

ASSESSOR GUIDE

Assessing a vendor's post-quantum readiness

Criteria for judging supplier responses, and the action that follows each outcome.

Companion to the vendor questionnaire, for teams evaluating supplier responses

October 2026 · Free to use and adapt with attribution

This toolkit supports preliminary supplier assessment and migration planning. It does not certify vendor readiness, verify security claims, or replace technical assessment, contractual review, or applicable regulatory requirements. Organizations in the United Arab Emirates should confirm the requirements that apply to them with the UAE Cyber Security Council and the National Cryptography Center, together with any sector requirements.

What this guide is for

Part of the cryptography protecting your organization sits inside products you buy, on release schedules you do not control. The vendor questionnaire asks twenty questions about one named product. This guide sets out which suppliers to send it to, the criteria for judging the responses, and the actions that follow.

How the two documents are used

The questionnaire is the document you send to a supplier. This guide stays with the team reading the answers, and sets out the criteria they judge those answers against. Share it across your assessment team, and with anyone who will act on the result.

THE PROCESS

Four steps

1. Decide who to ask

List the products you depend on. Give each one an assessment tier, which sets how many of the twenty questions you send. Part 2 explains how.

2. Send the questionnaire

One questionnaire per product, not per company. Name the product, version and deployment you are asking about.

3. Judge the answers

Read each response against the criteria in part 4. Record each answer as accepted, clarification needed, or not supported, then give the product one overall outcome using part 6.

4. Act on the outcome

Chase missing evidence, and where a supplier's date sits on your critical path, move it into your own migration plan. Part 6 sets out the action for each outcome, and part 7 the follow-up that applies to every assessment.

Not every supplier needs all twenty

An assessment tier decides how many questions a given product gets.

Twenty questions to every supplier produces more responses than can be reviewed properly, and uses supplier effort you will need later on the products that matter.

Set the tier from four properties of your environment, not from anything the vendor says: how sensitive the data is, how long it has to stay confidential, how critical the service is, and how hard the supplier would be to replace. Where the supplier manages the keys and the protocol configuration, raise the tier.

Tier the product, not the company. A supplier may be well advanced in one product and have done nothing in another.

Tier 1

All twenty questions

The supplier manages cryptography protecting sensitive information, carries data with a long confidentiality requirement, supports a critical service, or would be hard to replace. Request evidence with every answer.

Tier 2

Sections A and C, plus Q14 and Q20

Important but not critical, or you hold most of the cryptographic control yourself. This gives you the inventory, the current capability, a date, and a notification route.

Tier 3

Q1, Q9 and Q14

Low sensitivity, easily replaced, or little cryptographic dependency. Enough to tell you whether a fuller assessment is needed later.

What a vendor means by we support post-quantum

The same phrase covers five different claims.

A vendor can say a product supports post-quantum cryptography and mean any of the five claims below. Each can be accurate on its own. They are not a sequence: a product can be commercially available before a module validation completes, and validation is not available or required for every implementation. Treat them as five separate claims to verify, and record which ones the response actually makes.

1 The algorithm is standardized	Proves a relevant standard exists. It says nothing about any particular product.
2 The product implements it	Proves the supplier has implemented the algorithm for a specific function. Check the version, the parameter set, and which functions are covered.
3 The implementation is validated	Proves specified testing or validation has been completed, within a defined scope. Check the certificate number, the module version, and what the scope actually covers.
4 The capability is commercially available	Proves customers can deploy a supported version, not a preview or a demonstration.
5 The capability is enabled in your environment	Proves the feature has actually been configured and tested in your deployment. Only this claim means the protection is running.

Claims, not stages

A product at claim two can be announced as supporting post-quantum cryptography. Recorded as claim five, it enters your inventory as protected while the capability is not yet running anywhere. Verify each claim on its own evidence; Q10 separates announced from generally available.

Which algorithm does what

What Q9 asks about. The four are not interchangeable.

A sufficiently capable quantum computer breaks the public key cryptography used to agree keys and to sign. The following algorithms address different cryptographic functions: three are finalized standards, while FN-DSA remains in standardization. Key establishment and signatures are separate functions, so a product that covers one has not covered the other.

ML-KEM Key establishment	Establishes shared keying material from which the keys protecting a connection are derived. This is the urgent case for data with a long confidentiality requirement: traffic that can be intercepted and recorded today can be decrypted later, so the protection has to be in place before sensitive communications are exposed to capture.
ML-DSA Digital signatures	Authentication, certificates, and signing software and firmware. Judge each use by how long the signature must remain trustworthy and verifiable: a session signature is verified and discarded, while a firmware signing key, an archived signed record, or a long-lived certificate has to resist forgery for years. The required lifetime depends on the use case.
SLH-DSA Digital signatures	Hash-based, so it rests on different and more conservative assumptions than ML-DSA. Signatures are larger and signing is slower, which shapes where it fits. A long-lived trust anchor is one such case, not the limit of what it is for.
FN-DSA Digital signatures, not yet finalized	Compact signatures for constrained environments. Selected but still in standardization, so treat vendor support as a roadmap item rather than a standards claim.

Ask for the parameter set

The family name is not enough. ML-KEM-768 and ML-KEM-1024 are different security levels, and two products that both claim ML-KEM will not interoperate unless they agree on one.

Scope

These questions cover public key cryptography, where the quantum risk sits. Symmetric algorithms and hash functions are affected far less, and are covered through key and output lengths in the inventory at Q1.

How to judge each answer

The twenty questions, what a useful answer to each one contains, and what should send you back to the vendor.

SECTION A

Cryptographic visibility and dependencies

Q1**Cryptographic inventory**

Can you provide a current inventory of the cryptographic algorithms, protocols, libraries, and certificates used by this product?

A useful answer. A dated inventory that names algorithms and key sizes, says which product versions it covers, and is explicit about what sits outside its scope.

Follow up if. A statement that the product uses industry standard encryption, with no inventory and no indication of where cryptography is implemented.

Q2**Where public key cryptography is used**

Where does this product use public key cryptography, and for what?

A useful answer. A function by function answer that separates key establishment from signatures, and covers internal component traffic as well as customer facing connections.

Follow up if. An answer that only addresses the customer facing connection, usually TLS, and leaves signing and internal traffic unmentioned.

Q3**Third party dependencies**

Which third party libraries, hardware components, cloud services, or suppliers could affect your migration timeline?

A useful answer. Named components with named owners, and a statement of which dependencies the vendor does not control.

Follow up if. A general assurance that suppliers are being engaged, with no components named.

Q4**Upgrade path**

Can the cryptography in this product be changed without replacing hardware or the platform?

A useful answer. The update mechanism described, with the specific components that cannot be updated in place.

Follow up if. A yes with no explanation of the mechanism, or silence on embedded and field deployed equipment.

Q5

Products that cannot be upgraded

Where this product, or components of it, cannot be upgraded to post-quantum cryptography in place, what do you commit to for affected customers?

A useful answer. Named components with the options the vendor will offer, such as replacement, a migration path, or compensating controls, each with a timeline.

Follow up if. The limitation acknowledged with no commitment on what happens to affected customers, or affected components left unnamed.

SECTION B**Risk assessment and governance**

Q6

Risk assessment

Have you assessed this product's exposure to a cryptographically relevant quantum computer?

A useful answer. A dated assessment with a stated scope, the resulting priorities, and a review cycle.

Follow up if. A readiness claim with no assessment date, scope, or findings.

Q7

Long-lived data confidentiality

How have you assessed the risk that encrypted customer information collected today could be decrypted in the future by a cryptographically relevant quantum computer?

A useful answer. The data flows evaluated, the mechanisms protecting each, the confidentiality lifetime assumed, and the mitigations or migration plans that follow from it.

Follow up if. An answer that treats the risk as starting only when a quantum computer arrives, with nothing about data that can be recorded today.

Q8

Accountability and governance

Which role and department are accountable for your migration program, and how is progress governed?

A useful answer. An accountable role above project level, identified with its department, an approved plan, and a regular reporting cycle.

Follow up if. A public commitment with no accountable role identified and no plan behind it.

SECTION C

Standards and technical capability

Q9

Algorithm support

Which standardized post-quantum algorithms does this product support today, and for which functions? Give a status for each algorithm, and name the exact parameter sets.

A useful answer. A status per algorithm, with exact parameter sets such as ML-KEM-768 or ML-DSA-65, tied to named product versions and named functions.

Follow up if. A claim of full post-quantum support with no algorithm names, parameter sets, or versions attached.

Q10

Production availability

For each algorithm you named in Q9, what is its release status for production use today? Answer for each one separately.

A useful answer. Each capability named in Q9 labelled generally available, limited release, beta, or demonstration, with the support terms for each.

Follow up if. A capability shown in a laboratory or preview program, described in the same terms as a generally available feature.

Q11

Hybrid and post-quantum only modes

Does this product support a hybrid mode combining a traditional algorithm with a post-quantum algorithm, and does it support a post-quantum only mode? Answer for each mode separately.

A useful answer. Named combinations with interoperability evidence, and a clear statement of whether hybrid is positioned as transitional or long-term.

Follow up if. Hybrid named without the combinations, or no answer on whether a post-quantum only mode exists or is planned.

Q12

Validation and interoperability

Which of the following can you provide, and what is in progress? Each kind of evidence proves something different, so answer for each one separately.

A useful answer. Evidence labelled by kind: algorithm test results, validated module certificates with the module version and scope, third party assessments, and interoperability reports. Each proves something different.

Follow up if. Compliance claimed in general terms, or a certificate for one module version presented as covering every product and deployment that uses it.

Q13

Crypto-agility

How can cryptographic algorithms be changed as standards and requirements change?

A useful answer. Algorithm choice exposed through configuration or policy, with a documented rollback path.

Follow up if. One planned upgrade described as agility, with no mechanism for changes after it.

SECTION D

Migration plan and customer impact

Q14

Product roadmap

Can you provide a migration roadmap for this product with dated milestones?

A useful answer. Dated milestones at product level, with the dependencies and open decisions stated alongside them.

Follow up if. A roadmap commitment with no dates, or dates that apply to the vendor's portfolio rather than to the product you buy.

Q15

Changes required

What changes will be required in the product, and in the customer's environment?

A useful answer. A list separating what the vendor changes from what the customer changes, with the effort for each.

Follow up if. A statement that the change will be seamless, with no customer side requirements identified.

Q16

Deployment and testing

Which of the following exist today for the post-quantum capabilities in this product, and can be shared during the assessment?

A useful answer. Documentation that exists today and can be shared now, with a rollback path described.

Follow up if. Documentation promised at release, with nothing available to review during the assessment.

Q17

Interoperability during transition

How will this product interoperate with systems that have not migrated?

A useful answer. Named transitional configurations with their limits stated, and downgrade protection addressed explicitly.

Follow up if. No transitional configuration named, or a plan that assumes both ends upgrade at the same time.

SECTION E

Cost and support

Q18

Cost

Will the post-quantum capabilities in this product require additional licensing or hardware?

A useful answer. A statement of what the current agreement covers and what is chargeable, or an explicit not yet decided.

Follow up if. No answer on hardware, or cost deferred without saying whether the capability is included today.

Q19

Documentation and support

What documentation, technical support, and migration assistance will you provide?

A useful answer. Named material, a support arrangement covering the migration period, and a named escalation route.

Follow up if. Standard support quoted with no arrangement specific to the migration.

Q20

Notification

How will you notify customers of changes to algorithms, of vulnerabilities, and of changes to migration timelines?

A useful answer. A defined channel with a notice period for material changes, ideally reflected in the agreement.

Follow up if. Notification by release notes alone, with no notice period and no commitment to flag cryptographic changes.

Neither a yes nor a no

An illustrative VPN supplier whose answers are mixed, which is how most real responses arrive.

Part 4 judges answers one at a time. The harder judgement is the overall one, when the vendor has made genuine progress and the gaps still matter. The responses below are illustrative.

Area	Vendor response	What it tells you
PQC support	ML-KEM available in the latest gateway version	Real capability, for one version. Which parameter set, and for which functions?
Hybrid modes	Supported in some configurations	Limited. The supported configurations are not named.
Existing clients	Older client versions unsupported	The blocker. A full rollout depends on upgrading or replacing these.
Cryptographic inventory	Partial	Scope unknown. What is excluded, and why?
Migration roadmap	Q2 2027 target for full support	A date to hold the vendor to, with its dependencies unstated.
Testing documentation	Available on request	Request it during the assessment, not at deployment.

The vendor has made progress, but important dependencies remain. The organization cannot assume its current VPN environment is protected: the capability exists at the gateway, and the estate includes clients it does not cover. The response is neither accepted nor rejected. It defines the work.

Recorded outcome

Clarification needed, with the dependencies named: an inventory of affected clients, the supported configurations confirmed in writing, the inventory's exclusions, the testing documentation, and a dated plan for client support. Overall assessment: partially ready.

From twenty answers to one outcome

So results can be compared across suppliers and acted on.

Record each answer as accepted, clarification needed, or not supported. Then give the product one overall outcome from the five below. The action for each one is on the following page.

Ready for technical verification	The relevant capabilities appear available, with sufficient evidence to begin customer testing.
Partially ready	Some of what you need is usable today, with material gaps or dependencies around it. The worked example in part 5 lands here.
Roadmap dependent	The capability you need is planned but not available today. The assessment rests on dates the vendor has committed to.
Insufficient information	The vendor has not provided enough evidence for a meaningful assessment.
Material readiness gap	A significant unsupported capability affects the customer's migration plan.

When two outcomes both seem to fit

Partially ready and roadmap dependent are the pair most often confused. The test is whether anything you need is usable today. If you can begin testing part of it now, record partially ready. If the capability is not available yet and the assessment rests entirely on committed dates, record roadmap dependent. Where the vendor has not given you enough to tell, that is insufficient information, which is a statement about the response rather than about the product.

Advisory, not a certification

These outcomes support prioritization and follow-up; they do not certify anything. A supplier can be partially ready and still be appropriate for a specific deployment, depending on what that deployment requires and when.

What each outcome calls for

The action that follows each of the five, once it is recorded.

Ready for technical verification

Arrange technical verification and an implementation review.

Partially ready

Verify what exists, and plan around what does not: confirm the clarifications, then treat the remaining gaps as roadmap items or risks.

Roadmap dependent

Record the dates and dependencies in your migration plan, and agree follow-up milestones with the supplier.

Insufficient information

Request specific evidence, assign a follow-up owner, and set a response deadline.

Material readiness gap

Assess the business impact, escalate the risk, and consider alternative suppliers, compensating controls, or replacement plans.

What to do once the answers are in

Where the answers go, and who owns each gap.

Record what you learned

Put supplier gaps into your risk register with an owner, alongside every other third party risk.

Close the evidence gaps

Go back for the specific documents, naming each one.

Put dependencies into your plan

Where a supplier date sits on your critical path, it belongs in your migration plan, not only in the assessment.

Change what you buy next

Move the questions that mattered into your standard procurement pack, so new suppliers answer them before you sign.

Set a review date

Revisit tier 1 suppliers at least annually, and at every contract renewal.

The request

Name the product and version, state what the answers will be used for, and set a deadline that allows the supplier to coordinate across product, engineering and legal. Four weeks is a reasonable default for a tier 1 request.

Where this sits

A vendor questionnaire can tell you what a supplier knows about its cryptography and migration plans. It cannot tell you every cryptographic component running across your own environment. Supplier assessment sits alongside cryptographic discovery, risk assessment, and migration planning, not in place of them.

Assessment record sheet

One row per product. Copy it, print it, or keep it alongside the responses.

Supplier and product	Tier	Outcome	Evidence still owed	Owner and date

Filling it in

Outcome is one of the five in part 6. Evidence still owed is the specific document or answer you are waiting on, named rather than described. Owner is a person on your side, not the supplier, because an unowned gap is the one that goes unchased.