you how to tell the difference between a supplier who has done the engineering and one who has done the marketing.

That gap matters more in cryptography than in almost any other procurement category, for three reasons.

Cryptographic failure is silent. A misconfigured firewall announces itself. A constant-time violation in a key encapsulation routine does not. You will not discover it from a dashboard, a customer complaint or an outage. You will discover it from an adversary, or never.

The decision has a multi-decade tail. Data encrypted today under a quantum-vulnerable algorithm remains exposed for as long as it retains value. Hardware roots of trust and firmware signing keys committed today constrain systems that will still be running in 2045.

The market is younger than the demand. Regulatory deadlines arrived before the supply side matured. That combination produces exactly the incentive structure buyers should expect: capability claims running ahead of capability.

PQ-VES is built to be falsifiable. Every criterion specifies what evidence would satisfy it and what evidence would not. Every score is capped by the quality of the evidence behind it, not by the confidence of the person making the claim.

Who this is for

Procurement leads, CISOs, chief architects, risk officers and technical assessors selecting PQC discovery tooling, cryptographic libraries, hardware security modules, PKI and certificate lifecycle platforms, network encryptors, signing infrastructure, embedded cryptographic IP, or migration services. It is written to be usable by a government department, a systemically important bank, a critical infrastructure operator and a commercial enterprise, with profile weightings for each.

How to use it

Work through the stages in order. Do not start at the scorecard. The most common failure in PQC procurement is scoring vendors against a requirement the buyer has not yet defined.

Stage	What you do	Output
0	Establish your requirement	Risk horizon, jurisdiction map, product category, non-negotiables
1	Apply the hard gates	A shortlist, and a documented reason for every exclusion
2	Score against twelve criteria, capped by evidence tier	A weighted, defensible ranking
3	Verify the claims that decide the outcome	A verification log
4	Run a falsifiable pilot	Pass or fail against pre-agreed acceptance criteria
5	Contract for agility	Signed terms that survive the next algorithm change

Stage	What you do	Output
6	Govern the vendor after signature	Re-evaluation triggers and an exit path

Licence and status

PQ-VES 1.0 is published under Creative Commons Attribution 4.0. Copy it, fork it, embed it in your tender documents, strip the branding, disagree with the weightings in public. A framework that cannot be adapted will not be adopted, and a framework that cannot be criticised should not be trusted.

Version 1.0 reflects the regulatory and standards position as at 12 August 2026. Cryptographic policy is moving quickly. Check the status of every dated claim before you rely on it in a tender document, and see the section on maintaining this standard for what triggers a revision.

Table of contents

1. Key takeaways

Score capability, but cap the score by evidence. A vendor's claim, their documentation, a live demonstration, an independent test and an accredited certification are five different things. PQ-VES caps the maximum score for any criterion at the tier of evidence supplied. This single mechanic does more to separate real capability from marketing than any weighting scheme.

Three PQC standards are final, not four or five. FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA) were finalised on 13 August 2024. FIPS 206 (FN-DSA) has not been published, not even as a draft. HQC was selected in March 2025 and has no published standard. Any vendor listing FN-DSA or HQC as a standardised algorithm is either careless or misleading, and the distinction is worth establishing early.

"Uses the NIST reference implementation" is a risk signal, not a reassurance. The CRYSTALS reference code carried the KyberSlash timing vulnerabilities and the compiler-introduced branch that became CVE-2024-37880. Reference implementations exist to demonstrate correctness, not to resist attack. Ask which library, at which commit, with which fixes.

"Formally verified" is meaningless without four qualifiers. Which artefact was verified (Rust source, C source or shipped assembly), against which specification, for which properties, under what trusted computing base. Verification of source code does not establish constant-time behaviour in the compiled binary, and no formal verification in current practice proves resistance to power, electromagnetic or fault attacks.

"FIPS validated" is module-scoped, not algorithm-scoped. A vendor can hold a valid FIPS 140-3 certificate whose approved algorithm list contains no PQC at all. Ask for the CMVP certificate number, confirm the PQC algorithm sits inside the cryptographic boundary in approved mode, and confirm the deployed version matches the validated version. A CAVP algorithm certificate is a different and weaker thing. "In the validation queue" is not validation.

Crypto-agility is testable, and most claims fail the test. The question is not whether a vendor uses the word. It is whether the algorithm identifier is a configuration item or a compile-time constant, whether a substitution can be made without replacing the product, and whether the vendor can demonstrate a completed rotation rather than describe one.

Jurisdictions have already diverged on hybrid deployment. France's ANSSI mandates hybrid. The ENISA agreed mechanisms list states that LWE and MLWE based schemes should not be used standalone. Australia's ASD does not recommend hybrid. The NSA's CNSA 2.0 does not require it. If you operate across these markets, a vendor that supports only one posture creates a compliance conflict you will inherit.

Deployment model and data governance are one criterion among twelve, not the organising principle. For defence, intelligence and classified environments they are decisive and should be weighted accordingly. For most buyers they are a constraint to be satisfied, not the basis of the decision.

Discovery tooling is defined by what it structurally cannot see. Network-based, code-based, agent-based and declarative discovery each have a blind spot that no amount of product maturity removes. Ask for the coverage statement, and treat a vendor who will not produce one as having failed the question.

Buy the migration, not the inventory. Producing a cryptographic inventory is now a commodity capability marketed as a differentiator. The hard problems are prioritisation against your risk model, execution in legacy and operational technology estates, and re-verification after change. Weight your evaluation towards the hard problems.

2. What changed, and why 2026 selection is different

Three shifts since the first wave of PQC procurement make older evaluation habits unsafe.

The mandates became binding

Until mid-2025, almost all national PQC guidance was advisory. That is no longer true in several major jurisdictions. Canada's Treasury Board issued a binding Security Policy Implementation Notice on 9 October 2025 requiring, among other things, that from 1 April 2026 all Government of Canada contracts with digital components include PQC procurement clauses. The United States issued Executive Order 14412 on 22 June 2026, with OMB M-26-15 following on 24 June 2026. Together they impose dated migration obligations on federal civilian agencies, and signal a Federal Acquisition Regulation rule that would extend PQC compliance to covered contractors by 31 December 2030. Australia's Protective Security Policy Framework Release 2026, effective 1 July 2026, makes a maintained PQC transition plan a requirement for Commonwealth non-corporate entities.

The practical consequence for a buyer is that vendor selection now has a compliance consequence, not only a security one. A supplier who cannot evidence conformance becomes your audit finding.

The failure modes became public

The 2024 disclosures changed what a competent buyer should ask. KyberSlash demonstrated full secret-key recovery against widely deployed Kyber implementations by exploiting secret-dependent division timing, in one case recovering a Kyber768 key on a Cortex-M4 in about four minutes. CVE-2024-37880 showed that a correct constant-time idiom in source code was transformed by Clang 15 and later into a secret-dependent branch in the binary. Published work on ML-DSA has since shown that leakage from rejected signing attempts, which implementers routinely discard, can enable private-key recovery from under thirty traces in a laboratory setting.

None of these were failures of the algorithms. All were failures of implementation, and all were present in code that vendors could accurately describe as standards-conformant. Standards conformance and implementation assurance are separate criteria and must be scored separately.

The assurance infrastructure did not keep pace

Validation supply has not matched demand. The Cryptographic Module Validation Program modules-in-process list stood at 217 modules in August 2026, and NIST's own draft material acknowledges that the review process "has struggled to keep pace." Executive Order 14412 directs Commerce to revise CMVP processes to accelerate validations, with that work not yet delivered. There is no Common Criteria protection profile written specifically for post-quantum cryptography; PQC is being certified inside existing secure-element and smartcard profiles, which limits the signal to hardware.

The effect on buyers is a structural incentive for vendors to overstate validation status, because the honest answer for many capable suppliers is "in the queue." A framework that treats validation as a binary pass or fail will either exclude good vendors or accept bad claims. PQ-VES handles this with evidence tiers rather than a gate.

3. Stage 0: Establish your requirement

Do not approach the market until you can answer these five questions in writing. Every one of them changes which vendor wins.

3.1 Quantify the exposure with Mosca's inequality

Mosca's inequality is the standard risk model and remains the clearest way to convert an abstract threat into a procurement deadline.

Let:

- **X** = the number of years your data must remain confidential (its security shelf life)
- **Y** = the number of years your organisation needs to migrate to quantum-safe cryptography
- **Z** = the number of years until a cryptographically relevant quantum computer (CRQC) exists

If **X + Y > Z**, you are already exposed. Data encrypted today will still require protection at a point when it can be decrypted. Migration must begin no later than **Z minus X minus Y** years from now, which for most organisations with long-lived data is a date in the past.

Calibrate Z from a defensible source rather than a vendor slide. The Global Risk Institute's *Quantum Threat Timeline Report 2025* was published on 9 March 2026 and is based on a survey of 26 experts. It places the probability of a CRQC capable of breaking RSA-2048 at roughly 28 to 49 per cent within ten years, and 51 to 70 per cent within fifteen. The report notes the timeline has accelerated relative to earlier editions.

Calibrate Y honestly. NIST has stated that a cryptographic transition "can take 10 to 20 years." The UK NCSC estimates two to three years for discovery and assessment alone. If your internal estimate for Y is under two years, you have almost certainly not scoped the operational technology and embedded estate.

Record X, Y and Z as a board-visible number. They are the inputs that justify the urgency, the budget and the weighting you apply in Stage 2.

3.2 Map your jurisdictions

List every jurisdiction whose cryptographic policy binds you, either directly as a regulated entity or indirectly through your customers and contracts. Then check the algorithm policy of each against Section 13, and the hybrid posture of each against Section 14. Buyers who skip this step routinely discover, after signature, that a product configured for one regulator's expectations is non-conformant for another's.

3.3 Identify the product category

PQC vendors are not comparable across categories. A discovery platform, a cryptographic library, a hardware security module and a certificate lifecycle platform solve different problems and fail in different ways. Scoring them on one axis produces a number that means nothing. Use the category overlays in Section 8, and run a separate evaluation per category.

3.4 Decide your data governance and deployment constraints

Establish, before you see a demonstration, what must be true about where data goes.

- Which classes of data may leave your infrastructure boundary, and under whose jurisdiction may they be processed?

- Do any target environments have no external network connectivity, and if so what is the approved path for installation and update?
- Can the vendor obtain remote access to a production environment, and under what control?
- Where do scan results, cryptographic inventories, key material and credentials reside, and who can technically read them irrespective of what the contract says?

For defence, intelligence and classified environments these are decisive. For most other buyers they are constraints to be satisfied. Either way, write them down before the vendor tells you what is possible.

3.5 Define what a successful outcome looks like

Write the acceptance criteria for the pilot now, at Stage 0, before any vendor has had the opportunity to shape them. A criterion a vendor helped you write is not a test.

4. The evidence tier system

This is the mechanism that makes PQ-VES different from a capability matrix. Every criterion is scored one to five for capability, and that score is then **capped** by the tier of evidence supplied. A vendor with genuinely excellent capability and no evidence scores as though they had no capability, because from the buyer's position those two states are indistinguishable.

Tier	Evidence class	What it looks like	Score cap
E0	Unevidenced claim	Sales assertion, website copy, marketing collateral, a slide	**1**
E1	Documented claim	Product documentation, written tender response, published specification, versioned release notes	**2**
E2	Demonstrated	Working demonstration on your data or a representative environment, reproducible benchmark, vendor-run test you observed	**3**
E3	Independently tested	Third-party audit report, published interoperability test, CAVP algorithm certificate, peer-reviewed research, open source code you can inspect and build	**4**
E4	Accredited certification	CMVP FIPS 140-3 certificate, Common Criteria certificate, EUCC conformance, with the deployed configuration confirmed inside the certified boundary	**5**

Applying the cap

Score the criterion as if the claim were true, then apply the cap.

Worked example. A vendor claims a formally verified ML-KEM implementation with constant-time guarantees. On capability, that would score 5. They supply a marketing page describing it as "formally verified and constant-time." That is E0. **The criterion scores 1.**

The same vendor then supplies the repository, the proof artefacts, the name of the prover, the specification the proof targets, and a continuous integration log showing the proofs re-run on every commit in non-lax mode. That is E3, and independently checkable. **The criterion scores 4.**

They then supply a CMVP certificate number covering the shipped configuration. **The criterion scores 5.**

Nothing about the product changed between those three states. What changed is what you can defend if the decision is later questioned.

Two rules that prevent gaming

Evidence must cover the configuration you will deploy. A certificate covering an AVX2 build on x86-64 does not evidence the Arm build you intend to run at the edge. A verification covering ML-KEM does not evidence ML-DSA. Record the delta and score the delta at the lower tier.

Evidence must be current. A validation certificate on the CMVP historical list, a verification of a commit two years behind the shipping version, or an audit predating a major architectural change all drop one tier. Ask for the date of every artefact and put it in your log.

5. Stage 1: The hard gates

Hard gates are pass or fail. A vendor who fails any gate is excluded regardless of strength elsewhere, and the exclusion is documented. The purpose is to protect the evaluation from a common failure: a supplier compensating for a structural defect with an impressive score in a category that does not matter.

Ten gates apply to all buyers. Profiles in Section 7 add more.

G1. Named algorithms and named parameter sets. The vendor states, in writing, exactly which algorithms and parameter sets are implemented, using standardised names: ML-KEM-768, ML-DSA-65, SLH-DSA-SHA2-128s. Brand-era names (Kyber, Dilithium, Falcon, SPHINCS+) in current product documentation indicate the documentation has not been maintained since 2024. “Supports post-quantum cryptography” without specification is a fail.

G2. No proprietary core primitive. The confidentiality and authenticity of the system must not depend on an algorithm the vendor will not publish. This is Kerckhoffs’s principle, and it is not negotiable in 2026. Proprietary implementations of published standards are acceptable. Proprietary cryptography is not.

G3. Deployment model satisfies your data governance constraint. Tested against the answers you wrote at Stage 0.4, not against the vendor’s description of what is theoretically possible. If your constraint is disconnected operation, “supports air-gapped deployment” is a claim to be tested at Stage 3, and a vendor who requires periodic connectivity for licensing, telemetry or updates fails here.

G4. Algorithm substitution without product replacement. The vendor can describe, and later demonstrate, changing a cryptographic algorithm or parameter set through configuration or a signed update, without replacing the product or requiring a re-architecture. A vendor whose answer is “we would issue a new version” has told you their crypto-agility is a roadmap item.

G5. Machine-readable cryptographic inventory output. For any product that discovers, inventories or reports on cryptography: output in CycloneDX 1.6 or later, ideally 1.7, with populated `cryptoProperties`. Note that the worked pilot in Section 10 requires 1.7 output, so raise this gate to 1.7 if you intend to run that pilot. A PDF report is a deliverable, not an inventory. You cannot diff a PDF, and re-verification after change is the whole point.

G6. Known-vulnerability currency. The vendor can state which cryptographic library, at which version and commit, underpins the product, and can confirm the KyberSlash fixes and the CVE-2024-37880 mitigation are present. A vendor unable to answer this within one business day has told you something about their software supply chain.

G7. Jurisdictional algorithm policy coverage. The product can be configured to satisfy the algorithm policy of every jurisdiction on your Stage 0.2 map, including hybrid posture. See Section 14.

G8. Named implementation provenance. The vendor identifies the origin of the cryptographic implementation, whether written in-house, derived from a named open source project, or licensed, and states its verification and testing status. “Proprietary implementation” with no further detail is a fail. Note that PQClean is being archived as of July 2026; a product shipping PQClean-derived code without a migration plan is a finding.

G9. Vulnerability disclosure and cryptographic weakness commitment. A published vulnerability disclosure policy, a security contact, a stated remediation target, and an explicit commitment to notify customers of cryptographic weaknesses and of any use of non-approved algorithms discovered in the product.

G10. No substitution of quantum key distribution for post-quantum cryptography. QKD is a distinct technology addressing a different problem, with its own deployment constraints and no built-in authentication. The UK NCSC stated in August 2025 that it "will not support the use of QKD for government or military applications," and comparable positions are held elsewhere. A vendor offering QKD as an answer to a PQC requirement has misunderstood the requirement or is relying on you to.

Recording exclusions

For every vendor excluded at a gate, record the gate, the evidence, the date and the assessor. If the decision is challenged, whether by an unsuccessful bidder, an auditor or a board, the gate log is what defends it.

6. Stage 2: The twelve criteria

Twelve criteria, grouped into four pillars. The default weights below suit a general enterprise or critical infrastructure buyer. Section 7 gives profile-specific weightings.

Pillar	Weight	Criteria
A. Cryptographic assurance	30%	A1 Standards conformance (10), A2 Implementation assurance (12), A3 Independent validation (8)
B. Architectural fitness	30%	B1 Crypto-agility (13), B2 Integration and interoperability (9), B3 Deployment model and data governance (8)
C. Program enablement	25%	C1 Discovery and inventory quality (10), C2 Machine-readable evidence (7), C3 Compliance mapping and audit evidence (8)
D. Counterparty risk	15%	D1 Vendor viability and execution (6), D2 Security posture and disclosure (5), D3 Commercial terms and lifecycle economics (4)

Each criterion is scored one to five, capped by evidence tier, then multiplied by its weight. The maximum possible score is 500.

Pillar A: Cryptographic assurance (30%)

A1. Standards conformance and algorithm coverage (10%)

What you are assessing. Whether the vendor implements the right algorithms, at the right parameter sets, correctly, and whether they describe the standards landscape accurately.

Establish the baseline. Three PQC standards are final: FIPS 203 (ML-KEM, parameter sets ML-KEM-512, ML-KEM-768 and ML-KEM-1024), FIPS 204 (ML-DSA, parameter sets ML-DSA-44, ML-DSA-65 and ML-DSA-87) and FIPS 205 (SLH-DSA, twelve parameter sets across SHA2 and SHAKE variants). All three were finalised on 13 August 2024. FIPS 206 (FN-DSA) is not published in any form. HQC was selected in March 2025 with no published standard. For stateful hash-based signatures used in firmware signing, the relevant references are SP 800-208, LMS and XMSS.

What to ask.

- Which parameter sets are implemented, and which are enabled in the default configuration?
- Which are in the shipping build versus the roadmap, with dates?
- Are the algorithms available for all cryptographic functions you need, or only some? Key generation, encapsulation, decapsulation, signing and verification are separately implemented and separately testable.
- What is the vendor’s position on FIPS 206 and HQC, and does their published material describe them accurately?
- For protocol-level products: which code points and which standards? Hybrid TLS 1.3 key agreement is standardised. RFC 10024 (Proposed Standard, August 2026) defines the X25519MLKEM768, SecP256r1MLKEM768 and SecP384r1MLKEM1024 groups and their code points, with the framework

described in the Informational RFC 9954. ML-KEM in IKEv2 and SSH, and composite ML-DSA for X.509, were all approved and in the RFC Editor queue as at August 2026, with none yet published as an RFC. Treat all three as approved but unpublished. Ask a vendor claiming standards-compliant composite certificates which draft revision and which object identifiers are implemented, and what happens if those identifiers change before publication.

Scoring anchors. 1: unspecified PQC support. 2: one algorithm family, limited parameter sets, brand-era naming. 3: ML-KEM and ML-DSA at the parameter sets you require, accurately described. 4: full parameter set coverage across ML-KEM, ML-DSA and SLH-DSA, correct protocol code points, accurate public position on unpublished standards. 5: as 4, plus stateful hash-based signature support where relevant, and demonstrated interoperability against independent implementations.

Disqualifying answers. Listing FN-DSA or HQC as standardised. Refusing to name parameter sets. Claiming a proprietary algorithm is “equivalent to” a NIST standard.

A2. Implementation assurance (12%)

What you are assessing. Whether the code that runs is resistant to the attacks that have actually broken PQC deployments. This is the highest-weighted criterion in Pillar A because it is where the published failures are and where buyer scrutiny is weakest.

Ask about provenance first. Which library, which version, which commit. Whether it is a fork, and if so what has diverged from upstream. Whether the KyberSlash fixes and the CVE-2024-37880 mitigation are present, with a commit reference. Whether any PQClean-derived code remains, given that project’s archival in July 2026.

Then ask about constant-time behaviour, at the binary. Constant-time source code compiled by an optimising compiler is not necessarily constant-time. That is not a theoretical concern: it is precisely what CVE-2024-37880 was. Ask which compiler, which version, which flags and which target were used, and what binary-level evidence exists. Acceptable evidence includes constant-time testing under a dynamic analysis tool, statistical timing analysis, or assembly-level proofs.

Then interrogate any formal verification claim on four axes.

1. **Which artefact** was verified: high-level source, C source, intermediate representation, or the shipped assembly?
2. **Against which specification**, and is that specification published and independently reviewable against the FIPS text?
3. **Which properties** were proven? Name them individually: memory safety, panic freedom, functional correctness, secret independence, constant-time, speculative constant-time. These are not interchangeable.
4. **What is the trusted computing base?** Which prover, which compiler, and which dependencies are assumed correct rather than proven?

Then ask the two operational questions that catch most weak claims: are the proofs re-run in continuous integration on every commit, in non-lax mode, with no unproven assumptions admitted, and can you see the log? And is there a published soundness or caveats document stating the residual risk? Amazon’s practice of publishing a `SOUNDNESS.md` alongside its verification work is the benchmark here, and a vendor who has never considered publishing one has probably not thought hard about the limits of their own claim.

Understand what formal verification does not give you. It does not establish resistance to power analysis, electromagnetic emissions or fault injection. It does not cover unverified glue code, key management plumbing or random number generation. Verification of one algorithm on one platform

does not extend to others. And a proof against an incorrect specification proves nothing, which has been demonstrated in practice rather than argued in theory.

Ask about entropy. PQC key generation is entropy-hungry, and hedged ML-DSA signing is entropy-sensitive. Ask which random number generator is used, and for hardware or certified products, which functionality class under BSI AIS 20/31 and which version it was evaluated against.

For ML-DSA specifically, ask whether rejection-sampling iterations are protected. Leakage from rejected signing attempts, which implementers often assume are harmless because they are discarded, has been shown to enable private-key recovery.

Scoring anchors. 1: cannot name the implementation. 2: names a library, no constant-time or verification evidence. 3: named library at a current version with known fixes confirmed, documented constant-time testing methodology. 4: independent audit or published verification with artefact, specification, properties and trusted computing base all named, and continuous integration evidence. 5: as 4, plus assembly-level constant-time proofs on the shipped build, hardware side-channel and fault-injection test results, and a published caveats document.

A3. Independent validation and certification (8%)

What you are assessing. What an accredited third party has actually attested, as distinct from what the vendor asserts.

Separate the signals. A CAVP algorithm certificate proves that an algorithm implementation passes known-answer tests. It says nothing about side-channel resistance or product integration. A CMVP FIPS 140-3 module certificate is the harder and more meaningful signal, but it is module-scoped: the certificate tells you nothing until you read the security policy and confirm which algorithms sit inside the cryptographic boundary in approved mode. Common Criteria certification for PQC currently exists inside secure element and smartcard protection profiles rather than a dedicated PQC profile, and is therefore largely a hardware signal.

What to request.

- The CMVP certificate number, and the security policy document.
- Confirmation that the PQC algorithms are inside the validated boundary and in the approved mode of operation.
- Confirmation that the certificate is on the active list, not the historical list, and whether it carries an interim validation caveat with a shortened expiry.
- Confirmation that the version you will deploy is the version validated.
- If in the modules-in-process queue: the date of submission and the current stage. This is legitimate information and should be scored at E1, not treated as a fail.
- For European sales: conformance with the ENISA agreed cryptographic mechanisms, and awareness that the list’s requirements differ from NIST’s.

Scoring anchors. 1: no validation, no queue position, claims validation it does not hold. 2: CAVP certificates only, presented accurately. 3: CAVP plus a credible independent audit. Note that a documented CMVP queue position scores well on capability but is evidenced at E1, so it caps at 2. 4: active CMVP certificate covering the deployed configuration. 5: as 4, plus Common Criteria or EUCC conformance where the product class supports it, and evidence the vendor maintains certification across versions rather than certifying once.

Disqualifying answers. Presenting a CAVP certificate as module validation. Presenting a queue position as validation. Presenting a quantum key distribution protection profile as PQC certification. Using the phrase “quantum-safe certified”, which describes a certification that does not exist.

Pillar B: Architectural fitness (30%)

B1. Crypto-agility (13%)

What you are assessing. Whether you can change cryptographic algorithms after deployment without a replacement program. This carries the single highest weight in the framework, because it is the only criterion that protects you against being wrong about everything else.

The definition to test against. NIST CSWP 39, *Considerations for Achieving Crypto Agility*, is final as of December 2025 and was updated in June 2026. It defines cryptographic agility as the capabilities needed to replace and adapt cryptographic algorithms across protocols, applications, software, hardware, firmware and infrastructure while preserving security and ongoing operations.

The maturity scale to score against. The Crypto Agility Maturity Model (CAMM) provides five levels, from 0 (not possible) to 4 (sophisticated). Level 3, “practiced”, is the meaningful procurement bar: migration between cryptographic methods is demonstrably, effectively and securely feasible. Note the word demonstrably. A vendor at CAMM level 2 has prepared for agility. A vendor at level 3 has done it.

Six questions that separate real agility from the word.

1. Is the algorithm identifier a configuration item, or a compile-time constant?
2. Can an algorithm be changed without replacing the product, and without a firmware or hardware refresh?
3. Has the vendor completed an algorithm migration in a customer environment, and will they describe it, including what broke?
4. Are hybrid modes supported, and can the hybrid posture be changed by configuration?
5. What is the vendor’s stated time from a new algorithm being standardised to it being available in the shipping product, and what is their track record against that number?
6. Are cryptographic dependencies inventoried inside the product itself, so that you can tell what would need to change?

Scoring anchors. 1: algorithms hardcoded, change requires a new product version. 2: configurable in principle, never demonstrated (CAMM 1 to 2). 3: configurable and demonstrated in a test environment, hybrid supported. 4: demonstrated production algorithm migration with a customer reference, documented agility roadmap, product-internal cryptographic dependency inventory (CAMM 3). 5: as 4, plus a contractual commitment to support new standardised algorithms within a stated period, and negotiable hybrid posture per jurisdiction (CAMM 4).

B2. Integration and interoperability (9%)

What you are assessing. Whether the product works with the estate you have, rather than the estate a reference architecture assumes.

What to ask.

- Named integrations with your identity provider, certificate authority, hardware security modules, key management system, SIEM, configuration management database and ticketing system. Named, versioned and documented, not “supports standard APIs.”

- Demonstrated interoperability with independent implementations of the same standards. Two products that only interoperate with themselves have not been tested.
- Behaviour under mixed estates, where some endpoints support PQC and some do not. Downgrade handling is a security property, not a convenience feature.
- Performance and size impact, measured in your conditions. ML-KEM and ML-DSA change handshake sizes and signature sizes materially, and the effect is felt hardest in constrained, high-volume and latency-sensitive paths.
- Constrained environment support: embedded targets, operational technology protocols, devices with fixed firmware, and long-lived hardware where the migration path is replacement rather than update.
- Whether the vendor's approach to legacy systems is direct upgrade or a wrapper. Proxy and gateway architectures that terminate PQC in front of a quantum-vulnerable estate are a mitigation with a defined expiry, not a migration, and should be scored and contracted as such.

Scoring anchors. 1: no named integrations. 2: named integrations, no evidence. 3: documented integrations plus a demonstration in a representative environment. 4: proven interoperability with independent implementations, measured performance data from your own conditions, documented mixed-estate behaviour. 5: as 4, plus demonstrated operation in constrained or operational technology environments comparable to yours.

B3. Deployment model, data governance and jurisdictional control (8%)

What you are assessing. Where your data, keys and cryptographic inventory actually reside, who can technically access them, and under which legal regime.

This criterion carries the sovereignty and residency requirements that dominate defence and government procurement. For those buyers it should be reweighted upward substantially, and Section 7 does so. For most buyers it is a constraint to be satisfied rather than a differentiator.

What to ask, in order of how often the answer surprises buyers.

1. **Key custody.** Does the vendor's architecture ever place them in possession of, or in a position to access, your key material? Under what conditions, and enforced by what technical control rather than what contractual term?
2. **Data residency for derived artefacts.** Discovery findings, cryptographic inventories, credentials and scan results are as sensitive as an asset register and a vulnerability report combined. Where do they live? A product that keeps keys local but ships inventories to a vendor-hosted analytics tier has moved the crown jewels one layer down.
3. **Egress behaviour.** What network connections does the product make, to where, and can each be disabled without loss of core function? Ask for a documented egress list, then verify it during the pilot with your own packet capture.
4. **Disconnected operation.** For environments with no external connectivity: is installation possible from approved media with a signed, verifiable bundle? Do licensing, entitlement checks, telemetry or updates require connectivity at any point? Can updates be delivered through your change management process rather than an automatic channel? Many vendors claim disconnected support and require periodic connectivity for one of these four.
5. **Vendor access.** Can the vendor obtain remote access to a production environment, for support or any other purpose? What technical control prevents it, and what audit record would show it happened?

6. **Legal jurisdiction.** Under which country's law does the vendor operate, where is data processed, and what is the vendor's stated position on lawful access requests from a foreign jurisdiction? This is a legal question with a technical answer: the strongest position is an architecture in which the vendor could not comply even if compelled.

Scoring anchors. 1: vendor-hosted only, no residency control. 2: hosted with residency options, vendor retains technical access to inventory data. 3: customer-hosted deployment available, documented egress, no vendor key custody. 4: as 3, plus verified disconnected operation, signed installation bundles, and inventory data held in customer-controlled storage. 5: as 4, plus no vendor technical access path to production by architecture, verified during the pilot, and a documented position on foreign lawful access.

Pillar C: Program enablement (25%)

C1. Discovery and cryptographic inventory quality (10%)

What you are assessing. Whether the tool finds the cryptography you have, and whether the vendor is honest about what it cannot find.

Method determines the blind spot. This is the most important thing a buyer can understand about this category, and it is rarely stated plainly by vendors.

Discovery method	Sees	Structurally cannot see
Passive network analysis	Cryptography in observed traffic, protocol negotiation, certificates in use	Data at rest, code paths not exercised, encrypted-tunnel interiors, anything on unmonitored segments
Static code and binary analysis	Cryptographic calls in source and binaries, library dependencies	Runtime configuration, dynamically negotiated parameters, hardware roots of trust, code you do not hold
Host agent or endpoint telemetry	Local configuration, certificate and key stores, running processes	Unmanaged hosts, appliances that reject agents, operational technology, embedded devices
Declarative or questionnaire-based	Whatever the estate owner already knows	Everything the estate owner does not know, which is the reason you bought the tool

No method is complete. A credible vendor tells you this before you ask. Combining methods is the practical answer, and a serious evaluation compares a vendor's discovery output against a subset of the estate you have already inventoried by hand.

What to ask.

- Which methods does the product use, and what is the documented coverage statement, including explicit exclusions?
- What is the false positive and false negative profile, and how was it measured?
- Does discovery identify the cryptographic asset (algorithm, parameter set, key length, protocol, certificate) or only the presence of cryptography?
- Does it map assets to owning systems, business services and data classifications, so that prioritisation is possible?
- Does it detect quantum-vulnerable use specifically, distinguishing an algorithm that is quantum-vulnerable in context from one that is not?

- How is the inventory maintained after the first scan? A point-in-time inventory decays from the day it is produced.
- Can the tool run in your most constrained environment, and what does it need in order to do so?

The test that matters. Give the vendor a scoped segment for which you hold a hand-built ground truth. Score them on what they found, what they missed and what they invented. This is the single most informative hour in the whole evaluation.

Scoring anchors. 1: declarative only, or no coverage statement. 2: single method, coverage statement on request. 3: two or more methods, published coverage statement including exclusions, asset-level detail. 4: as 3, plus validated against your ground truth with an acceptable miss rate, and mapping to owning systems. 5: as 4, plus continuous or scheduled re-discovery, change detection, and demonstrated operation in your constrained environments.

C2. Machine-readable evidence and CBOM (7%)

What you are assessing. Whether the product's output is usable as an input to other systems, or only as a report.

A Cryptographic Bill of Materials is not a separate document format. It is a CycloneDX bill of materials whose components carry `cryptoProperties`. CycloneDX 1.6 was ratified as ECMA-424, and 1.7, released in October 2025, added standardised algorithm-family and elliptic-curve registries specifically to support quantum readiness assessment. Executive Order 14412 is the first instrument to address CBOMs directly, directing CISA, in coordination with NIST, to publish guidance on the minimum elements of a CBOM within 270 days, meaning approximately 19 March 2027. It does not itself require agencies or contractors to produce CBOMs. Whether a production obligation follows will depend on that guidance and on any subsequent Federal Acquisition Regulation rule.

What to demand in the output. For each cryptographic asset: the primitive and the parameter set identifier using standardised naming, the object identifier, the NIST quantum security level and the classical security level, the implementation platform and execution environment so that hardware-resident and software-resident assets are distinguishable, the certification level cross-referenced to a CAVP or CMVP certificate number where one exists, the cryptographic functions supported, protocol bindings including code points, and explicit dependency links from cryptographic assets to the software components that use them.

Then demand the metadata about the CBOM itself. How it was generated (static, dynamic, agent or declarative), what the generation could not cover, the refresh cadence, and whether the CBOM is signed or attested. A hand-authored declarative CBOM is a marketing document with a schema.

Scoring anchors. 1: PDF reports only. 2: exportable data in a proprietary format or CSV. 3: CycloneDX 1.6 or later with basic `cryptoProperties`. 4: CycloneDX 1.7 with full property population including parameter sets, OIDs, security levels and dependency links, plus a generation and coverage statement. 5: as 4, plus signed or attested CBOMs, automated refresh, and demonstrated ingestion into your own tooling.

C3. Compliance mapping and audit evidence (8%)

What you are assessing. Whether the product reduces your reporting burden or adds to it.

What to ask.

- Which control frameworks does the product map findings to, and is the mapping to specific control identifiers rather than framework names? “Maps to ISO 27001” is not a mapping. “Maps to ISO/IEC 27001:2022 Annex A 8.24” is.
- Does it map to the frameworks you actually report against, including sector and national frameworks, and if not, can mappings be added by you rather than only by the vendor?
- Does the product produce evidence an auditor will accept: timestamped, attributable, tamper-evident, exportable?
- Is every action taken through the product auditable, including vendor and administrator actions?
- Does the vendor maintain mappings as frameworks change, and at what cadence?
- For regulated buyers: can the product evidence the specific obligations you carry, such as a maintained cryptographic inventory, a documented transition plan, or dated migration milestones?

Treat a long list of framework logos with scepticism. Ask to see the mapping for one control you know well, and judge the rest by it.

Scoring anchors. 1: no mapping. 2: framework names, no control identifiers. 3: control-level mapping to two or more frameworks you use, exportable evidence. 4: as 3, plus full audit trail of all actions, maintained mappings with a stated cadence, and evidence formats your auditors have accepted before. 5: as 4, plus customer-extensible mappings and demonstrated support for your specific regulatory obligations.

Pillar D: Counterparty risk (15%)

D1. Vendor viability and execution capability (6%)

What you are assessing. Whether the vendor will still be able to support this product across a migration measured in years and an asset lifecycle measured in decades.

What to ask. Funding position and runway. Size and composition of the engineering team, specifically how many people hold cryptographic engineering expertise as distinct from general software engineering. Whether named cryptographers are associated with the product publicly. Participation in standards bodies and open source projects, which is a low-cost signal that is hard to fake. Delivery track record against previously published roadmap dates, which you can check yourself against archived versions of their site. Customer references in your sector and at your scale, contacted directly.

Then ask the question most buyers avoid. What happens to your deployment if the vendor is acquired, ceases trading or discontinues the product? Source code escrow, data portability in open formats, and documented exit procedures are the answers. Score the answer, and contract for it in Section 11.

Scoring anchors. 1: no verifiable track record, no cryptographic expertise evidenced. 2: some references, roadmap history not checkable. 3: verifiable delivery record, identifiable cryptographic expertise, references in adjacent sectors. 4: as 3, plus standards or open source participation, references at your scale and sector, and a documented continuity position. 5: as 4, plus escrow and a tested exit path.

D2. Security posture and vulnerability handling (5%)

What you are assessing. The vendor as a component of your attack surface, and their behaviour when something goes wrong.

What to ask. Their own security certifications and the scope statement behind them, which is where most certification claims lose their force. Software supply chain practices, including SBOM production for their own product, dependency management and build reproducibility. Penetration test cadence and whether summary reports are shared. Vulnerability disclosure policy, remediation targets by severity, and a bug bounty if one exists.

Then use the two 2024 cryptographic events as a natural experiment. How long did the vendor take to ship the KyberSlash fixes and the CVE-2024-37880 mitigation? How did they notify customers? That is a measured data point about future behaviour, available to you at no cost, and it discriminates far better than any policy document.

Scoring anchors. 1: no disclosure policy, cannot answer the 2024 question. 2: policy exists, remediation targets vague. 3: certifications with clear scope, published policy with targets, credible answer on 2024 patch latency. 4: as 3, plus shared test summaries, SBOM for their own product, documented customer notification process. 5: as 4, plus a public track record of proactive cryptographic disclosure, including disclosing issues found in their own code.

D3. Commercial terms and lifecycle economics (4%)

What you are assessing. The total cost across the migration, and whether the commercial model creates a lock-in that undermines the agility you are paying for.

What to ask. Licensing basis and how cost scales with your actual growth vector, whether that is endpoints, certificates, transactions or scanned assets. What is included versus chargeable: additional algorithms, additional environments, additional integrations, professional services. Support tiers, response commitments and the cost of the tier you will actually need. Cost of the exit: data export, transition assistance, and what happens to your inventory history.

Then model the lifecycle, not the licence. Migration costs are dominated by internal effort, not licence fees. Analyst guidance in 2026 places completion of planning, remediation and execution around 2030, which compresses the window for anyone starting pilots after 2026 and raises the cost of the internal effort accordingly. Score the vendor on how much of your internal effort their product removes, which is a question their references can answer and their sales team cannot.

Scoring anchors. 1: opaque pricing, punitive exit. 2: clear licence cost, unclear total cost. 3: transparent pricing, defined inclusions, reasonable exit terms. 4: as 3, plus predictable scaling, contractual support commitments, and reference-validated reduction in internal effort. 5: as 4, plus pricing that does not penalise crypto-agility, such as no charge for adding newly standardised algorithms.

7. Buyer profile weightings

The default weights suit a general enterprise or critical infrastructure buyer. Five profiles adjust them. Use the profile closest to your position, then adjust once with a documented reason. Adjusting twice usually means you have chosen the wrong profile.

Criterion	Default	National security and defence	Civilian government	Regulated financial services	Critical infrastructure and OT	Commercial enterprise
A1 Standards conformance	10	12	10	10	8	10
A2 Implementation assurance	12	18	12	12	12	9
A3 Independent validation	8	14	12	10	6	5
B1 Crypto-agility	13	12	12	14	15	15
B2 Integration and interoperability	9	6	8	10	14	13
B3 Deployment and data governance	8	18	12	8	8	5
C1 Discovery and inventory quality	10	6	10	10	12	13
C2 Machine-readable evidence	7	5	7	6	6	8
C3 Compliance mapping	8	5	10	12	8	7
D1 Vendor viability	6	2	3	4	5	7
D2 Security posture	5	2	3	3	4	5
D3 Commercial terms	4	0	1	1	2	3
Total	**100**	**100**	**100**	**100**	**100**	**100**

Profile notes

National security and defence. Implementation assurance, independent validation and deployment control together carry half the weight. Add hard gates: mandatory conformance with the applicable national algorithm suite at its required parameter sets, verified disconnected operation, signed and verifiable installation bundles, and no vendor technical access path to production. Commercial terms are weighted at zero because they are not permitted to influence the outcome, not because they do not matter.

Civilian government. Compliance mapping and independent validation rise because the reporting obligation is real and dated. Deployment control rises above default but below defence. Add a gate for the specific inventory and transition-plan obligations in your jurisdiction.

Regulated financial services. Compliance mapping and crypto-agility carry the weight, reflecting supervisory attention to cryptographic inventory, transition planning and the ability to respond to cryptanalytic developments. Add a gate for your regulator's stated expectations, and note that several regulators have signalled formal expectations arriving during 2026 and 2027.

Critical infrastructure and operational technology. Integration and crypto-agility dominate, because the binding constraint is not the cryptography but the twenty to thirty year asset lifecycle it must live inside. Add a gate requiring demonstrated operation on your actual protocol set and device classes. Treat any wrapper or gateway approach as a time-limited mitigation with a contractual expiry.

Commercial enterprise. Crypto-agility, discovery quality and integration dominate. Validation weight falls because you are not bound by a validation requirement, and paying a premium for a certificate you do not need is a real cost. Vendor viability rises because you have less leverage to compel continuity.

8. Product category overlays

Score within a category, never across categories. Each overlay adds category-specific gates and questions to the twelve criteria.

8.1 Discovery, inventory and CBOM tooling

Additional gates. Published coverage statement with explicit exclusions. CycloneDX 1.6 or later output. Ability to operate in your most constrained environment.

Additional questions. How does the tool distinguish quantum-vulnerable use from quantum-vulnerable capability, given that a quantum-vulnerable algorithm present but unused is a different finding from one in production use? How does it treat cryptography inside third-party binaries, firmware and hardware roots of trust? What is the re-scan cost, in time and in production impact?

The decisive test. Ground truth comparison, as described in criterion C1.

8.2 Cryptographic libraries and SDKs

Additional gates. Named upstream provenance. Current with KyberSlash and CVE-2024-37880. Not PQClean-derived without a stated migration path.

Additional questions. Which platforms and instruction set extensions are covered by the assurance evidence, and which shipped configurations are not? What is the API stability commitment across algorithm changes? What is the performance profile on your target hardware, measured rather than quoted? How are algorithm identifiers surfaced to calling applications, since this determines your own crypto-agility downstream?

Weighting adjustment. Raise A2 (implementation assurance) by a further 4 points, taken from C1 and C3, which are largely inapplicable to this category.

8.3 Hardware security modules and key management

Additional gates. FIPS 140-3 validation covering the PQC algorithms in the approved mode, or a documented queue position with dates. Stated firmware upgrade path to future algorithms.

Additional questions. Can new algorithms be added by firmware update, or does support require hardware replacement? What is the performance impact of PQC operations at your transaction volumes? What is the key backup, escrow and migration path for post-quantum key material, whose sizes differ materially from classical keys? What is the entropy source and its evaluated functionality class?

8.4 PKI and certificate lifecycle management

Additional gates. Support for the certificate profiles you require, with accurate positioning on which are standardised. Ability to operate a hybrid or dual-certificate estate during transition.

Additional questions. How is the root of trust migrated, which is the hardest problem in this category and the one most often deferred? What is the position on composite certificates, which were approved but not yet published as an RFC as at August 2026? How does certificate lifetime interact with your migration timeline, and does the product support the shortened lifetimes now being adopted? What is the revocation and rollback path if a PQC deployment fails in production?

8.5 Network encryptors, VPN and secure tunnels

Additional gates. Standardised hybrid key exchange with named code points. Documented behaviour on downgrade.

Additional questions. Which protocol standards are implemented and at what maturity, noting that ML-KEM in IKEv2 and SSH was approved but not yet published as an RFC as at August 2026? State the draft revision implemented. What is the throughput and latency impact under your traffic profile? How does the device behave against peers that do not support PQC, and can downgrade be prohibited by policy? What is the firmware upgrade path across the device's service life?

8.6 Code signing, firmware signing and software supply chain

Additional gates. Support for stateful hash-based signatures where your threat model requires them, with correct state management.

Additional questions. How is signing key state managed for LMS and XMSS, where state reuse is catastrophic and is a genuine operational hazard rather than a theoretical one? What is the verification path on devices already in the field, which is the constraint that usually determines the answer? How does the product support a dual-signing transition period?

8.7 Embedded, silicon and cryptographic IP

Additional gates. Side-channel and fault-injection test evidence. Certification under an applicable protection profile if the deployment requires it.

Additional questions. What is the die area, power and performance cost? What countermeasures are implemented against power, electromagnetic and fault attacks, and what independent testing supports them? Is the algorithm implementation updatable post-fabrication, and if not, what is the obsolescence plan?

8.8 Migration services and consulting

Additional gates. Named cryptographic expertise on the delivery team, not only in the pitch team. Deliverables specified as artefacts, not activities.

Additional questions. What is delivered as a machine-readable artefact you retain and can use without the vendor? What is the tooling dependency, and does the engagement create a dependency on a product you have not separately evaluated? What is the knowledge transfer commitment? Who specifically will do the work, and what is their availability?

9. Stage 3: The verification playbook

Score the vendors, then verify the claims that decide the outcome. You do not need to verify everything. You need to verify every claim that, if false, would change the ranking. Identify those claims before you start.

Claim type	How to verify	Time
CMVP or CAVP certification	Search the public validation lists by certificate number. Read the security policy. Confirm algorithms, mode, boundary, version and active status.	30 minutes
Queue position	Check the public modules-in-process list for the vendor and module name.	10 minutes
Algorithm and parameter set support	Request the configuration file or API reference showing the enumeration. Test in the pilot.	1 hour
Library provenance and patch currency	Ask for library, version and commit. Check the upstream repository for the relevant fixes at or before that commit.	30 minutes
Formal verification	Request repository, proof artefacts, specification, property list and continuous integration log. Confirm proofs run in non-lax mode with no admitted assumptions. Have a cryptographic engineer read the caveats document.	4 hours, plus expert time
Constant-time behaviour	Request compiler, version, flags and target, plus binary-level test evidence. Reproduce on a build you compile.	4 hours
Crypto-agility	Do not accept a description. Require a live algorithm substitution during the pilot, timed and observed.	Pilot
Disconnected operation	Deploy with egress blocked at the network layer. Run for the full licensing and update cycle. Capture all attempted connections.	Pilot
Data residency and egress	Packet capture during a full workflow. Compare against the vendor’s documented egress list.	Pilot
Discovery coverage	Ground truth comparison against a hand-built inventory of a scoped segment.	1 day
Interoperability	Test against an independent implementation, not only against the vendor’s own client.	1 day
Compliance mapping	Pick one control you know well. Read the mapping. Judge the remainder by it.	1 hour

Claim type	How to verify	Time
Customer references	Speak to references you sourced yourself, not only those the vendor supplied. Ask what went wrong and what they would do differently.	2 hours
Vendor roadmap credibility	Compare current roadmap claims against archived versions of the vendor's site from twelve and twenty-four months ago.	1 hour

Keep a verification log. Claim, evidence tier, verification method, result, date, assessor. It is the document that turns a procurement decision into a defensible one, and it is the document that will exist long after the people who made the decision have moved on.

10. Stage 4: Designing a falsifiable pilot

A pilot that cannot fail is a demonstration with a longer duration. Design it so that failure is possible, specified in advance, and consequential.

The rules

Write acceptance criteria before the vendor is selected. Criteria written after a preferred vendor emerges will be shaped, consciously or not, to fit that vendor.

Make every criterion falsifiable. “Demonstrates crypto-agility” is not a criterion. “Substitutes ML-KEM-768 for ML-KEM-1024 across the pilot estate through configuration change, with no service interruption, in under four hours, evidenced by packet capture” is a criterion.

Use your environment and your data. A vendor-hosted sandbox tests the vendor’s sandbox.

Include at least one thing you expect to be hard. Your most constrained network segment, your oldest system still in production, your most complex certificate chain. A pilot scoped to the easy part of the estate predicts nothing about the hard part, which is where the migration will actually be decided.

Fix the fee and the scope. An open-ended pilot becomes an unbudgeted implementation.

Run the same pilot with two vendors where the decision is close and the stakes justify it. Comparative pilots are more expensive and considerably more informative.

A worked pilot specification

Scope. One network segment, one business application and one certificate authority, selected to include at least one legacy or operational technology component.

Duration. Four to eight weeks. Under four weeks does not exercise the update cycle. Over eight weeks becomes an implementation.

Mandatory deliverables. A cryptographic inventory of the scoped environment in CycloneDX 1.7. A prioritised risk assessment identifying quantum-vulnerable assets ranked against your data shelf life. A documented migration path for the scoped estate. A written coverage statement identifying what the tooling could not see and why. All raw data and artefacts, retained by you, in open formats, irrespective of whether you proceed.

Acceptance criteria, all falsifiable.

1. Discovery identifies at least 95 per cent of the cryptographic assets in your hand-built ground truth for the scoped segment, with fewer than 10 per cent false positives.
2. The inventory validates against the CycloneDX 1.7 schema and imports without error into your configuration management database or security tooling.
3. Every discovered asset carries a primitive, a parameter set identifier and a security level, using standardised naming.
4. A live algorithm substitution completes within the stated window through configuration change, without product replacement, evidenced by packet capture.
5. With egress blocked at the network layer, the product completes a full discovery, reporting and update cycle. All attempted external connections are captured and reconciled against the vendor’s documented egress list, with no unexplained connections.
6. No key material, credential or inventory record is observed leaving the environment.

7. Compliance output maps to control identifiers in your reporting framework and is accepted by your internal audit function on review.
8. Total internal effort consumed is recorded and compared against the vendor's estimate.

Failure handling. Specify in advance what happens on failure of each criterion: remediation with a re-test window, partial acceptance with a documented gap, or termination. Agree it before the pilot starts, when the answer is still uncontested.

11. Stage 5: Contracting for agility

The contract is where a good evaluation is either preserved or given away. Ten clauses, none of them exotic, all of them frequently absent.

1. Algorithm substitution right. The customer may require support for any algorithm subsequently standardised by a named body, within a stated period, at no additional licence cost. Without this clause, crypto-agility is a feature you rent and re-purchase.

2. Cryptographic vulnerability notification. The vendor notifies the customer within a stated period of becoming aware of any cryptographic weakness in the product, any use of a non-approved algorithm, or any relevant published attack against an algorithm or implementation in use.

3. Patch commitment by severity. Stated remediation windows for cryptographic vulnerabilities specifically, distinct from general software defects, with a mechanism if they are missed.

4. CBOM delivery obligation. The vendor supplies a current CycloneDX CBOM for the product itself on each release, and on request. You cannot manage cryptographic risk in a product whose own cryptography is undisclosed.

5. Certification maintenance. Where certification formed part of the evaluation, the vendor maintains it across versions and notifies the customer if the deployed version falls outside the certified boundary. Certification decays quietly otherwise.

6. Data residency and access warranty. Contractual restatement of the architectural position established at criterion B3, including a warranty on where data is processed and a notification obligation for any change to the egress profile.

7. Interoperability warranty. The product interoperates with independent implementations of the standards it claims to support, with a remedy if it does not.

8. Performance warranty. Stated performance under stated conditions, measured against the pilot baseline rather than a datasheet.

9. Exit and portability. Data export in open formats, including full inventory history. Transition assistance at a pre-agreed rate. Source code escrow where the deployment is critical and the vendor’s viability score justified the concern.

10. Roadmap commitment with consequence. Dated commitments for capability that was material to the selection but not yet shipped, with a service credit or termination right attached. A roadmap commitment without a consequence is a statement of intent.

12. Stage 6: Governing the vendor after signature

PQC vendor selection is not a decision with an end date. The standards will change, the regulatory position will change, and the threat estimate will change. Build the re-evaluation into the relationship rather than discovering the need for it in an audit.

Re-evaluate on trigger, not only on renewal. The triggers that should force a review:

- A new algorithm is standardised, or an existing one is deprecated by a body that binds you.
- A published attack materially affects an algorithm or implementation you have deployed.
- The vendor's certification status changes, including a certificate moving to the historical list.
- The vendor is acquired, restructures, or changes its jurisdiction of operation.
- Your own regulatory position changes, including entry into a new market.
- The vendor misses a contracted roadmap date.

Maintain four artefacts continuously. A current cryptographic inventory. A current CBOM for each product in the estate. A verification log updated on each material vendor claim. A dated migration plan with named owners.

Measure the vendor on the things you weighted. If crypto-agility carried the highest weight in your selection, then time from standardisation to shipped support is the metric to track. Track it, and raise it every quarter.

Keep the exit warm. Data export in open formats is worth nothing if it has never been tested. Export annually and confirm the export is usable without the vendor's tooling.

13. The regulatory map

Status as at 12 August 2026. **Binding** means a legal or policy instrument carrying a compliance obligation. **Advisory** means guidance, however authoritative. The distinction matters commercially: a vendor may honestly describe alignment with advisory guidance while leaving you non-compliant with a binding instrument.

Verify every dated claim against the primary source before using it in a tender document. Several widely repeated dates in circulation do not survive contact with the source.

13.1 Standards

Standard	Algorithm	Status	Date
FIPS 203	ML-KEM (512, 768, 1024)	**Final**	13 Aug 2024
FIPS 204	ML-DSA (44, 65, 87)	**Final**	13 Aug 2024
FIPS 205	SLH-DSA (12 parameter sets)	**Final**	13 Aug 2024
SP 800-208	LMS, XMSS (stateful hash-based)	**Final**	2020
SP 800-227	KEM recommendations	**Final**	18 Sep 2025
FIPS 206	FN-DSA (Falcon)	**Not published, no draft**	Pending
HQC standard	HQC	**Algorithm selected, no draft standard**	Selected 11 Mar 2025
NIST IR 8547	Transition milestones	**Initial public draft only**	12 Nov 2024
NIST CSWP 39upd1	Crypto-agility	**Final**	29 Jun 2026

On NIST IR 8547. Its milestones are widely quoted as though they were a mandate. They are not: it remains an initial public draft, and its content is that ECDSA, RSA, finite-field and elliptic-curve Diffie-Hellman and MQV, and RSA key transport at 112-bit security strength are deprecated after 2030 and disallowed after 2035, and that those same algorithms plus EdDSA at 128-bit security strength and above are disallowed after 2035. Treat it as strong signalling, cite it as a draft, and do not describe it as a requirement.

13.2 Jurisdictional obligations

Jurisdiction	Instrument	Binding?	Key dates
US (NSS)	NSA CNSA 2.0	**Binding** for national security systems	ML-KEM-1024 and ML-DSA-87 required, with AES-256 and SHA-384 or SHA-512, and LMS or XMSS for software and firmware signing. Software and firmware signing exclusive use by 2030; networking equipment 2030; browsers, servers, cloud and operating systems 2033. New NSS acquisitions CNSA 2.0 compliant from 1 Jan 2027; equipment unable to support CNSA 2.0 phased out by 31 Dec 2030; algorithms mandated 31 Dec 2031; transition complete 2035

Jurisdiction	Instrument	Binding?	Key dates
US (federal civilian)	EO 14412 (22 Jun 2026) and OMB M-26-15 (24 Jun 2026)	**Binding** on agencies	Agency PQC migration plans due approximately 22 Oct 2026. TLS 1.3 or successor by 2 Jan 2030. High value assets and high impact systems: key establishment by 31 Dec 2030, digital signatures by 31 Dec 2031. Full migration 2035. CBOM minimum-element guidance expected around Mar 2027
US (contractors)	FAR rule directed by EO 14412	**Directed, not yet proposed**	EO 14412 directs the FAR Council to publish a proposed rule by approximately 19 Dec 2026, requiring covered contractors to comply by 31 Dec 2030 with NIST FIPS including those incorporating PQC. No proposed rule published as at 12 Aug 2026
US (federal, inventory)	OMB M-23-02 and the Quantum Computing Cybersecurity Preparedness Act	**Binding**	Annual prioritised cryptographic inventory to 2035, plus funding assessment
US (FedRAMP, CMMC)	Current rules	**No PQC-specific requirement in force**	Department of War PQC Strategy (1 Apr 2026) states intent to add PQC to CMMC; the rule change has not been made
Canada	TBS Security Policy Implementation Notice, *Migrating the Government of Canada to Post-Quantum Cryptography* (9 Oct 2025)	**Binding** on listed organisations	1 Apr 2026: departmental migration plan, and **all contracts with digital components must include PQC procurement clauses**. 1 Apr 2027: plans updated. 1 Apr 2028: system records updated, high-priority systems identified, transition begins. End 2031: high-priority systems complete. End 2035: all systems
Canada (guidance)	CCCS ITSM.40.001 (23 Jun 2025)	Advisory	Same milestone structure
Australia	ASD Information Security Manual (June 2026 release)	Advisory as a framework, **binding via the PSPF** for Commonwealth non-corporate entities	ism-2073: a PQC transition plan is developed, implemented and maintained. ism-1917 (June 2026 release): “The development and procurement of new cryptographic equipment, applications and libraries ensures support for the use of ML-DSA-87, ML-KEM-1024, SHA-384, SHA-512 and AES-256 by no later than 2030.” RSA, DH, ECDH and ECDSA not approved beyond 2030. **Also not approved beyond 2030: ML-KEM-768, ML-DSA-65, AES-128, AES-192, SHA-224, SHA-256**
Australia (PSPF)	PSPF Release 2026, effective 1 Jul 2026	**Binding**	Maintained PQC transition plan, and approved post-quantum algorithms on newly procured equipment
UK	NCSC *Timelines for migration to post-quantum cryptography* (20 Mar 2025)	**Advisory**	2028: define goals, complete discovery, build initial migration plan. 2031: complete highest-priority migration, refine roadmap. 2035: complete migration. Neither the Cyber Assessment Framework v4.0 nor the Cyber Security and Resilience Bill imposes a PQC requirement
EU	NIS Cooperation Group *Coordinated Implementation Roadmap*, v1.1 (11 Jun 2025)	**Advisory** to Member States	31 Dec 2026: national roadmaps established. 31 Dec 2030: high-risk use cases complete. 31 Dec 2035: medium-risk complete

Jurisdiction	Instrument	Binding?	Key dates
EU (certification)	ECCG/ENISA Agreed Cryptographic Mechanisms v2.0 (May 2025), v3.0 in draft	**Binding** where EUCC certification applies	Includes ML-KEM, ML-DSA, SLH-DSA, XMSS, LMS and FrodoKEM. **LWE and MLWE based mechanisms, which include ML-KEM and ML-DSA, should not be used standalone and should be combined with a well established classical mechanism.** In EUCC practice this operates as a strong expectation rather than an absolute prohibition, so confirm the treatment with your certification body. RSA below 3000 bits and DH groups below 3072 bits lost approved status 31 Dec 2025
France	ANSSI position papers (2022, follow-up Dec 2023)	Advisory, but drives *Visa de sécurité* certification	Phase 2, from 2025 to at least 2030: **hybrid mandatory** for any product claiming quantum resistance, except where the mitigation relies solely on hash-based signatures
Germany	BSI TR-02102-1, version 2026-01 (23 Jan 2026), and BSI press release of 11 Feb 2026	Advisory in general, binding where referenced in federal procurement	BSI recommends that classical asymmetric mechanisms no longer be used standalone: end of 2030 for highly sensitive applications, end of 2031 for key agreement generally, end of 2035 for classical signatures. BSI recommends combining them in hybrid form with post-quantum cryptography rather than immediate replacement
Japan	National Cyber Office and Cabinet Secretariat inter-ministerial interim summary (published late 2025)	Advisory, becoming binding via the Unified Standards for Cybersecurity	Migration to PQC by 2035 as a general rule; detailed agency roadmaps during FY2026
India	DST task force report, *Implementation of Quantum Safe Ecosystem in India* (dated 4 Feb 2026)	**Advisory**, explicitly not a regulatory mandate	Critical information infrastructure: 2027 foundations, 2028 high-priority migration, 2029 full adoption. Other government and enterprise: 2028, 2030, 2033
Singapore	MAS advisory MAS/TCRS/2024/01 (20 Feb 2024); CSA Quantum-Safe Handbook and Quantum Readiness Index v1.0 (16 Jul 2026)	**Advisory**	MAS asks financial institutions to maintain a cryptographic inventory, build capability and require quantum-resistant solutions from vendors. MAS has signalled formal supervisory expectations during 2026. Reported CII deadlines circulating in secondary sources should be verified before use
Malaysia	NACSA National PQC Readiness Roadmap (29 Oct 2025); MyKriptografi national cryptography policy (published Feb 2026)	**Advisory**	NACSA has described the roadmap as a strategic framework, not a regulatory mandate. NACSA is not a control framework and should not be presented as a mapping target
Global finance	G7 Cyber Expert Group statement (Jan 2026)	**Advisory**, explicitly not regulatory expectation	2030 to 2032: migrate most critical systems. 2035: sector target
Switzerland	FINMA Guidance 05/2026 (9 Jul 2026)	**Advisory**, with signalled supervisory attention	Recommends a board-approved PQC roadmap by mid-2027, with cryptographic inventory and crypto-agility in procurement. Excludes QKD

Jurisdiction	Instrument	Binding?	Key dates
EU (DORA)	Regulation 2022/2554 and Delegated Regulation 2024/1774	**Binding**, but no PQC-specific obligation	DORA does not mention quantum. The delegated regulation requires provisions for updating cryptographic technology in response to cryptanalytic developments. Recital 9 references quantum advancements, and a recital is interpretive, not operative
Payments	PCI DSS v4.0.1 requirement 12.3.3 (effective 31 Mar 2025)	**Binding** on in-scope entities	Requires a documented cipher suite and protocol inventory, annual review, active monitoring of cryptographic trends, and a documented response strategy. **It does not name quantum, PQC or any migration date.** It is a crypto-agility hook, not a PQC mandate

13.3 What this table means for vendor selection

Three practical conclusions.

Procurement clauses are already contractual in at least one jurisdiction. Canada's requirement that all contracts with digital components include PQC procurement clauses from 1 April 2026 means vendor selection is now inside the compliance perimeter, not upstream of it.

The binding dates cluster on 2030 and 2031, not 2035. The 2035 figure appears in almost every roadmap and is the least useful number in the set. The dates that will determine whether your program succeeded are 2030 and 2031, and working backwards from them through a two to three year discovery phase puts the decision point in the present.

Advisory guidance from an authoritative body still binds you commercially. A vendor whose product cannot satisfy NCSC guidance may still be sold to a UK buyer, but that buyer will carry the gap. Score against the guidance that applies to you, not only against the law.

14. The hybrid divergence problem

This is the most consequential unresolved question in PQC procurement, and it is almost entirely absent from vendor evaluation material.

A hybrid or composite construction combines a post-quantum algorithm with a classical one, so that the result is secure if either component holds. Regulators disagree, sharply and in writing, about whether this is required, recommended or discouraged.

Authority	Position on hybrid	Practical effect
ANSSI (France)	**Mandatory.** Any product including post-quantum mitigation must implement hybridisation, except where the mitigation relies solely on hash-based signatures such as XMSS, LMS or SPHINCS+	A standalone ML-KEM product cannot obtain a French security visa in the current phase
ECCG/ENISA (EU certification)	**Effectively required for LWE and MLWE based mechanisms.** The agreed mechanisms state these should not be used standalone and should be combined with a well established classical mechanism. Hash-based signatures may stand alone	Standalone ML-KEM or ML-DSA is unlikely to be accepted for EUCC purposes. Confirm with your certification body
BSI (Germany)	**Recommended, and required in practice where BSI guidance is referenced in procurement.** TR-02102-1 recommends combining a post-quantum mechanism with a classical one, and recognises FrodoKEM and Classic McEliece alongside ML-KEM	A standalone ML-KEM product is unlikely to satisfy BSI-referenced federal procurement, and support for non-NIST KEMs may also be expected
NCSC (UK)	**Temporary measure only.** Hybrid is a migration mechanism, not an end state	A hybrid-only product implies a second migration later
ASD (Australia)	**Not recommended, not prohibited.** ASD's stated reasoning is that against a cryptographically relevant quantum computer the security of a hybrid scheme reduces to that of its post-quantum component. Where hybrid is used, at least one component must be an approved algorithm	Hybrid is tolerated but confers no benefit in ASD's view
NSA (US, CNSA 2.0)	**Not required.** CNSA 2.0 specifies standalone ML-KEM-1024 and ML-DSA-87	Hybrid adds complexity without meeting a requirement

What a buyer should do

Establish which positions bind you, using your Stage 0.2 jurisdiction map. A vendor selling into Europe and Australia faces requirements that are close to opposite.

Make configurable hybrid posture a gate, not a preference. The correct product answer is not "we do hybrid" or "we do standalone." It is "hybrid posture is a configuration item, settable per deployment, per jurisdiction, per protocol." Anything less transfers the divergence risk to you.

Ask which specific constructions are supported, and against which standards. Hybrid key exchange in TLS 1.3 is standardised through RFC 10024, with the framework in the Informational RFC 9954 and X25519MLKEM768 the recommended code point. Composite post-quantum certificates were approved and in the RFC Editor queue as at August 2026, not yet published. A vendor treating a queued draft as a published standard has not read the datatracker.

Cost the second migration. If your jurisdiction treats hybrid as temporary, you are buying two migrations. Say so in the business case rather than discovering it in 2032.

15. Disqualifiers and red flags

Terminology that should end the conversation

“Quantum-safe certified.” No such certification exists. FIPS 140-3 validates cryptographic modules. Common Criteria certifies products against protection profiles. Neither produces a certificate that says quantum-safe.

“Quantum-proof”, “unbreakable”, “unhackable”, “future-proof”. No cryptography carries these properties, and a vendor selling to a technical buyer knows it.

“Military-grade” or “quantum-grade” encryption. Neither term has a definition. Where a real standard exists, a competent vendor cites the standard.

“Quantum-enhanced” as an undefined prefix. Ask what it modifies. The answer is usually nothing.

“Unconditionally secure” or “perfect secrecy” stated without preconditions. These are precise terms with strict assumptions, and stripping the assumptions inverts the meaning.

Structural red flags

A proprietary core algorithm. A refusal to publish the primitive is a refusal to allow cryptanalysis. This has been settled since the nineteenth century.

QKD offered as an answer to a PQC requirement. Different technology, different problem, different constraints. Several national authorities have stated they will not support QKD for government use, and none of the binding PQC instruments accept it as a substitute.

Deflecting technical questions rather than answering them. A vendor who redirects a question about parameter sets to a discussion of business outcomes has given you the answer.

Credential laundering. Awards from pay-to-enter schemes, papers in predatory venues, advisory boards with no verifiable involvement, or logos of standards bodies where the involvement is membership rather than contribution.

Refusal to allow independent technical review. A vendor confident in their implementation welcomes a cryptographer in the room.

Technical red flags

Reference implementation without patch confirmation. The CRYSTALS reference code carried KyberSlash and the CVE-2024-37880 pattern. A vendor who cannot confirm the fixes has not looked.

PQClean-derived code with no migration plan, given that project’s archival in July 2026.

A CAVP certificate presented as module validation, or a modules-in-process listing presented as validation.

A quantum key distribution protection profile presented as PQC certification. This specific substitution occurs and is easy to miss.

“Formally verified” without artefact, specification, property list and trusted computing base. All four, or the claim is unassessable.

“Constant-time” without binary-level evidence on the toolchain and target you will deploy.

Hand-authored declarative CBOMs presented as discovery output.

Brand-era algorithm names in current documentation. Kyber, Dilithium and SPHINCS+ became ML-KEM, ML-DSA and SLH-DSA in the draft standards of August 2023, and those names carried into the final standards of August 2024. Falcon is designated FN-DSA, though FIPS 206 remains unpublished. Documentation that has not caught up is documentation that has not been maintained.

A single hybrid posture with no configurability, given Section 14.

16. The eight most common buyer mistakes

1. Buying the inventory instead of the migration. Cryptographic discovery is now close to a commodity. Prioritisation against your risk model, execution in legacy and operational technology estates, and re-verification after change are the hard parts, and they are where the value is. Analyst commentary through 2026 has noted that a substantial share of what is marketed as novel PQC capability is cryptographic inventory, certificate tracking and dependency mapping that mature security programs should already perform.

2. Treating algorithm support as the decision. Algorithm support is table stakes and easy to verify. Implementation quality, crypto-agility and integration decide whether the migration succeeds, and all three are harder to assess, which is precisely why they get less attention than they deserve.

3. Accepting source-level claims about binary-level properties. Constant-time source code compiled by an optimising compiler is not necessarily constant-time. This is documented, not hypothetical.

4. Confusing validation types. CAVP is not CMVP. In process is not validated. A module certificate does not tell you the PQC algorithms are inside the boundary until you read the security policy.

5. Scoping the pilot to the easy part of the estate. The migration will be decided in operational technology, embedded systems, long-lived hardware and the systems nobody wants to touch. A pilot that avoids them predicts nothing.

6. Ignoring jurisdictional divergence until after signature. Particularly on hybrid. Section 14 is a compliance conflict waiting to be inherited.

7. Letting the vendor write the acceptance criteria. A test the supplier helped design is a demonstration.

8. Treating selection as a one-time decision. Standards will change, algorithms will be deprecated, attacks will be published and vendors will be acquired. Build the re-evaluation triggers into the contract, as in Section 12, or you will be running this evaluation again from a weaker position.

17. Scope limits: what this standard does not cover

Stating limits is part of being usable. PQ-VES 1.0 does not cover:

Quantum key distribution. A distinct technology with distinct assumptions, constraints and authority positions. It should not be scored on the same axis as PQC, and this framework does not attempt to.

Quantum random number generation. Relevant to cryptographic implementation, and evaluated here only indirectly through entropy source questions in criterion A2. A dedicated evaluation should assess it against BSI AIS 20/31 functionality classes.

Non-cryptographic quantum security claims. Products marketed as quantum-related without a cryptographic function are outside scope.

Internal migration program management. How you sequence, resource and govern your own migration is addressed by migration roadmaps from several bodies, and this standard assumes that work is happening in parallel.

Pricing benchmarks. The market is too young and too varied for a defensible benchmark, and a wrong benchmark is worse than none.

Jurisdictions not listed in Section 13. Absence indicates that a primary source could not be verified as at August 2026, not that no requirement exists.

18. Frequently asked questions

How many post-quantum algorithms are actually standardised?

Three. FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA), all finalised on 13 August 2024. SP 800-208 covers the stateful hash-based signature schemes LMS and XMSS. FIPS 206 (FN-DSA) has not been published, not even as a draft. HQC was selected in March 2025 and has no published standard. A vendor describing either as standardised is either behind or overstating.

What does "FIPS validated" actually tell me?

Less than most buyers assume. FIPS 140-3 validation is module-scoped: a vendor can hold a valid certificate whose approved algorithm list contains no post-quantum algorithm at all. Ask for the certificate number, read the security policy, and confirm that the PQC algorithms sit inside the cryptographic boundary in approved mode, that the certificate is active rather than historical, that it does not carry an interim validation caveat with a shortened expiry, and that the version you will deploy is the version validated. A CAVP algorithm certificate is a weaker and different signal. A modules-in-process listing is not validation at all, though it is legitimate information and should be scored as such rather than dismissed.

How do I verify a formal verification claim?

Ask four questions and expect precise answers. Which artefact was verified, meaning source, intermediate representation or shipped assembly. Against which specification, and is it published. Which properties were proven, named individually rather than gestured at. What is the trusted computing base, meaning which prover, which compiler and which dependencies are assumed correct. Then ask whether the proofs re-run in continuous integration on every commit in non-lax mode with no admitted assumptions, and ask to see the log. Finally, ask for the published caveats document. A vendor who has never written one has probably not thought about the limits of the claim.

What does formal verification not prove?

Resistance to power analysis, electromagnetic emission and fault injection. Correctness of unverified glue code, key management or random number generation. Constant-time behaviour of the compiled binary, unless the verification specifically targets assembly. Anything about algorithms, platforms or build configurations outside the stated scope. And nothing at all, if the specification the proof targets is itself wrong, which has occurred in practice.

Is hybrid deployment required?

It depends on your jurisdiction, and the positions are close to opposite. France's ANSSI mandates it. The EU's agreed cryptographic mechanisms state that LWE and MLWE based schemes should not be used standalone. Germany's BSI recommends hybrid deployment with dated milestones. The UK's NCSC treats it as a temporary migration measure. Australia's ASD does not recommend it while not prohibiting it. The NSA's CNSA 2.0 does not require it. If you operate across these markets, require configurable hybrid posture as a hard gate. See Section 14.

What should a pilot deliver?

A cryptographic inventory of the scoped environment in CycloneDX 1.7, a prioritised risk assessment ranking quantum-vulnerable assets against your data shelf life, a documented migration path, and a written coverage statement identifying what the tooling could not see. All raw data and artefacts should be retained by you in open formats regardless of whether you proceed. If a vendor cannot produce these in a pilot, they cannot produce them in production.

Can PQC tooling work in fully disconnected environments?

Some can. Test rather than accept the claim. The specific things that break disconnected deployments are licensing checks, entitlement validation, telemetry upload and automatic update channels. Require installation from approved media using a signed and independently verifiable bundle, require updates to be deliverable through your change management process, and verify by running a full cycle with egress blocked at the network layer while capturing every attempted connection.

How do I compare a discovery tool against a cryptographic library?

You do not. They solve different problems and fail in different ways. Run separate evaluations per product category using the overlays in Section 8, and combine the results at the architecture level rather than in a single score.

Is quantum key distribution an alternative to PQC?

No, and treating it as one is a red flag. QKD addresses key distribution over a physical channel with different assumptions, no built-in authentication and significant deployment constraints. The UK's NCSC stated in August 2025 that it will not support QKD for government or military applications and recommends PQC as the mitigation, and comparable positions are held by other authorities. QKD may be appropriate for specific problems. It does not satisfy a PQC requirement.

How often should this evaluation be repeated?

On trigger rather than on a schedule. A new algorithm is standardised or deprecated. A published attack affects something you have deployed. A vendor's certification status changes. A vendor is acquired or changes jurisdiction. Your own regulatory position changes. A contracted roadmap date is missed. Section 12 sets out the governance model.

19. Maintaining this standard

PQ-VES 1.0 is dated deliberately. A framework that presents itself as timeless in a field moving this quickly is misleading its readers.

Revision triggers. Publication of FIPS 206 or the HQC standard. Finalisation of NIST IR 8547. A material change to CNSA 2.0. Publication of CBOM minimum elements under EO 14412. Adoption of the proposed FAR rule. A change to the ECCG/ENISA position on hybrid. Any new binding national instrument.

What version 2.0 should add. Quantitative benchmarks for discovery coverage drawn from real evaluations rather than assertion. A maturity model for buyer organisations, since the framework currently assumes a competent buyer. Sector-specific overlays for health, energy and telecommunications. Worked scoring examples contributed by organisations that have run the process.

Criticism is the point. The weightings are a considered opinion, not a finding. If your evaluation experience contradicts them, that is more useful than agreement.

Appendix A: Glossary

CAMM. Crypto Agility Maturity Model. A five-level scale (0 to 4) for assessing cryptographic agility, with level 3 requiring demonstrated migration between cryptographic methods.

CAVP. Cryptographic Algorithm Validation Program. Validates that an algorithm implementation passes known-answer tests. Not a module validation.

CBOM. Cryptographic Bill of Materials. A CycloneDX bill of materials whose components carry cryptographic properties. Not a separate file format.

CMVP. Cryptographic Module Validation Program. Validates cryptographic modules against FIPS 140-3. Module-scoped, not algorithm-scoped.

CNSA 2.0. Commercial National Security Algorithm Suite 2.0. The NSA's algorithm requirements for US national security systems. Requires ML-KEM-1024, ML-DSA-87, AES-256 and SHA-384 or SHA-512, with LMS or XMSS for software and firmware signing.

Constant-time. An implementation property in which execution time does not depend on secret data. A property of the compiled binary on a specific toolchain and target, not of the source.

CRQC. Cryptographically relevant quantum computer. A quantum computer capable of breaking currently deployed public-key cryptography.

Crypto-agility. Per NIST CSWP 39, the capabilities needed to replace and adapt cryptographic algorithms across protocols, applications, software, hardware, firmware and infrastructure while preserving security and ongoing operations.

EUCC. The European Union common criteria-based cybersecurity certification scheme.

Formal verification. A machine-checked proof that a specific artefact satisfies specific stated properties relative to a specific specification, under a specific trusted computing base. All four qualifiers are load-bearing.

Harvest now, decrypt later (HNDL). An adversary recording encrypted traffic today for decryption once a CRQC is available, converting a future capability into a present-day confidentiality loss.

Hybrid. A construction combining a post-quantum algorithm with a classical one, secure if either component holds. Required by some authorities, discouraged by others.

ML-DSA. Module-Lattice-Based Digital Signature Algorithm, FIPS 204. Parameter sets 44, 65 and 87.

ML-KEM. Module-Lattice-Based Key Encapsulation Mechanism, FIPS 203. Parameter sets 512, 768 and 1024.

Mosca's inequality. If X plus Y exceeds Z, where X is data shelf life, Y is migration time and Z is time to a CRQC, the organisation is already exposed.

QKD. Quantum key distribution. A physical-layer key distribution technology, distinct from PQC, without built-in authentication.

SLH-DSA. Stateless Hash-Based Digital Signature Algorithm, FIPS 205.

Speculative constant-time. Constant-time behaviour maintained under speculative execution. A stronger property than constant-time, and rarely proven.

Trusted computing base. The set of components whose correctness a security claim depends on, and which are assumed rather than proven.

Appendix B: Primary sources

Cited where a claim in this document depends on them. Verify status before relying on any dated claim.

Standards and technical

- FIPS 203, 204, 205: https://csrc.nist.gov/pubs/fips/203/final, /204/final, /205/final
- NIST IR 8547 (initial public draft): https://csrc.nist.gov/pubs/ir/8547/ipd
- NIST CSWP 39upd1, crypto-agility: https://csrc.nist.gov/pubs/cswp/39/upd1/considerations-for-achieving-crypto-agility/final
- CMVP and modules in process: https://csrc.nist.gov/projects/cryptographic-module-validation-program
- CycloneDX CBOM: https://cyclonedx.org/capabilities/cbom/
- RFC 9954, hybrid key exchange in TLS 1.3: https://datatracker.ietf.org/doc/rfc9954/
- Crypto Agility Maturity Model: https://camm.h-da.io/model/

Policy and regulatory

- NSA CNSA 2.0 resources: https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/
- Executive Order 14412: https://www.federalregister.gov/documents/2026/06/25/2026-12909/securing-the-nation-against-advanced-cryptographic-attacks
- OMB M-26-15: https://www.whitehouse.gov/wp-content/uploads/2026/06/M-26-15-Execution-of-the-Migration-to-Post-Quantum-Cryptography.pdf
- Canada, TBS Security Policy Implementation Notice: https://www.canada.ca/en/government/system/digital-government/policies-standards/spin/migrating-government-canada-post-quantum-cryptography.html
- Canada, CCCS ITSM.40.001: https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001
- UK NCSC migration timelines: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines
- EU coordinated implementation roadmap: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
- ANSSI position on the PQC transition: https://cyber.gouv.fr/en/publications/anssi-views-post-quantum-cryptography-transition
- ASD Information Security Manual, machine-readable catalogue: https://github.com/AustralianCyberSecurityCentre/ism-oscal
- BSI TR-02102-1 and the BSI recommendation of 11 February 2026: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/260211_Ende_klassischer_Verschluesselungsverfahren.html
- RFC 10024, post-quantum hybrid ECDHE-MLKEM key agreement for TLS 1.3: https://www.rfc-editor.org/info/rfc10024/
- MAS advisory on quantum risks: https://www.mas.gov.sg/regulation/circulars/advisory-on-addressing-the-cybersecurity-risks-associated-with-quantum
- G7 Cyber Expert Group quantum roadmap: https://home.treasury.gov/system/files/136/G7-CEG-Quantum-Roadmap.pdf
- FINMA Guidance 05/2026: https://www.finma.ch/en/documentation/finma-guidance/

Evaluation frameworks and research

- PQCC PQC Solution Analysis Guide (27 May 2026): https://pqcc.org/solution-analysis-guide/
- PQCC International PQC Requirements: https://pqcc.org/international-pqc-requirements/
- PKI Consortium PQC Capabilities Matrix: https://pkic.org/wg/pqc/pqccm/
- ETSI TR 104 016, repeatable framework for quantum-safe migrations
- GSMA PQ.03, PQC guidelines for telecom use cases
- Cloud Security Alliance, A Practitioner's Guide to Post-Quantum Cryptography
- KyberSlash: https://kyberslash.cr.yp.to/ and https://eprint.iacr.org/2024/1049.pdf
- CVE-2024-37880 analysis: https://blog.cr.yp.to/20240803-clang.html
- Global Risk Institute Quantum Threat Timeline Report 2025: https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/
- NCSC on quantum networking technologies and QKD: https://www.ncsc.gov.uk/paper/quantum-networking-technologies

Publisher note and disclosure

Published by ExeQuantum. ExeQuantum is a post-quantum cryptographic engineering company. It is a vendor in the market this document describes.

That is a conflict of interest, and the honest response to it is disclosure plus design. This standard names no products, including ExeQuantum's. It contains no vendor recommendations and no product comparisons. Every criterion is written so that it could be applied to ExeQuantum by a buyer, with the same evidence tiers and the same disqualifiers, and we would expect to be held to them. Several criteria are ones on which ExeQuantum, like most vendors in this market, would not score full marks today.

We published it because the alternative was worse. Buyers are making multi-decade cryptographic decisions against evaluation material that stops at what vendors say they support, and a market in which nobody can tell good engineering from good marketing is a market that eventually punishes both.

Contributions and criticism. PQ-VES 1.0 is released under Creative Commons Attribution 4.0. Fork it, strip the attribution if you prefer, embed it in your tender documents. If you disagree with a weighting, a gate or a scoring anchor, we would rather hear it than not. Corrections to any factual claim in Section 13 are particularly welcome, and will be reflected in the next revision with acknowledgement.

Version 1.0. Published 12 August 2026. Content current as at that date.

Sovereign · Transparent · Agile · Compliant